Leitfaden für

TARGET2-Nutzer

Version 15.1

März 2022

Das vorliegende Dokument ist eine Übersetzung des englischen Originaltextes durch die Deutsche Bundesbank.

Der englische und rechtlich verbindliche Originaltext ist auf der Website der Deutschen Bundesbank als pdf-Download verfügbar. Dort ist auch diese Übersetzung als pdf-Datei abrufbar.

Leitfaden

Inhalt

LEITFADEN FÜR TARGET2-NUTZER

Inhalt

Inhalt

Inhalt

Inhalt

Inhalt

Verzeichnis der Abbildungen, Tabellen und Kästen

Abbildungen

Tabellen

Verzeichnis der Abbildungen, Tabellen und Kästen

Kästen

1 Einleitung

Der vorliegende „Leitfaden für TARGET2-Nutzer“ (nachfolgend „TARGET2-Leitfaden“) versteht sich als Standardwerk für **TARGET2-Nutzer** (Kreditinstitute, Nebensysteme und sonstige Einrichtungen, die Zahlungen in TARGET2 abwickeln[1] sowie Einrichtungen, die über mindestens ein TIPS-Geldkonto und/oder T2S-Geldkonto verfügen), das ihnen ein besseres Verständnis der allgemeinen Funktionsweise des TARGET2-Systems und eine möglichst effiziente Nutzung ermöglichen soll. In dem Leitfaden sollen sämtliche operativen Aspekte im Zusammenhang mit der alltäglichen TARGET2-Nutzung einschließlich der Geldverrechnung über TARGET Instant Payment Settlement (TIPS) und TARGET2-Securities (T2S) in Euro behandelt werden, um einen reibungslosen Betrieb zu gewährleisten.

Außerdem stellt der TARGET2-Leitfaden die Funktionalität des Gesamtsystems sowie die Besonderheiten im Hinblick auf die einzelnen Zentralbanken dar, d. h. die nationalen Zentralbanken im Euroraum (NZBen), die Europäische Zentralbank (EZB) und sonstige nationale Zentralbanken, die an TARGET2 angeschlossen sind. Dokumentiert sind die zentralbankspezifischen Besonderheiten auf der Website der jeweiligen nationalen Notenbank.

Der TARGET2-Leitfaden wurde so konzipiert, dass er wann immer erforderlich aktualisierbar ist und sowohl die Zentralbanken – einschließlich der drei bzw. vier Anbieter-Zentralbanken (3ZB/4ZB) und der Zentralbanken, die die TIPS-Plattform bereitstellen[2] – wie auch die TARGET2-Nutzer an seiner Ausgestaltung mitwirken können. Er ist als ein dynamisches Dokument gedacht, in dem Aktualisierungen aufgegriffen werden, die entweder von nationalen TARGET2-Stakeholder-Gruppen (NSG) ausgehen, aus vom Europäischen System der Zentralbanken (ESZB) für TARGET2-Nutzer auf Euroraumebene organisierten Veranstaltungen resultieren oder aus operativen Erfahrungen und neuen Systemversionen rühren.

Es ist durchaus denkbar, dass der Leitfaden auch für andere mit TARGET2 befasste Gruppen oder für die Öffentlichkeit von Interesse ist, weshalb er auf der TARGET2-Website (www.target2.eu) zur Verfügung steht.

Aus dem Inhalt des Leitfadens leiten sich keinerlei Rechte für TARGET2-Nutzer und sonstige natürliche oder juristische Personen bzw. Rechte hinsichtlich der Abwicklung der Geschäfte ab. Die Zeitangaben im Dokument beziehen sich auf die Ortszeit am Sitz der Europäischen Zentralbank, also mitteleuropäische Zeit (MEZ).

---

1 Nähere Informationen finden sich in Abschnitt 3.

2 Die 3ZB sind die technischen Anbieter der Gemeinschaftsplattform: Banca d’Italia, Banque de France und Deutsche Bundesbank. Bei den 4ZB handelt es sich um die technischen Anbieter der T2S-Plattform: Banca d’Italia, Banque de France, Deutsche Bundesbank und Banco de España. Die nationalen Zentralbanken, die die TIPS-Plattform bereitstellen, sind die Deutsche Bundesbank, die Banco de España, die Banque de France und die Banca d’Italia. Diese Zentralbanken (im Folgenden ebenfalls „4ZB“) sind für die Errichtung und den Betrieb der TIPS-Plattform für das Eurosystem verantwortlich.

Einleitung

1.1 Benutzerhinweise für den TARGET2-Leitfaden

Der Leitfaden dient TARGET2-Nutzern als Referenz für den täglichen Betrieb. Er enthält auch Informationen über andere Dokumente, die für die Nutzer von großem Interesse sein können, und darüber, wo diese zu finden sind.

Abschnitt 2 bietet eine Darstellung von TARGET2, TIPS und TARGET2-Securities, der Leitungs- und technischen Struktur von TARGET2/TIPS, der Organisationsstruktur auf Zentralbankebene, der Kommunikation mit den Nutzern, der Öffnungstage und des Zeitplans an einem Geschäftstag, der über TARGET2 durchgeführten Transaktionen sowie der Abwicklung von Nebensystemen.

Abschnitt 3 erläutert die Teilnahmevoraussetzungen, das Vorgehen zur Beantragung und zur Registrierung (vor allem im Hinblick auf die Stammdatenerhebung), die Zertifizierungstests, die Maßnahmen zur Gewährleistung von Sicherheit und operationeller Zuverlässigkeit, die Arten der Teilnahme, die Kündigung oder Suspendierung von TARGET2-Nutzern sowie die Rechnungsstellung in TARGET2.

In Abschnitt 4 werden die Abläufe der unterschiedlichen Phasen eines normalen Geschäftstags dargelegt. Abschnitt 5, Abschnitt 6, Abschnitt 7, Abschnitt 8 und Abschnitt 9 beschäftigen sich mit den Verfahren, die bei außergewöhnlichen Ereignissen anzuwenden sind. Dabei wählen Abschnitt 5 bis 9 eine chronologische Darstellung der Abläufe während eines Geschäftstags, d. h., zunächst werden die Verfahren zu Beginn des Betriebstags (am Abend des vorherigen Werktags), gefolgt von der Nachtverarbeitung, der Tagverarbeitung und schließlich der Tagesendeverarbeitung, erläutert.

Abschnitt 10 beschreibt die Testanforderungen, die für die Notfallmaßnahmen (Contingency) und für die Vorkehrungen zur Aufrechterhaltung des Geschäftsbetriebs (Business Continuity) gelten. Abschnitt 11 erläutert das Change Management mit Blick auf die jährlichen TARGET2-Releases sowie die Notfalländerungen und sogenannten Hot Fixes. Eine Beschreibung der Verfahren zur TARGET2-Ausgleichsregelung findet sich in Abschnitt 12.

Die Anhänge des Leitfadens enthalten eingehende Informationen zum Wiederherstellungsprozess bei einer interregionalen Ausfallsicherung mit Datenverlust in TARGET2 (Anhang I), einen Störungsbericht (Anhang II), die Selbstzertifizierungserklärung für TARGET2-Teilnehmer (Anhang III) und ein Formular für Änderungsvorschläge (Anhang IV) sowie ein Glossar einschließlich Abkürzungsverzeichnis (Anhang V).

1.2 Weitere wichtige Dokumente

Rechtliche Dokumentation (abrufbar auf der EZB-Website)

- TARGET2-Leitlinie (einschließlich nachfolgender Änderungsleitlinien)

Die TARGET2-Leitlinie (EZB/2012/27) stellt das rechtliche Rahmenwerk für TARGET2 dar, mit dem der TARGET2-Leitfaden in vollem Einklang stehen muss. Sie umfasst in ihrem Geltungsbereich unter anderem die auf Euro lautenden TIPS-Geldkonten (TIPS DCAs) und die auf Euro lautenden T2S-Geldkonten (T2S DCAs). Sonstige T2S-Aspekte werden in der T2S-Leitlinie (EZB/2012/13) abgedeckt.

Die TARGET2-Leitlinie richtet sich an Zentralbanken und basiert, obgleich sie dezentral von jeder Notenbank selbst umzusetzen ist, auf dem Prinzip höchstmöglicher Harmonisierung. In den Anhängen werden die Governance, die Harmonisierten Bedingungen für TARGET2-Teilnehmer und die Innertageskredit-/Selbstbesicherungsfazilitäten abgehandelt.

- Harmonisierte Bedingungen

Jede teilnehmende Zentralbank erlässt Regelungen zur Umsetzung der Harmonisierten Bedingungen für die Teilnahme an TARGET2, der Harmonisierten Bedingungen für die Eröffnung und Führung eines T2S-Geldkontos und der Harmonisierten Bedingungen für die Eröffnung und Führung eines TIPS-Geldkontos,[3] die in der TARGET2-Leitlinie niedergelegt sind und ausschließlich das Verhältnis zwischen der betreffenden nationalen Zentralbank und ihren TARGET2-Nutzern regeln.

Die Harmonisierten Bedingungen, die für die TARGET2-Nutzer gelten, enthalten eine Darstellung von TARGET2/T2S/TIPS und erläutern unter anderem Zugangsvoraussetzungen, Kontenverwaltung, Abwicklung von Zahlungsaufträgen, Rechte und Pflichten der Parteien sowie Finalität und Haftung. In ihren Anhängen bieten sie ferner technische Spezifikationen zur Verarbeitung von Zahlungsaufträgen, Muster für Rechtsfähigkeits- bzw. Ländergutachten sowie das Gebührenverzeichnis und erläutern unter anderem Betriebszeiten, Notfallverfahren, die Modalitäten des Liquiditätspooling und die Ausgleichsregelung.

[3] Harmonisierte Bedingungen für die Eröffnung und Führung eines PM-Kontos in TARGET2 (vgl. Anhang II), Ergänzende und geänderte Harmonisierte Bedingungen für die Eröffnung und Führung eines PM-Kontos in TARGET2 im Rahmen des internetbasierten Zugangs (vgl. Anhang V), Harmonisierte Bedingungen für die Eröffnung und Führung eines T2S-Geldkontos in TARGET2 (vgl. Anhang IIa) und Harmonisierte Bedingungen für die Eröffnung und Führung eines TIPS-Geldkontos in TARGET2 (vgl. Anhang IIb).

Betriebsdokumentation (abrufbar auf der TARGET2-Website)

- Reference and static data registration user guide

Hier finden potenzielle TARGET2-Nutzer alle zum Ausfüllen der Registrierungsformulare erforderliche Informationen.

- User information guide to the TARGET2 pricing
- TIPS pricing

Diese Dokumente enthalten detaillierte Angaben zur Preisgestaltung und Rechnungsstellung in TARGET2 und TIPS.

- Settlement times of ancillary systems

Dieses Dokument enthält vor allem Erläuterungen zu den Verarbeitungszeiten der Nebensysteme.

Spezifikationen (abrufbar auf der TARGET2-Website)

- TARGET2 General Functional Specifications (GFS) und TARGET2 User Detailed Functional Specifications (UDFS)

Diese Dokumente enthalten technische Einzelheiten zur Funktionsweise der Gemeinschaftsplattform (Single Shared Platform – SSP).

- ICM User Handbook

Dieses Handbuch liefert detaillierte Angaben zur Funktionsweise des Informations- und Steuerungsmoduls (Information and Control Module – ICM).

- Benutzerhandbuch zur Public-Key-Zertifizierung für den Internetzugang (User manual internet access for the public key certification service)

In diesem Handbuch werden die Verfahren beschrieben, welche die Banca d'Italia als akkreditierte Zertifizierungsstelle für die Ausstellung und Verwendung elektronischer Zertifikate im Rahmen des internetbasierten Zugangs zu TARGET2 einsetzt. Die Dienstleistung wird im Auftrag des Eurosystems von der Banca d'Italia erbracht.

- SWIFT-Dokumentation

Die SWIFT-Dokumentation liefert Einzelheiten zu den unterschiedlichen SWIFT-Standards, abrufbar auf der SWIFT-Website.

TIPS-Dokumentation (abrufbar auf der TIPS-Website)

- User Detailed Functional Specifications (UDFS)

Dieses Dokument liefert detaillierte technische Angaben zur Funktionsweise von TIPS.

- The Mobile Proxy Lookup User Detailed Functional Specifications (MPL UDFS)

Dieses Dokument liefert detaillierte technische Angaben zur Funktionsweise des MPL-Services.

- Benutzerhandbuch (User Handbook)

Das TIPS-Benutzerhandbuch liefert detaillierte technische Angaben zur Funktionsweise der grafischen Benutzeroberfläche (GUI) von TIPS.

- Dokumentation zum gemeinsamen Referenzdatenmanagement (Common Reference Data Management – CRDM)

Da TIPS als effizienter und leistungsfähiger Service für die Abwicklung von Instant-Zahlungen konzipiert ist, werden innerhalb von TIPS selbst keine Referenzdaten (zur Konfiguration von Teilnehmern, Konten etc.) erstellt und geführt; dies geschieht in einem eigens dafür vorgesehenen Modul für das gemeinsame Referenzdatenmanagement. Dieser Ansatz wurde auch mit Blick auf eine Integration der TIPS-Referenzdaten in die gemeinsamen Komponenten der künftigen TARGET Services gewählt. Die Dokumentation zum gemeinsamen Referenzdatenmanagement ist in folgenden Dokumenten enthalten: „T2 User Detailed Functional Specifications – Common Reference Data Management (CRDM)“ sowie „T2 User Handbook – Common Reference Data Management (CRDM)“. Darin werden die technischen Einzelheiten des CRDM beschrieben, das bei TIPS zur Anwendung kommt, und es wird detailliert auf die Nutzung des CRDM über die entsprechende grafische Benutzeroberfläche eingegangen.

- Dokumentation zum Eurosystem Single Market Infrastructure Gateway (ESMIG)

Der Zugang zu TIPS über einen TIPS-Netzwerkdienstleister erfolgt über das ESMIG. Über das ESMIG werden Authentifizierungs- und Autorisierungsdienste sowie Funktionen für die Nachrichtenverwaltung bereitgestellt. Die Dokumente „T2 User Detailed Functional Specifications – Common Reference Data Management (CRDM)“ und „T2 User Handbook – Common Reference Data Management (CRDM)“ liefern detaillierte technische Angaben zur Funktionsweise des TIPS ESMIG.

- Connectivity-Dossier

Das Connectivity-Dossier für TIPS besteht aus dem Connectivity Guide, in dem der Verbindungsprozess zu TIPS über einen TIPS-Netzwerkdienstleister beschrieben wird, und den technischen Voraussetzungen für die TIPS-Anbindung (Connectivity Technical Requirements). In den Connectivity Technical Requirements werden die technischen und operativen Anforderungen dargelegt,

die ein Netzwerkdienstleister erfüllen muss, um den TIPS-Akteuren die notwendigen Konnektivitätsdienste bereitstellen zu können.

- Dokumente zu TARGET2-Securities

Von besonderer Bedeutung sind die T2S User Detailed Functional Specifications (UDFS), das T2S User Handbook (UHB) und das User Requirements Document (URD), die auf der T2S-Website veröffentlicht sind. Die oben genannten Dokumente stehen auf der TARGET2-Website der Deutschen Bundesbank (www.bundesbank.de) zur Verfügung.

Außerdem sind dort weitere Informationen zu bestimmten nationalen Besonderheiten und Verfahren veröffentlicht.

2 Allgemeines

2.1 Was ist TARGET2?

TARGET2 (Trans-European Automated Real-time Gross settlement Express Transfer, zweite Systemgeneration) bezeichnet das Individualzahlungssystem des Eurosystems. Es wurde entwickelt, um die Festlegung und Durchführung der Geldpolitik im Euroraum und die Förderung einer reibungslosen Funktionsweise der Zahlungssysteme im Rahmen der Zielsetzung des Eurosystems zu unterstützen und damit zur Integration und Stabilität des Euro-Geldmarkts beizutragen.

Technisch wird TARGET2 auf einer einzigen Gemeinschaftsplattform (SSP)[4] betrieben, über die allen Nutzern dasselbe Leistungsspektrum zur Verfügung steht. TARGET2 ist so ausgelegt und konstruiert, dass es höchste Ansprüche an die Systemstabilität und -zuverlässigkeit erfüllt und grenzüberschreitende Euro-Zahlungen ebenso reibungslos wie inländische Zahlungen verarbeitet. TARGET2 wickelt ausschließlich auf Euro lautende Zahlungsaufträge – vor allem Großzahlungen wie z. B. Zahlungen im Zusammenhang mit Devisen-, Wertpapier- und Geldmarktgeschäften – ab, die kostengünstig, äußerst sicher und in sehr kurzer Verarbeitungszeit ausgeführt werden.

Es handelt sich um ein Echtzeit-Bruttosystem (Real-Time Gross Settlement System – RTGS), bei dem Zahlungen individuell abwickelt werden: Zahlungsaufträge werden in einem kontinuierlichen automatisierten Verfahren einzeln verarbeitet. Damit gewährleistet TARGET2 eine umgehende Abwicklung mit sofortiger Finalität aller Zahlungen, vorausgesetzt der Zahlungspflichtige verfügt auf seinem Konto bei der Zentralbank über ausreichendes Guthaben bzw. hinreichende Überziehungsfazilitäten,[5] wobei für TARGET2-Zahlungen keine Mindestbeträge vorgeschrieben sind.

Zudem beinhaltet TARGET2 **auf Euro lautende Geldkonten**. Dazu zählen die TIPS-Geldkonten, die technisch auf der TIPS-Plattform angesiedelt sind, sowie die T2S-Geldkonten, die technisch auf der T2S-Plattform angesiedelt sind (siehe Zusatzinformationen unten).

Jede Einrichtung, die mindestens ein PM-Konto und/oder ein TIPS-Geldkonto und/oder ein T2S-Geldkonto bei einer Zentralbank des Eurosystems oder einer angeschlossenen Zentralbank hält, ist ein TARGET2-Teilnehmer.

TARGET2-Nutzer bezieht sich auf TARGET2-Teilnehmer und Nebensysteme.

---

4 SSP (Single Shared Platform) bezeichnet die technische Plattform, auf der die TARGET2-bezogenen Dienstleistungen bereitgestellt werden. Dienste in Zusammenhang mit TARGET2-Securities werden über die T2S-Plattform erbracht.

5 Mit einigen Ausnahmen wie z. B. gespeicherten Zahlungsaufträgen (warehoused payments) oder Zahlungen an einen suspendierten Teilnehmer.

2.2 Was ist TARGET Instant Payment Settlement (TIPS)?

TIPS wurde im Auftrag des Eurosystems von den Anbieter-NZBen der TIPS-Plattform (nachfolgend als „4ZB“ bezeichnet) entwickelt und wird von diesen betrieben. Dabei handelt es sich um folgende Zentralbanken: Banca d’Italia, Deutsche Bundesbank, Banque de France und Banco de España.

TIPS ist ein harmonisierter und standardisierter paneuropäischer Service zur sofortigen Abwicklung von Zahlungen in Zentralbankgeld, der über eine hohe Kapazität verfügt und an 365 Tagen im Jahr rund um die Uhr zur Verfügung steht. Hierzu ermöglicht TIPS die Kommunikation mit der zentralisierten Abwicklungskomponente und stellt Dienste zur Authentifizierung sowie zur sicheren Übermittlung von Nachrichten an die bzw. von der zentralisierten Abwicklungskomponente bereit. In TIPS gibt es zwei Arten von Konten: Geldkonten und technische Nebensystem-Konten (TIPS ASTAs). Die Inhaber von TIPS-Geldkonten verbinden sich über einen TIPS-Netzwerkdienstleister (TIPS NSP) mit der TIPS-Plattform, um Instant-Zahlungen, Liquiditätsübertragungen von TIPS-Geldkonten auf PM-Konten, Liquiditätsübertragungen zwischen TIPS-Geldkonten und TIPS ASTAs und positive Rückruf-Antworten senden und empfangen zu können sowie um zahlungsrelevante Nachrichten austauschen zu können, die dem ISO 20022-Standard entsprechen und mit dem SEPA Instant Credit Transfer (SCT^{Inst}) Scheme im Einklang stehen. Diese Instant-Zahlungen werden über bei der jeweiligen Zentralbank unterhaltene TIPS-Geldkonten abgewickelt. Inhaber solcher Konten haben zudem die technische Möglichkeit, abgewickelte Instant-Zahlungen zurückzurufen oder Nachforschungen zu Instant-Zahlungen, die an TIPS übermittelt werden, einzuleiten. Ferner können auch einreichende Parteien, die im Auftrag von TIPS-Geldkontoinhabern handeln, die genannten Aktionen durchführen.

TIPS wurde für die Bereitstellung von Dienstleistungen in verschiedenen Währungen konzipiert. Der TARGET2-Leitfaden trägt diesem Aspekt Rechnung und beschreibt die entsprechenden Verfahren aus Sicht des Systems unabhängig von der jeweiligen Währung. Alle **für den Euro** relevanten Verfahren werden im Leitfaden genau erläutert. Nur für den Euro geltende Verfahren werden dabei explizit als solche kenntlich gemacht. **Bei anderen Währungen** sind die Zentralbanken, die diese Währung in TARGET bereitstellen, für die entsprechenden operativen Verfahren verantwortlich, die im vorliegenden Dokument nicht dargestellt werden. Hierbei übernimmt das RTGS-System der betreffenden Zentralbank dieselbe Rolle wie TARGET2 für den Euro. Dies bedeutet, dass Liquiditätsübertragungen in einer anderen Währung als dem Euro von einem Konto im RTGS-System der betreffenden Zentralbank auf ein TIPS-Geldkonto getätigt werden und umgekehrt. Der Zeitrahmen für die Liquiditätsübertragungen wird von der Zentralbank, die eine andere Währung als den Euro anbietet, festgelegt und kann daher vom Zeitrahmen für Liquiditätsübertragungen in Euro abweichen. Das RTGS-System löst auch den Wechsel des Geschäftstags in TIPS für eine andere Währung als den Euro aus. Der Geschäftstag (Zeitplan) kann daher von demjenigen für den Euro abweichen.

Mit dem Release 4.0 im November 2021 wurden auch automatisierte Clearinghäuser (ACHs) in TIPS eingebunden und können über technische Nebensystem-Konten (TIPS ASTAs) an TIPS teilnehmen. Diese Konten werden in TIPS verwendet, um a) die Mittel, die zur Gewährleistung einer sofortigen finalen Abwicklung benötigt werden, bereitzustellen bzw. abzuziehen, und b) um Instant-Zahlungen und Rückrufantworten abzuwickeln. Instant-Zahlungen und Rückrufantworten können zwischen einem TIPS ASTA und einem TIPS-Geldkonto oder zwischen zwei TIPS ASTAs erfolgen. Darüber hinaus können Liquiditätsübertragungen zwischen TIPS-Geldkonten und TIPS ASTAs durchgeführt werden.

Die Verbindung von TARGET2 und TIPS basiert auf einem Application-to-Application-Ansatz (A2A-Ansatz), der durch die TIPS-Schnittstelle gewährleistet wird. Dadurch wird vor allem der Liquiditätsaustausch zwischen PM-Konten und TIPS-Geldkonten ermöglicht.

Außerdem wurde im Rahmen des TIPS-Release 3.0 vom November 2020 der Mobile-Proxy-Lookup-Service (MPL-Service) in TIPS entwickelt.[6] Dabei handelt es sich um einen Dienst, der IBANs Rufnummern zuweist, sodass die Endnutzer (d. h. die Kunden von TIPS-Akteuren) bei Zahlungsanweisungen an ihren Zahlungsdienstleister (PSP) den Zahlungsempfänger anhand der Rufnummer statt der IBAN identifizieren können[7]

Wichtige Aspekte im Zusammenhang mit TIPS im Hinblick auf den Euro:

1) Wenngleich die in Euro denominierten TIPS-Geldkonten technisch auf der TIPS-Plattform angesiedelt sind, fallen sie unter den rechtlichen und operativen Rahmen von TARGET2. Somit werden rechtliche Fragen im Zusammenhang mit den TIPS-Geldkonten in der TARGET2-Leitlinie behandelt und die operativen Verfahren in Bezug auf die TIPS-Geldkonten vom operativen Rahmenwerk für TARGET2 abgedeckt, das vor allem aus dem TARGET2 Manual of Procedures (TARGET2 MOP) und dem Leitfaden für TARGET2-Nutzer besteht.

2) Vorbehaltlich der Erfüllung der einschlägigen Zulassungsvoraussetzungen kann eine Institution bei jeder Zentralbank, die an TARGET2 teilnimmt, ein TIPS-Geldkonto in Euro eröffnen (siehe Punkt 6 zum RM-/SF-Link). Die Zulassungskriterien für die Eröffnung eines TIPS-Geldkontos entsprechen – gemäß der TARGET2-Leitlinie – jenen für die Eröffnung eines PM-Kontos.

6 Einige Elemente des MPL-Services (z. B. Frontend-Software) waren bereits in der TIPS-Version 2.5 vom Juni 2020 umgesetzt. Komplett bereitgestellt wurde der MPL-Service allerdings erst im November 2020.

7 Da der MPL-Service derzeit noch nicht intensiv genutzt wird, gibt es für ihn vorläufig keine besonderen Vereinbarungen. Die Kritikalität des Services und die Notwendigkeit, spezifische operative Verfahren zu entwickeln, werden zu einem späteren Zeitpunkt überprüft.

3) Für die Liquiditätssteuerung ist es notwendig, dass jedes TIPS-Geldkonto mit einem einzigen PM-Konto, dem sog. verknüpften PM-Konto, über eine Liquiditätssteuerungsverbindung (LM-Link) verbunden ist. Ein PM-Konto kann mit maximal zehn TIPS-Geldkonten verbunden sein. Der LM-Link kann zwischen einem TIPS-Geldkonto und einem PM-Konto, die jeweils bei einer beliebigen an TARGET2 teilnehmenden Zentralbank eröffnet wurden, eingerichtet werden (somit sind auch grenzüberschreitende Verbindungen möglich). Der Inhaber eines TIPS-Geldkontos und der Inhaber des damit verknüpften PM-Kontos können unterschiedliche Institutionen sein. Die vertragliche Vereinbarung zwischen dem TIPS-Geldkontoinhaber und dem PM-Kontoinhaber liegt in deren eigener Verantwortung.

4) Sämtliche TIPS-Gebühren, die aus den (per LM-Links) verbundenen TIPS-Geldkonten erwachsen, werden von dem verknüpften PM-Konto eingezogen.

5) Die TIPS-Geldkonten können zu keinem Zeitpunkt einen Negativsaldo aufweisen. Da TIPS ein kontinuierlich zur Verfügung stehender Dienst ist, ist es möglich, dass außerhalb der TARGET2-Geschäftszeiten und -tage auf den TIPS-Geldkonten noch Liquidität vorhanden ist.

6) Zur Berechnung der Mindestreserven, zur Verzinsung von Übernachtguthaben und zur automatisierten Inanspruchnahme der Spitzenrefinanzierungsfazilität (Übernachtkredit) muss der TIPS-Geldkontoinhaber sein TIPS-Geldkonto über den RM-/SF-Link an ein PM-/Heimatkonto[8] anbinden, das er bei derselben Zentralbank hält (d. h., der PM-Kontoinhaber und der TIPS-Geldkontoinhaber müssen ein und dieselbe juristische Person sein). Ein PM-/Heimatkonto kann über den RM-/SF-Link mit mehreren TIPS-Geldkonten verlinkt sein, aber ein TIPS-Geldkonto über den RM-/SF-Link nur mit einem einzigen PM-/Heimatkonto. In Bezug auf den RM-/SF-Link gilt Folgendes[9]:

a) Der Saldo des TIPS-Geldkontos wird auf die Erfüllung der Mindestreservepflicht und die Überschussreserven angerechnet.
b) Die Verbuchung der für die Übernachtguthaben auf TIPS-Geldkonten entstehenden Zinsen erfolgt auf dem PM-/Heimatkonto, das über einen RM-/SF-Link verbunden ist.
c) Die automatisierte Inanspruchnahme der Spitzenrefinanzierungsfazilität (Übernachtkredit) durch den Inhaber des PM-Kontos wird durch den Saldo/die Salden auf dessen TIPS-Geldkonto/-Geldkonten verringert.

[8] Der Link kann auch bei Teilnehmern mit internetbasiertem Zugang eingesetzt werden.
[9] Eine ausführliche Beschreibung der Funktionsweise von RM-/SF-Links findet sich in Abschnitt 3.5.3.3.

d) NZBen, die das RM- und/oder SF-Modul nicht verwenden, müssen sicherstellen, dass die Mindestreserveverwaltung, die Verzinsung (zur Verwaltung der Überschussliquidität) und die Verringerung der automatisierten Inanspruchnahme der Spitzenrefinanzierungsfazilität (Übernachtkredit) außerhalb von TARGET2 ordnungsgemäß funktionieren.

Das TIPS-Geldkonto kann wie folgt verwaltet werden:

a) über die TIPS-Plattform im U2A-Modus, A2A-Modus oder beidem und/oder

b) über die TARGET2-Liquiditätssteuerungsfunktionen für TIPS.

7) Die Zentralbanken sind verantwortlich für die Geschäftsbeziehung mit ihren TIPS-Geldkontoinhabern und sollten sich um alle Vorfälle, Fragen oder Probleme, die von diesen aufgeworfen werden, kümmern. Bei Konnektivitätsproblemen kann ein TIPS-Geldkontoinhaber den TIPS Service Desk aber auch direkt kontaktieren (siehe Abschnitt 2.5).

2.3 Was ist TARGET2-Securities?

Eine weitere wichtige Infrastruktur, die Abhängigkeiten mit TARGET2 hat, ist TARGET2-Securities (T2S). Das Eurosystem stellt T2S-Dienstleistungen über die von den 4ZB – der Deutschen Bundesbank, der Banque de France, der Banca d'Italia und der Banco de España – errichteten und betriebenen T2S-Plattform bereit.

T2S ermöglicht Zentralverwahrern (Central Securities Depositories – CSDs) national wie auch grenzüberschreitend eine harmonisierte und standardisierte Abwicklung von Wertpapiertransaktionen. Mit T2S gilt überall dort, wo T2S in Betrieb ist, ein einheitlicher Regel-, Normen- und Gebührenkatalog für alle Zentralverwahrer, die zur Abwicklung ihrer Wertpapiertransaktionen die T2S-Plattform nutzen. Auch die geldliche Verrechnung erfolgt in Zentralbankgeld und unterliegt einheitlichen Regeln und Standards.

T2S integriert die von den Marktteilnehmern bei einem bzw. mehreren Zentralverwahrern unterhaltenen Wertpapierkonten und die bei den jeweiligen Zentralbanken unterhaltenen T2S-Geldkonten auf einer gemeinsamen technischen Plattform.

T2S ist als Multiwährungssystem konzipiert. Der Euro ist die erste Währung, in der Wertpapiertransaktionen auf der T2S-Plattform abgewickelt werden. Somit sind T2S und TARGET2 im Hinblick auf die Euro-Liquiditätssteuerung eng miteinander verzahnt. Die Verbindung von TARGET2 und T2S basiert auf einem Application-to-Application-Ansatz (A2A-Ansatz), der durch die T2S-Schnittstelle (T2S Interface – T2SI) gewährleistet wird.

Der vorliegende Leitfaden befasst sich ausschließlich mit auf Euro lautenden Transaktionen und Konten.

Wichtige Aspekte im Zusammenhang mit T2S:

- Wenngleich die in Euro denominierten T2S-Geldkonten technisch auf der T2S-Plattform angesiedelt sind, fallen sie unter den rechtlichen Rahmen von TARGET2. Somit werden rechtliche Fragen in Zusammenhang mit den T2S-Geldkonten in der TARGET2-Leitlinie behandelt und die operativen Verfahren in Bezug auf die T2S-Geldkonten vom Leitfaden abgedeckt.
- Im Hinblick auf die Liquidität sind die Gemeinschaftsplattform (Single Shared Platform – SSP) von TARGET2 und die T2S-Plattform über sogenannte Zwischenkonten miteinander verknüpft, die den Liquiditätsaustausch zwischen PM-Konten und T2S-Geldkonten ermöglichen.
- Der Zugriff des T2S-Geldkontoinhabers oder des in dessen Namen handelnden Inhabers des PM-Hauptkontos (Main PM Account) auf das T2S-Geldkonto erfolgt a) über eine direkte Verbindung zur T2S-Plattform durch einen lizenzierten Anbieter von Mehrwertnetzwerkdiensten (Value-Added Network Service Providers – VA-NSP) für T2S (direkt angeschlossene T2S-Geldkontoinhaber) und/oder b) über einen indirekten Anschluss durch die TARGET2-Zusatzleistungen (Value-added Services – VAS) für T2S (indirekt angeschlossene T2S-Geldkontoinhaber).
- Vorbehaltlich der Erfüllung der einschlägigen Zulassungsvoraussetzungen kann eine Einrichtung bei jeder Zentralbank, die an TARGET2 teilnimmt, ein T2S-Geldkonto in Euro eröffnen. Diese Regel gilt unabhängig davon, in welcher Migrationswelle der nationale Zentralverwahrer zu T2S überwechselt. Die Zulassungskriterien für die Eröffnung eines T2S-Geldkontos entsprechen – gemäß der TARGET2-Leitlinie – jenen für die Eröffnung eines PM-Kontos.
- Jedes T2S-Geldkonto muss mit einem einzigen PM-Konto, dem sog. PM-Hauptkonto[10], verlinkt sein. Allerdings ist es zulässig, dass mehrere T2S-Geldkonten mit ein- und demselben PM-(Haupt)konto verknüpft sind. Das PM-Hauptkonto kann in den Büchern derselben Zentralbank wie das T2S-Geldkonto eröffnet werden, was allerdings nicht zwingend ist.
- Der T2S-Geldkontoinhaber und der PM-Hauptkontoinhaber können unterschiedliche Einrichtungen sein (d. h., der T2S-Geldkontoinhaber braucht kein PM-Konto zu unterhalten, selbst wenn das T2S-Geldkonto mit einem PM-Konto verknüpft sein muss). Die vertragliche

10 Externes RTGS-Konto, das mit dem T2S-Geldkonto unter der GUI-Bildschirmanzeige „Static Data > Dedicated Cash Account“ verlinkt ist.

Vereinbarung zwischen dem T2S-Geldkontoinhaber und dem PM-Kontoinhaber liegt in deren eigener Verantwortung.

- Der Inhaber des PM-Hauptkontos ist für die Zahlung der Gebühren der im Zusammenhang mit dem angeschlossenen T2S-Geldkonto erbrachten T2S-Dienstleistungen sowie für etwaige Strafentgelte im Falle einer Umbuchung von Sicherheiten (relocation of collateral) verantwortlich.
- Die T2S-Geldkonten können zu keinem Zeitpunkt einen Negativsaldo aufweisen (eine Ausnahme bilden die von einer Zentralbank selbst unterhaltenen T2S-Geldkonten). Außerdem muss der Saldo des T2S-Geldkontos am Tagesende auf null stehen. Realisiert wird dies durch den automatisierten „Cash Sweep“, der nach Annahmeschluss für eingehende Liquiditätsübertragungen (um 17.45 Uhr) etwaige auf dem T2S-Geldkonto verbleibende Liquidität automatisch auf das PM-Hauptkonto transferiert. Dennoch wird T2S-Geldkontoinhabern empfohlen, zur Wertpapierabwicklung nicht mehr benötigte Liquidität zu einem früheren Zeitpunkt von den T2S-Geldkonten auf die PM-Konten zu transferieren. Sollte der höchst unwahrscheinliche Fall eintreten, dass die auf T2S-Geldkonten gehaltene Liquidität aufgrund einer technischen Störung nicht auf die PM-Konten zurückgebucht werden kann, verbleibt die bei Tagesabschluss von T2S auf den T2S-Geldkonten vorhandene Liquidität über Nacht dort. Zu Beginn des nächsten Geschäftstags weisen die T2S-Geldkonten den Tagesabschlusssaldo des vorherigen Geschäftstags aus.
- T2S-Geldkontoinhaber können sich im Wege der Selbstbesicherung refinanzieren, d. h. durch einen von der Zentralbank gewährten Innertageskredit, der in Anspruch genommen wird, wenn die Liquidität auf den T2S-Geldkonten zur Abwicklung von Wertpapiertransaktionen nicht ausreicht. Dabei wird der Innertageskredit entweder mit Sicherheiten unterlegt, die vom T2S-Geldkontoinhaber erworben werden („collateral on flow“), oder mit Sicherheiten, die vom T2S-Geldkontoinhaber bereits gehalten werden und für die Selbstbesicherung bestimmt und entsprechend gekennzeichnet sind („collateral on stock“).
- Um die Möglichkeit der Zentralbank-Selbstbesicherung nutzen zu können, muss der T2S-Geldkontoinhaber ein PM-Konto mit Zugang zu Innertageskredit bei derselben Zentralbank unterhalten, bei der auch das T2S-Geldkonto geführt wird.
- Inhaber von T2S-Geldkonten können ihren Kunden (z. B. Wertpapierkontoinhabern) Kredite einräumen, die automatisch durch die Funktion „Client Auto-Collateralisation“ in T2S besichert werden. Die Client Auto-Collateralisation (Bereitstellung von Liquidität für Kunden) wird in Anspruch genommen, wenn das External Guarantee Limit des Kunden ausgeschöpft ist und

Wertpapiertransaktionen nicht mehr abgewickelt werden können; dabei könnten entweder die Sicherheiten verwendet werden, die vom Kunden erworben werden („collateral on flow“), oder vom Kunden bereits gehaltene Wertpapiere, die für die Selbstbesicherung bestimmt und als solche gekennzeichnet sind („collateral on stock“). Falls ein T2S-Geldkontoinhaber Client Auto-Collateralisation anbietet, muss er eine Liste mit Wertpapieren erstellen, die als Sicherheiten akzeptiert werden („list of eligible securities“), sowie die entsprechenden Bewertungen (d. h. jene Preise, die T2S zur Bewertung der Sicherheitenpositionen verwenden kann). Nähere Informationen dazu finden sich in Kasten 2 im Abschnitt 4.1.

- Zentralbanken sind verantwortlich für die Geschäftsbeziehung mit ihren Nutzern und sollten sich um alle Vorfälle, Fragen oder Probleme, die von diesen aufgeworfen werden, kümmern. Bei Konnektivitätsproblemen kann ein T2S-Geldkontoinhaber mit direkter T2S-Anbindung den T2S Service Desk aber auch direkt kontaktieren und umgekehrt (siehe Abschnitt 2.5).
- T2S ist kein Nebensystem und besitzt keinen Systemstatus (da T2S unter die rechtliche Abgrenzung von TARGET2 fällt, wird die Finalität im TARGET2-Leitfaden behandelt). Aus diesem Grund, aber auch wegen der engen Verknüpfung mit TARGET2, unterscheidet der Leitfaden zwischen den T2S-relevanten Bestimmungen und den Bestimmungen, die für das Nebensystem relevant sind.

2.3.1 Die Rolle der Zentralbanken im Kontext von TARGET2-Securities

Im Eurosystem lassen sich vier Rollen[11] unterscheiden, die die Zentralbanken im Rahmen von TARGET2-Securities ausfüllen:

- Rolle 1: **System-Entity** oder **Bank der Banken** – insbesondere bei der Geschäftsbeziehung mit den Banken im geldbezogenen Kontext und was die Eröffnung von T2S-Geldkonten betrifft,
- Rolle 2: **TARGET2-Systemeigner**, Status des Market Infrastructure Board (MIB) in Verbindung mit der Zentralbankrolle als an TARGET2 teilnehmende Zentralbank. Was die Leitung bzw. Governance betrifft, so verfügt der EZB-Rat (sog. Ebene 1 oder E1) über die oberste Zuständigkeit für TARGET2, während die Zentralbanken des Eurosystems (Ebene 2 oder E2), die durch das MIB vertreten werden, als Kollektiv eine subsidiäre Kompetenz in von der Ebene 1 delegierten Fragen besitzen,
- Rolle 3: Als **Sicherheitenverwalter** haben die Zentralbanken die Zuständigkeit dafür, wie im Eurosystem mit der Besicherung der geldpolitischen Geschäfte, der Innertageskredite und mit den

[11] Partielle Überlappungen der unterschiedlichen Rollen sind möglich. Die Rolle der Zentralbanken als Betreiber von Wertpapierabwicklungssystemen/Zentralverwahrer (z. B. in Belgien und Griechenland) bleibt unberücksichtigt

Selbstbesicherungsfazilitäten zu verfahren ist,

- Rolle 4: **Settlement Agent** – betrifft insbesondere die Abwicklung der eigenen Geschäfte in der Funktion als Kunde eines Zentralverwahrers (CSD-Teilnehmer).

Im vorliegenden Dokument werden die Rollen 1 und 2 behandelt, da sie für den Leitfaden von besonderer Bedeutung sind (in Abbildung 1 rot umrahmt). Auf Rolle 3 und Rolle 4 wird hier nicht näher eingegangen.

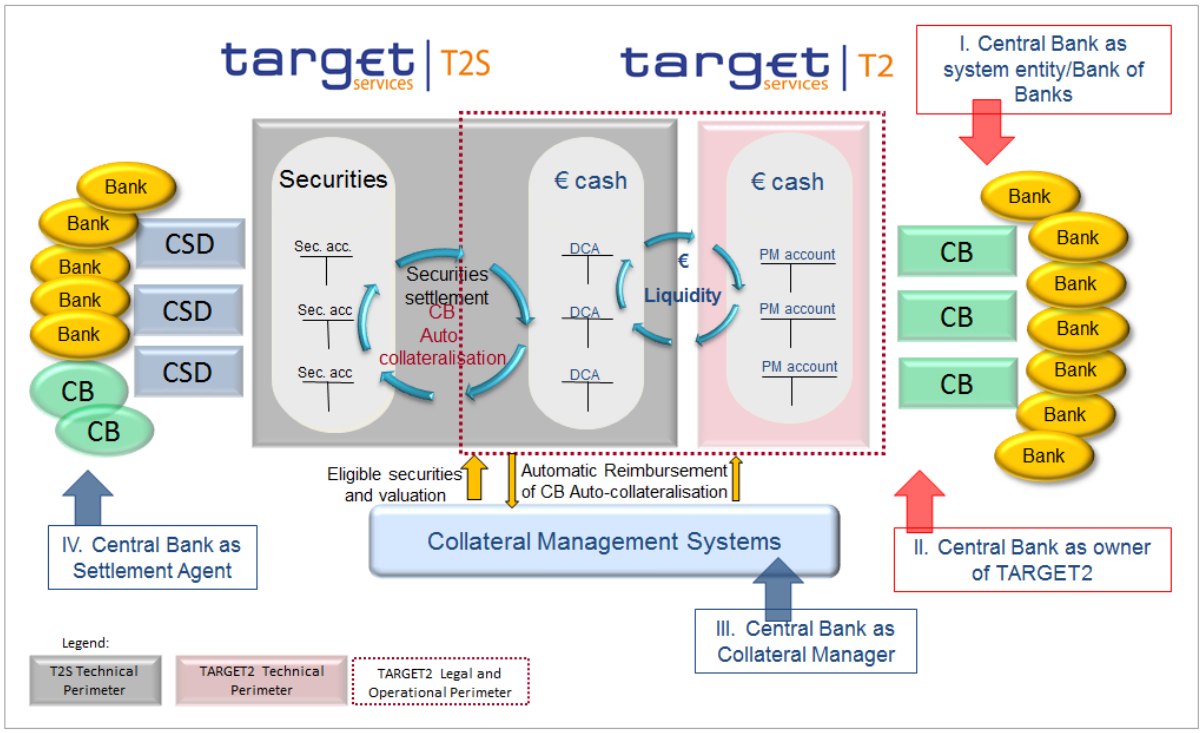


Abbildung 1: Die vier Rollen der Zentralbanken im Rahmen von T2S

2.3.2 Die Rollen der Banken im Kontext von TARGET2-Securities

Eine Bank kann im Kontext von T2S die folgenden Rollen einnehmen:

- T2S-Geldkontoinhaber, d. h. Inhaber eines oder mehrerer T2S-Geldkonten,
- CSD-Teilnehmer, d. h. Inhaber von Wertpapierkonten bei einem oder mehreren Zentralverwahrern,
- Liquiditätsbereitsteller, d. h. Institut, das die Abwicklung von Wertpapiertransaktionen seiner

Kunden (CSD-Teilnehmer) auf seinem T2S-Geldkonto ermöglicht, oder das über sein PM-Konto Liquidität für ein T2S-Geldkonto eines anderen Instituts bereitstellt,

- Kreditgeber, d. h. Institut, das Innertageskredite über die Client Auto-Collateralisation an seine Kunden (CSD-Teilnehmer) ausreicht.

2.4 TARGET2-Struktur

2.4.1 Leitungsstruktur (Governance) von TARGET2 und TIPS

Das TARGET2-Management beruht auf einer dreistufigen Leitungsstruktur. Die Aufgaben dabei werden vom EZB-Rat (Ebene 1), den Zentralbanken des Eurosystems (Ebene 2) und den Anbieter-Zentralbanken der Gemeinschaftsplattform/TIPS-Plattform (Ebene 3) wahrgenommen. Der **EZB-Rat** ist für die allgemeine Leitung von TARGET2 zuständig. Die Aufgaben der Ebene 1 fallen in die ausschließliche Zuständigkeit des EZB-Rats. Das Market Infrastructure Board (MIB) unterstützt den EZB-Rat als beratendes Gremium in allen Angelegenheiten, die Bezug zu TARGET2 haben. Neben seiner beratenden Funktion nimmt das MIB die Aufgaben der Ebene 2 wahr. Die **Anbieter-Zentralbanken** der Gemeinschaftsplattform/TIPS-Plattform (Ebene 3) treffen Entscheidungen zum täglichen Betrieb der SSP auf der Grundlage eines vorab definierten Service Level Agreements.

Ebene 1 EZB-Rat	Ebene 2 Technisches und operationales Leitungsgremium	Ebene 3 Anbieter-NZBen der SSP und der TIPS-Plattform (4ZB)
- Steuerung im Fall ernster Krisensituationen - Genehmigung der Einrichtung und des Betriebs des TARGET2-Simulators - Benennung der Zertifizierungsstellen für den internetbasierten Zugang - Festlegung der Sicherheitspolitik, -anforderungen und -kontrollen für die SSP und die TIPS-Plattform - Festlegung der Grundsätze für die Sicherheit der Zertifikate für den internetbasierten Zugang	- Management im Hinblick auf die Zuständigkeiten des Systemeigners (auch in Krisensituationen) - Kontakt mit Nutzern auf europäischer Ebene (unter Beachtung der ausschließlichen Verantwortung der Zentralbanken für die Geschäftsbeziehung zu ihren TARGET2-Nutzern) und Überwachung der täglichen Nutzeraktivitäten aus geschäftspolitischer Sicht (Aufgabe der Zentralbanken) - Überwachung der Geschäftsentwicklungen - Budgetierung, Finanzierung, Rechnungsstellung (Aufgabe der Zentralbanken) und sonstige administrativen Aufgaben	- Betrieb des Systems auf der Grundlage der in der TARGET2-Leitlinie genannten Vereinbarung

Tabelle 1: TARGET2-Leitungsstruktur

2.4.2 Technische Struktur

Was die technische Struktur betrifft, so weist TARGET2 folgende Merkmale auf:

- die Gemeinschaftsplattform (Single Shared Platform – SSP) mit dem Zahlungsabwicklungs- und Kontoführungssystem (Payment and Accounting Processing Services Systems – PAPSS) und dem Customer Related Services System (CRSS)
- das PAPSS mit dem Zahlungsmodul (Payments Module – PM), dem Modul für die ständigen

Fazilitäten (Standing Facilities Module – SF), dem Modul für die Mindestreserveverwaltung (Reserve Management Module – RM), dem Heimatkontomodul (Home Accounting Module – HAM), dem Stammdatenmodul (Static Data Module – SD), der Enhanced Contingency Solution (ECONS I) und dem Informations- und Steuerungsmodul (Information and Control Module – ICM)

- die ausschließlich für die Zentralbanken bestimmten Kundenbetreuungssysteme (CRSS-Hauptmeldefunktionen und CRISP – Consumption Report and Invoicing Support Process)
- die T2S-Schnittstelle (T2SI), die TARGET2 mit T2S verbindet. Die gemeinsame Systemschnittstelle basiert auf dem internen 4ZB-Netzwerk und nutzt den in den T2S-Anforderungen festgelegten XML-Nachrichtenstandard
- die Verbindung von SSP und TIPS-Plattform basiert auf einem Application-to-Application-Ansatz (A2A-Ansatz), der durch die TIPS-Schnittstelle (TIPSI) gewährleistet wird. Dadurch wird vor allem der Liquiditätsaustausch zwischen PM-Konten, TIPS ASTAs und TIPS-Geldkonten ermöglicht
- die Zentralbanken mit einem proprietären Heimatkonto (PHA), Mindestreserveverwaltung und Innertageskredit
- die Kreditinstitute und sonstigen in TARGET2 abwickelnden Einrichtungen (außer Nebensysteme), die über SWIFT oder Internet an die Gemeinschaftsplattform und/oder über einen TIPS-Netzwerkdienstleister (TIPS Network Service Provider –TIPS NSP) an die TIPS-Plattform und/oder über die lizenzierten Anbieter von Mehrwertnetzwerkdiensten (VA-NSP) an die T2S-Plattform angeschlossen sind
- die Nebensysteme, die an die SSP und an TIPS angebunden sind.

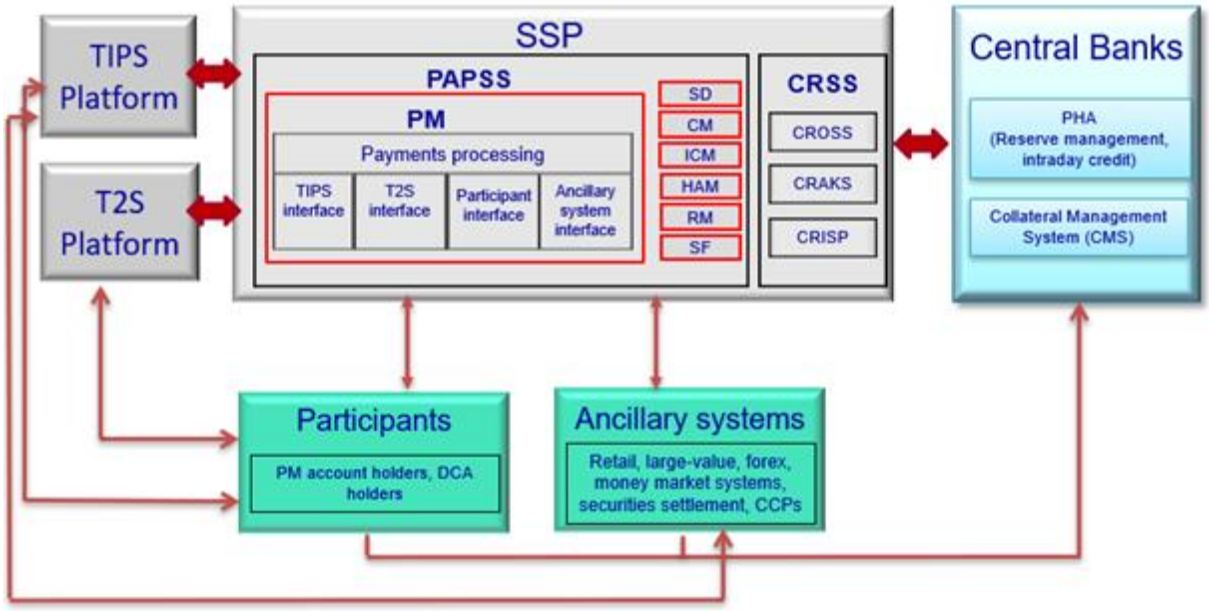


Abbildung 2: TARGET2-Struktur

2.4.3 Organisationsstruktur auf der Ebene der Zentralbanken

2.4.3.1 National Service Desks

Jede Zentralbank verfügt über einen **National Service Desk**, der als Ansprechpartner für die jeweiligen TARGET2-Nutzer fungiert. Im TARGET2-Rahmenwerk wird der National Service Desk durch die **Settlement-Manager** vertreten, die für die Verwaltung des täglichen Geschäftsbetriebs verantwortlich sind. Alle Settlement-Manager sind durch ein voreingestelltes Telekonferenzsystem („Settlement Managers Forum“) miteinander verbunden. An ihren Telefonkonferenzen nehmen die Settlement-Manager der Zentralbanken, die SSP-/TIPS-Service-Manager und der TARGET-Services-Koordinator teil.

Jede Zentralbank hat darüber hinaus einen **Krisenmanager**, der vom jeweiligen Settlement-Manager informiert und bei Eskalation eines Problems hinzugezogen wird. Die Krisenmanager sind ebenfalls über ein voreingestelltes Telekonferenzsystem miteinander verbunden. An den Telefonkonferenzen der Krisenmanager nehmen die Krisenmanager der Zentralbanken, die SSP-/TIPS-Krisenmanager und die EZB-Krisenmanager teil.

Die Settlement-Manager und die Krisenmanager der einzelnen Zentralbanken nehmen auch an den entsprechenden T2S-Telefonkonferenzen teil.

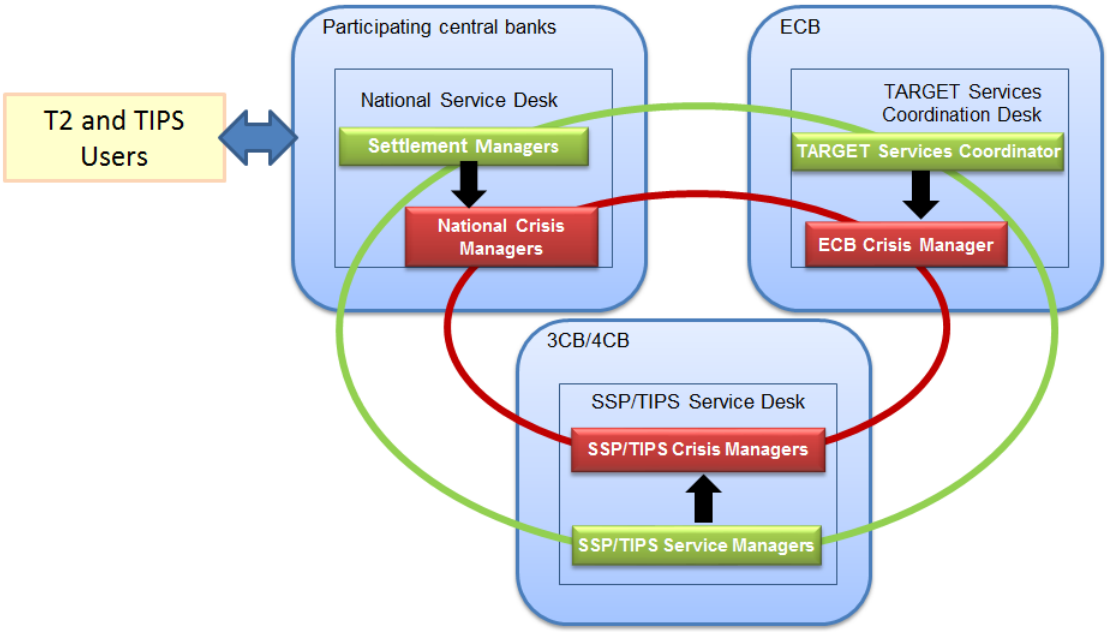


Abbildung 3: Überblick über die TARGET2-Beteiligten

2.4.3.1.1 Zuständigkeiten der National Service Desks

Da jede Zentralbank in vollem Umfang für die Geschäftsbeziehungen mit „ihren" Nutzern verantwortlich ist, wurden die Systeme TARGET2/TIPS/T2S „kundenbasiert" gestaltet, sodass die teilnehmenden Zentralbanken die Anforderungen in Bezug auf die Administration und Überwachung erfüllen können. Die National Service Desks sind unter anderem für Folgendes zuständig:

- Sie fungieren generell als Ansprechpartner und erbringen Business Support für ihre Kunden (d. h. für Kreditinstitute mit PM-Konten, TIPS-Konten, TIPS ASTAs und/oder T2S-Geldkonten sowie für Nebensysteme), einschließlich der Verwaltung der relevanten Stammdaten.
- Sie übernehmen das operative Management (z. B. die Eröffnung/Schließung der nationalen technischen Komponenten).
- Sie sind für das Monitoring des Zahlungsverkehrs ihrer Teilnehmer (z. B. Zahlungsströme, Liquidität und Nutzerverhalten) sowie die technische und betriebliche Überwachung etwaiger lokaler technischer Komponenten zuständig.
- Sie stellen ihren Teilnehmern Innertagesliquidität zur Verfügung (Innertageskredite und Selbstbesicherung).
- Sie kümmern sich um lokale Contingency-Arrangements und um Ausnahmesituationen.

- Sie stellen Stammdaten zur Nutzung bei der Selbstbesicherung bereit und arbeiten mit der für das Sicherheitenmanagement zuständigen Abteilung zusammen.
- Sie stellen einen Settlement Manager, der die Institution in TARGET-Services-Telekonferenzen und anderen Foren vertritt.

2.4.3.1.2 TARGET Crisis Communication Group (TC2-Gruppe)

Die 2020 aus Betriebsstörungen der TARGET-Services gesammelten Erfahrungen machten die Notwendigkeit deutlich, bei größeren Störungen von einer unidirektionalen auf eine bidirektionale Kommunikation umzustellen. Für die TARGET2-Krisenmanager ist es nämlich wichtig, Rückmeldungen von den Marktteilnehmern darüber zu erhalten, ob die Kommunikation ausreichend klar ist und ihre dringendsten Fragen hinreichend beantwortet wurden.

Um die Kommunikation zu verbessern, einen direkteren Draht zu den Marktteilnehmern zu erhalten und einen weiteren Kommunikationskanal für die Krisenmanager zu öffnen, über den sie bei größeren Störungen wertvolle Informationen sammeln können, wurde die TARGET Crisis Communication Group (TC2-Gruppe) ins Leben gerufen. Zu beachten ist, **dass das Störungsmanagement selbst nicht in den Aufgabenbereich dieser Gruppe fällt und weiter den Krisenmanagern überlassen bleibt.**

Zusammensetzung:

Zur TC2-Gruppe gehören alle TARGET2-Krisenmanager (einschließlich der 3ZB-Krisenmanager) sowie Vertreter von kritischen TARGET2-Teilnehmern, die ihr Interesse an der Teilnahme an dieser Gruppe bekundet haben (auf freiwilliger Basis). Die TC2-Telefonkonferenzen **werden vom EZB-Krisenmanager geleitet**. Je nach Art des Krisenszenarios (d. h. Störungen, die mit der Konnektivität in Verbindung stehen oder diese beeinflussen) können auch die Netzwerkdienstleister involviert sein.

Telefonkonferenzen der TC2-Gruppe

- Eine Telefonkonferenz der TC2-Gruppe erfolgt ausschließlich aufgrund eines **Beschlusses der Krisenmanager im Fall von schwerwiegenden Störungen**. Kennzeichen für eine schwerwiegende Störung sind entweder die Dauer der Störung oder die Besonderheit des Szenarios oder die Auswirkungen, die die Störung auf die Finanzmärkte haben könnte.
- Die TC2-Gruppe kann beispielsweise **einberufen werden bei**:
  - einer intra- oder interregionalen Ausfallsicherung,
  - lang andauernden Störungen,
  - einem erfolgreichen Cyberangriff, der die Integrität des Systems beeinträchtigt,
  - anderen von den Krisenmanagern ermittelten und vereinbarten Szenarien.

- **Wann die TC2-Gruppe involviert wird** und wie viele TC2-Telefonkonferenzen während einer Störung stattfinden, wird ebenfalls von den Krisenmanagern von Fall zu Fall entschieden. Zu beachten ist, **dass die TC2-Gruppe nicht unmittelbar nach Feststellung eines Problems eingebunden wird, sondern erst zu einem späteren Zeitpunkt**, wenn ein vollständiges Bild über die Auswirkungen vorliegt und klarer ist, welche möglichen provisorischen und endgültigen Lösungen es gibt.
- **Bei den TC2-Telefonkonferenzen** haben die Marktteilnehmer die Möglichkeit, **Fragen** zu stellen oder um die **Klarstellung** von Punkten zu ersuchen, die in der bisherigen Kommunikation nicht oder nicht ausreichend erörtert wurden. Außerdem **können die Krisenmanager wichtige Informationen** über die Auswirkungen der Störung auf die Geschäftsprozesse der Marktteilnehmer direkt von ihnen selbst erhalten. Dies würde es den Krisenmanagern ermöglichen, ihre Kommunikation beim nächsten Mal weiter zu verbessern.
- Die **TC2-Mitglieder dürfen bei der Kommunikation nicht bevorzugt behandelt werden**. Erhalten TC2-Mitglieder auf ihre Fragen zusätzliche Informationen, so müssen diese Informationen in der nächsten Kommunikation auch den übrigen Beteiligten zugänglich gemacht werden.
- Die TC2-Gruppe ersetzt keine bereits bestehenden Gruppen, die die nationalen Zentralbanken eingerichtet haben und im Krisenfall für ihre nationale Nutzergruppe aktivieren.
- **Während der TC2-Telefonkonferenzen:**
  - haben die Marktteilnehmer die Möglichkeit, Fragen zu stellen oder um die Klarstellung von Punkten zu ersuchen, die nicht oder nicht ausreichend in der bisherigen Kommunikation erörtert wurden;
  - bitten die Krisenmanager die Marktteilnehmer darum, ihnen wichtige Informationen über die Auswirkungen der Störung auf ihre Geschäftsprozesse mitzuteilen, mithilfe derer sie anschließend die Kommunikation beim nächsten Update weiter verbessern könnten.
- Die **Teilnahme an TC2-Telefonkonferenzen ist für Marktteilnehmer und** Krisenmanager der **NZBen freiwillig**. Die **Krisenmanager der EZB und der 3ZB müssen immer** an diesen Telefonkonferenzen **teilnehmen**.
- Die TARGET2-Krisenmanager sind rund um die Uhr erreichbar, was auch grundsätzlich für die TC2-Gruppe gilt. Die Teilnehmer können somit jederzeit angerufen werden.
- Um die korrekte Funktionsfähigkeit des Tools zu testen und das Verfahren zu simulieren, das im TARGET2-Störfall zu befolgen ist, organisiert die EZB Konnektivitätstests und Simulationen.

2.4.3.1.3 Erreichbarkeit der National Service Desks

Während der üblichen Supportzeiten sind die National Service Desks an allen TARGET2-Geschäftstagen von 6.45 Uhr bis 18.15 Uhr[12] MEZ erreichbar und unterstützen ihre Teilnehmer bei *Standardgeschäften* (hierzu zählen die Beantwortung von Anfragen, das Monitoring des Zahlungsverkehrs, die Bearbeitung von Serviceanfragen, die Verwaltung von Stammdaten, das Handeln im Auftrag von Teilnehmern und sonstige Kommunikationen) und bei der *Behebung von Störungen*.

Außerhalb der üblichen Supportzeiten sind weiterhin die Krisenmanager der Zentralbanken für die Behebung von Störungen verantwortlich,

a) und zwar in TARGET2 und T2S rund um die Uhr an allen TARGET2-Geschäftstagen und
b) in TIPS rund um die Uhr an 365 Tagen im Jahr.

Je nach Art der Störung und der Auswirkungen auf die Verfügbarkeit von TARGET2/T2S/TIPS informiert der zuständige National Service Desk die Teilnehmer entsprechend. Bei Störungen, die über die üblichen Supportzeiten der National Service Desks (d. h. 18.15 Uhr MEZ[13]) hinaus anhalten, bleiben die zuständigen National Service Desks so lange für ihre Märkte erreichbar, bis die Störung behoben ist.

Lediglich bei Konnektivitätsproblemen können sich T2S/TIPS-Geldkontoinhaber direkt an den T2S/TIPS-Servicedesk wenden. Dieser steht bei entsprechenden Problemen rund um die Uhr an 365 Tagen im Jahr – also auch an geschäftsfreien Tagen des TARGET2-Systems – zur Verfügung.

Weitere Informationen zu den Kommunikationswegen finden sich im nachfolgenden Kapitel.

2.4.3.1.4 Kommunikation mit den Nutzern

Ansprechpartner für TARGET2-Nutzer ist generell bei allen Fragen der National Service Desk. Dabei gilt jedoch:

a) Lediglich bei Konnektivitätsproblemen kann ein T2S-Geldkontoinhaber/TIPS-Geldkontoinhaber/TIPS-ASTA-Kontoinhaber mit direkter Anbindung an T2S/TIPS den T2S/TIPS

12 Am letzten Tag der Mindestreserve-Erfüllungsperiode bis 18.30 Uhr.
13 Am letzten Tag der Mindestreserve-Erfüllungsperiode bis 18.30 Uhr.

Service Desk direkt kontaktieren. Dieser öffnet ein Ticket und informiert die entsprechende Zentralbank. Bei Zweifeln darüber, ob es sich um ein Konnektivitätsproblem handelt, sollte der direkt angeschlossene T2S-Geldkontoinhaber/TIPS-Geldkontoinhaber den National Service Desk kontaktieren. Kontaktaufnahmen zum T2S/TIPS Service Desk, die nichts mit Konnektivitätsfragen zu tun haben, sollten an die National Service Desks weitergeleitet werden (und umgekehrt). Direkt angebundene T2S-Geldkontoinhaber/TIPS-Geldkontoinhaber erhalten die Kontaktdaten des T2S/TIPS Service Desk zum Zeitpunkt ihrer Anbindung an die Systeme über den zuständigen National Service Desk. T2S-Geldkontoinhaber/TIPS-Geldkontoinhaber können sich jedoch jederzeit proaktiv mit ihrem zuständigen National Service Desk in Verbindung setzen, um diese Daten erneut zu erfragen.

1) Der TIPS Service Desk ist rund um die Uhr an 365 Tagen im Jahr erreichbar.
2) Der T2S Service Desk ist von 6.30 Uhr bis 20.00 Uhr an T2S-Öffnungstagen erreichbar.

b) Bei Konnektivitätsfragen kann der T2S/TIPS Service Desk unmittelbar angeschlossene T2S-Geldkontoinhaber/TIPS-Geldkontoinhaber auch direkt kontaktieren, wovon er den National Service Desk in Kenntnis setzt. Die Kontaktdaten der Person bzw. des Teams, die/das für Fragen zur T2S-/TIPS-Konnektivität der jeweiligen direkt angebundenen Geldkontoinhaber verantwortlich ist, werden von der jeweiligen Zentralbank eingeholt. Möchte ein T2S-Geldkontoinhaber/TIPS-Geldkontoinhaber nicht direkt vom T2S/TIPS Service Desk kontaktiert werden, wird stattdessen Verbindung zum National Service Desk der Zentralbank aufgenommen (und dessen Kontaktdaten werden eingeholt).

c) Hat eine erreichbare Partei in TIPS Konnektivitätsprobleme, sind diese über den TIPS-Geldkontoinhaber, der die erreichbare Partei benannt hat, an den TIPS Service Desk weiterzuleiten.

Da **erreichbare Parteien und einreichende Parteien** im Rahmen von TIPS keine formale Geschäftsbeziehung zu einer bestimmten Zentralbank unterhalten, ist je nach Einzelfall wie im Folgenden dargestellt vorzugehen, um sicherzustellen, dass die erreichbaren und die einreichenden Parteien die erforderliche geschäftliche Unterstützung erhalten:

a) Fragen zur Funktionalität:

Einreichende Parteien können Fragen bezüglich der Funktionalität von TIPS an einen National Service Desk richten, und zwar entweder an den National Service Desk des eigenen Landes oder an den National Service Desk, der eine Geschäftsbeziehung zu einem TIPS-Geldkontoinhaber unterhält, welcher die einreichende Partei nutzt. Alternativ können solche Fragen auch von einem TIPS-Geldkontoinhaber gestellt werden, der die einreichende Partei nutzt. In diesem Fall richtet

der TIPS-Geldkontoinhaber seine Fragen an den National Service Desk der Zentralbank, mit der er eine vertragliche Beziehung unterhält. Der National Service Desk kann die Frage entweder selbst klären oder bindet den TIPS Service Desk mit ein.

Erreichbare Parteien sollten Fragen bezüglich der Funktionalität von TIPS an den TIPS-Geldkontoinhaber richten, mit dem sie in Geschäftsbeziehung stehen; dieser kann im Bedarfsfall den zuständigen National Service Desk kontaktieren.

b) Anfragen zu bestimmten TIPS-Geldkonten oder TIPS-Geldkontoinhabern:

Benötigt eine einreichende Partei Informationen über einen bestimmten TIPS-Geldkontoinhaber, der die einreichende Partei nutzt (wenn die einreichende Partei beispielsweise Fragen hinsichtlich einer bestimmten Transaktion hat), ist das schriftliche Einverständnis des TIPS-Geldkontoinhabers erforderlich (Einreichung einer Einverständniserklärung[14]), dass seine Heimatzentralbank der einreichenden Partei die erforderlichen Informationen über den TIPS-Geldkontoinhaber selbst und/oder über seine erreichbaren Parteien bereitstellen darf, um die Zentralbank von jeglicher rechtlichen Verpflichtung freizustellen.

Bei Anfragen seitens der einreichenden Partei wird unterstellt, dass dem TIPS-Geldkontoinhaber auch das Einverständnis seiner erreichbaren Parteien (falls vorhanden) vorliegt, dass derartige Informationen an die einreichende Partei weitergegeben werden dürfen.

c) Konnektivitätsprobleme:

Hat eine einreichende Partei Probleme bei der technischen Anbindung, so darf sie den TIPS Service Desk direkt kontaktieren. Bei der Prüfung des Problems könnte der Austausch von Informationen erforderlich werden. In diesem Fall prüft der TIPS Service Desk, ob die kontaktaufnehmende einreichende Partei über die Befugnis einer Zentralbank verfügt, konnektivitätsbezogene Informationen zu erhalten (z. B. Distinguished Names, technische Adressen von Parteien).

Wendet sich die einreichende Partei mit Problemen an den TIPS Service Desk, die nicht die Konnektivität betreffen, so wird die Anfrage zurückgewiesen. Die einreichende Partei sollte dann je nach Einzelfall gemäß den unter Punkt a) aufgeführten Verfahren vorgehen.

14 Formulare für die Einverständniserklärung werden im Laufe des Jahres 2020 zur Verfügung gestellt.

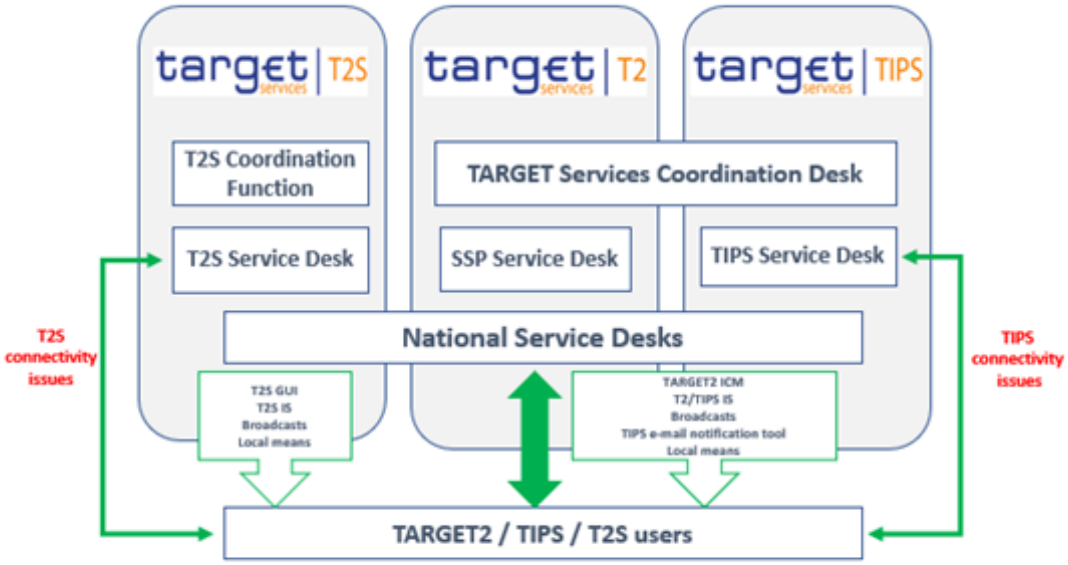


Abbildung 4: Informationsfluss

Kommunikationsmittel

Folgende Kommunikationsmittel können zwischen der jeweiligen Zentralbank und ihren Nutzern verwendet werden:

Informations- und Steuerungsmodul (ICM)

Das Informations- und Steuerungsmodul (Information and Control Module – ICM) verschafft PM-Kontoinhabern und Nebensystemen Zugang zu einem breitgefächerten Spektrum allgemeiner Informationen wie z. B. Guthaben oder Transaktionen. Es ermöglicht den National Service Desks darüber hinaus, Nachrichten an ihre jeweilige nationale Bankengemeinschaft (außer an T2S-Geldkontoinhaber) zu senden. Ein Nachrichtenticker im oberen Teil des Bildschirms eignet sich ferner zur Versendung wichtiger Informationen. Nutzbar sind diese Tools nur, wenn ein ICM-Zugang verfügbar ist. Daher sind sie bei Konnektivitätsproblemen von SWIFTNet oder einem Ausfall der Gemeinschaftsplattform unter Umständen nicht verwendbar.

T2S GUI

T2S GUI ermöglicht direkt angeschlossenen T2S-Geldkontoinhabern zur Überwachung und Steuerung ihres Geschäfts (z. B. für die Verwaltung von Limiten) den Zugriff auf ein breites Spektrum allgemeiner

Informationen (z. B. über Kontostände oder Transaktionen). Darüber hinaus gestattet es den National Service Desks die Versendung von Nachrichten an ihre jeweiligen T2S-Geldkontoinhaber.

E-Mail-Benachrichtigungstool von TIPS

Der TIPS-Betreiber hat die Möglichkeit, eine Störung, die die Verfügbarkeit von TIPS beeinträchtigt, per E-Mail mitzuteilen. Dieses Benachrichtigungstool wird **bei TIPS-Störungen verwendet, die die Verarbeitung von Instant Payments beeinflussen und außerhalb der üblichen Supportzeiten eintreten**. Informiert werden alle Zentralbanken sowie die TIPS-Geldkontoinhaber/TIPS-ASTA-Kontoinhaber/erreichbaren Parteien/einreichenden Parteien, die zu diesem Zweck ihre Kontaktdaten mitgeteilt haben. Der TIPS-Betreiber pflegt eine entsprechende Kontaktliste.

Die National Service Desks sind dafür verantwortlich, dem TIPS Service Desk die Änderungen mitzuteilen, die an dieser Kontaktliste für ihre jeweilige nationale Nutzergruppe vorgenommen werden müssen. Hierfür müssen die National Service Desks das entsprechende Formular ausfüllen und dem TIPS Service Desk einreichen, um:

a) neue TIPS-Geldkontoinhaber/TIPS-ASTA-Kontoinhaber/erreichbare Parteien/einreichende Parteien aufnehmen zu lassen,
b) die an der Kontaktliste erforderlichen Änderungen vornehmen zu lassen (Löschung von Teilnehmern oder Änderung der E-Mail-Adresse eines Teilnehmers).

Das E-Mail-Benachrichtigungstool von TIPS wird halbjährlich getestet. Hierbei erhalten alle registrierten Parteien eine Test-E-Mail von dem Tool. Der Zeitpunkt des Tests wird vorab vereinbart und über die jeweilige nationale Zentralbank bekanntgegeben.

Lokale Kommunikationsinstrumente

Mit lokalen Tools sind nationale Kommunikationsmittel gemeint. Die zuständige NZB informiert ihre TARGET2-Nutzer über die zur Verfügung stehenden nationalen Kommunikationskanäle. Abrufbar sind die Kontaktangaben für die einzelnen Länder neben sonstigen länderbezogenen Informationen unter „Contact Items“ im ICM.

Betriebsstatusseite der TARGET-Services auf der EZB-Website

Auf der Betriebsstatusseite der TARGET-Services (siehe Website der EZB) können die Nutzer von TARGET2, TIPS und T2S, die breite Öffentlichkeit und Nachrichtenagenturen den Betriebsstatus der drei Systeme einsehen. Die Informationen werden über das Market Information Dissemination System (MID-System)[15] der EZB bereitgestellt. Es wird angezeigt, ob die Systeme im Normalbetrieb (Tagesbeginn/Tagesende) laufen oder ob eine Ausnahmesituation herrscht. In letzterem Fall werden

15 Nähere Informationen zum MID-System der EZB finden sich auf der Website der EZB.

auch Angaben über die Art der Störung, seine Auswirkungen und die zur Problemlösung ins Auge gefassten Maßnahmen sowie den Zeitpunkt des nächsten Updates gemacht.

2.5 Öffnungstage

Die TARGET2-Öffnungstage sind de facto die Abwicklungstage für die Euro-Finanzmärkte sowie für Devisentransaktionen mit dem Euro als Währung.

Geöffnet ist TARGET2 täglich außer samstags, sonntags, Neujahr, Karfreitag und Ostermontag (nach dem am Sitz der EZB gültigen Kalender) und am 1. Mai und 25. und 26. Dezember.

Derselbe Kalender gilt für die T2S-Geldverrechnung in Euro.

Zwar steht T2S am 1. Mai zur Verfügung, doch es erfolgt keine Abwicklung in Euro (lediglich Free-of-payment-Transaktionen sind möglich). Das heißt, dass es in Bezug auf den Moment, in dem Daueraufträge zu Liquiditätsübertragungen von PM-Konten auf T2S-Geldkonten verarbeitet werden, am 1. Mai zu einer Zeitlücke zwischen der Gemeinschaftsplattform und der T2S-Plattform kommt. Die Verarbeitung auf der Gemeinschaftsplattform erfolgt um 19.30 Uhr am Vorabend des 1. Mai für den nächsten TARGET2-Geschäftstag, der auf den Tag nach dem 1. Mai fällt. Auf der T2S-Plattform erfolgt sie um 20.00 Uhr am Abend des 1. Mai, wenn der T2S-Geschäftstag beginnt, der dasselbe Wertstellungsdatum trägt wie in TARGET2. Anders formuliert, die Daueraufträge zu Liquiditätsübertragungen müssen auf die T2S-Abwicklung nicht 30 Minuten, sondern mindestens 24 Stunden und 30 Minuten warten.

TIPS ist rund um die Uhr an 365 Tagen im Jahr in Betrieb. Der Geschäftstag hängt jedoch vom RTGS-System für die in TIPS abzuwickelnde Währung ab (d. h., für den Euro sind die Öffnungstage von TARGET2 relevant und für alle anderen Währungen die Öffnungszeiten des entsprechenden nationalen RTGS-Systems).

Dies bedeutet **beispielsweise für auf Euro lautende** Instant Payments, die samstags und sonntags abgewickelt werden, dass sie als Wertstellungsdatum den nächsten TARGET2-Geschäftstag (also Montag) tragen.

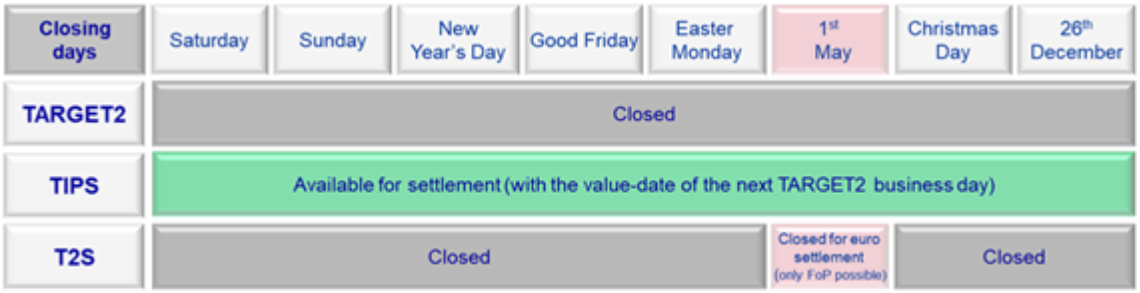


Abbildung 5: Geschäftsfreie Tage in TARGET2, TIPS und T2S

2.6 Tagesablauf

Nachstehende Tabelle zeigt die verschiedenen Phasen eines TARGET2-, TIPS[16]- und T2S-Geschäftstags, **die für Zahlungen in Euro gelten**.

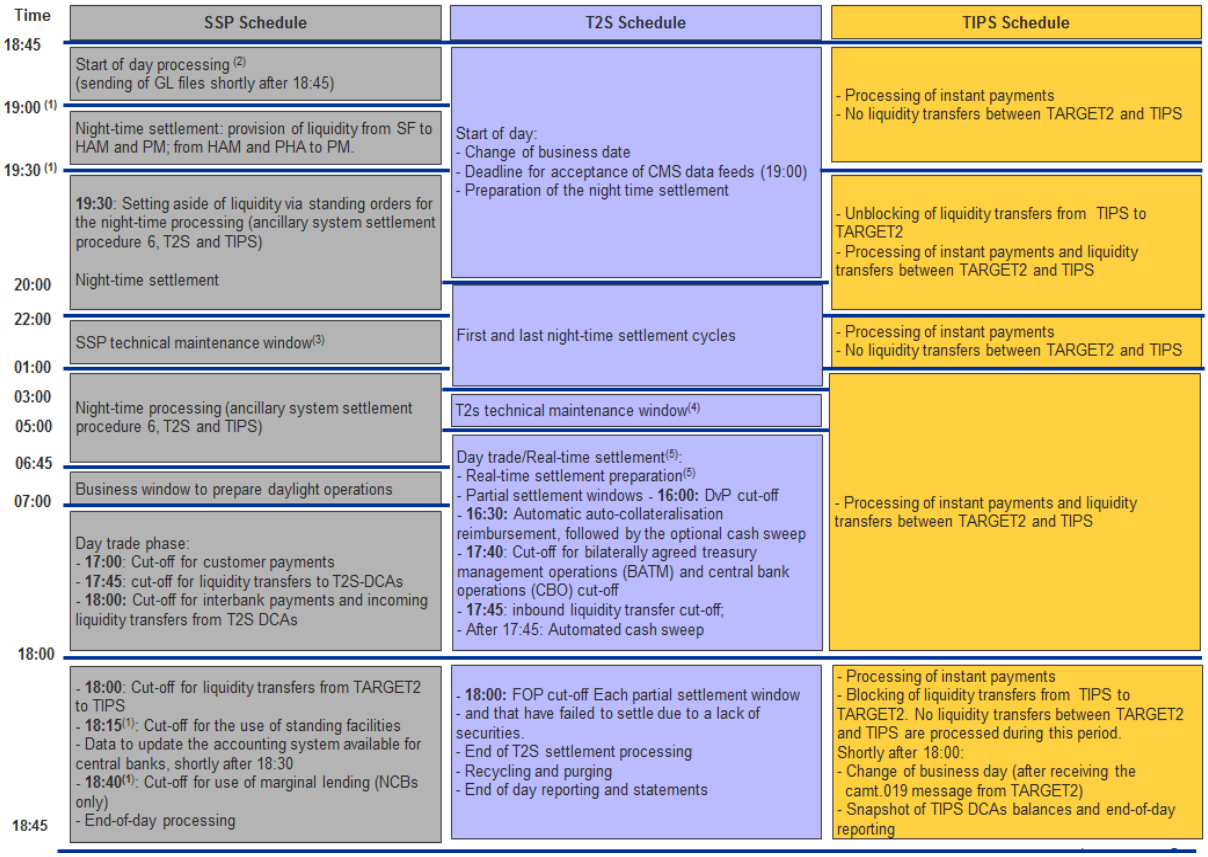


Tabelle 2: Zeitplan an einem Geschäftstag

(1) Beginnt/endet am letzten Tag der Mindestreserve-Erfüllungsperiode 15 Minuten später.

(2) In der TARGET2-Leitlinie dauert die Tagesbeginn-Verarbeitung bis 19.30 Uhr (d. h. einschließlich der nachfolgenden Liquiditätsbereitstellung von 19.00 Uhr bis 19.30 Uhr), da sie aus geschäftlicher Perspektive eigentlich als Vorbereitung für die Zahlungsverarbeitung gilt.

(3) An Wochenenden oder Feiertagen bleibt das technische TARGET2-Fenster über das ganze Wochenende oder den ganzen Feiertag geöffnet, d. h. von Freitag, 22.00 Uhr bis Montag, 1.00 Uhr bzw. von 22.00 Uhr des letzten Geschäftstags vor dem Feiertag bis 1.00 Uhr des nächstfolgenden

16 Der Zeitplan für TIPS weicht an Wochenenden und TARGET2-Feiertagen vom üblichen Muster, das in Tabelle 2 dargestellt ist, ab. Beispielsweise sind von Freitag, 22.00 Uhr bis Montag, 1.00 Uhr keine Liquiditätsübertragungen zwischen TIPS und TARGET2 möglich.

Geschäftstags.

(4) An Wochenenden oder Feiertagen bleibt das technische T2S-Fenster über das gesamte Wochenende oder den ganzen Feiertag geöffnet, d. h. von Samstag, 3.00 Uhr bis Montag, 5.00 Uhr bzw. von 3.00 Uhr am Feiertag bis 5.00 Uhr des nächstfolgenden Geschäftstags.

(5) Die Vorbereitung der Echtzeitabwicklung und die Echtzeitabwicklung können bereits vor dem Wartungsfenster beginnen, sofern der letzte Nachtverarbeitungszyklus vor 3.00 Uhr endet.

2.7 Transaktionen über TARGET2

Wie in Abschnitt 3.1 beschrieben, werden PM-Konten nur für bestimmte zugelassene Teilnehmer eröffnet, die zuvor auch eine Reihe von Zertifizierungstests bestanden haben müssen (siehe Abschnitt 3). Solange es keinen triftigen Grund für die Beendigung oder Suspendierung der Teilnahme eines TARGET2-Teilnehmers gibt (siehe Abschnitt 3.6), können PM-Konten nicht von der Abwicklung von Transaktionen ausgeschlossen werden. Im Interesse eines reibungslosen Betriebs von TARGET2 wird daher von jedem Teilnehmer erwartet, dass er Zahlungen von PM-Konten anderer Teilnehmer akzeptiert. Teilnehmer dürfen weder eingehende Zahlungen von bestimmten designierten PM-Konten noch Zahlungen von PM-Konten insgesamt „blockieren“.

Folgende Arten von Transaktionen werden in TARGET2 abgewickelt:

a) Kundenzahlungen

Kundenzahlungen werden über PM-Konten abgewickelt und sind als Zahlungen im Format SWIFTNet FIN MT 103 definiert (Standard oder STP). Kundenzahlungen können über TARGET2 zwischen 7.00 Uhr und 17.00 Uhr verarbeitet werden.

b) Interbankzahlungen

Interbankzahlungen werden über die PM-Konten abgewickelt und als Zahlungsnachrichten im Format SWIFTNet FIN MT 202 und MT 202 COV definiert. Diese Nachrichten werden vom oder im Namen des anweisenden Instituts an das Finanzinstitut des begünstigten Instituts – entweder direkt oder über einen Korrespondenten – übermittelt.

Interbankzahlungen, die über MT 202 verarbeitet werden, sind Zahlungen wie die geldliche Verrechnung am Geldmarkt oder Devisen- und Derivatetransaktionen, die zwischen Kreditinstituten oder zwischen Zentralbanken und Kreditinstituten erfolgen. MT 202 COV sind Interbankzahlungen, die ihnen zugrunde liegende Kundenzahlungen „decken“ und Felder für den Auftraggeber und den Empfänger der Überweisung enthalten. Interbankzahlungen können über TARGET2 von 7.00 Uhr bis 18.00 Uhr verarbeitet werden.

c) Lastschriften

Lastschriften werden über die PM-Konten abgewickelt und sind als Zahlungsnachrichten im Format SWIFTNet FIN MT 204 definiert. Lastschriften in TARGET2 sind Transaktionen zwischen Banken, die ausschließlich für Großeinreicher vorgesehen sind. Die betreffenden PM-Kontoinhaber müssen mit den Parteien, die eine Belastung ihrer Konten gestatten, die Bedingungen für die Inanspruchnahme dieser Dienstleistung vereinbaren. Der Inhaber des PM-Kontos gestattet es einem anderen PM-Kontoinhaber, eine Lastschrift einzureichen, und informiert seine Zentralbank, die für die Erfassung und Verwaltung der getroffenen Vereinbarungen zuständig ist, entsprechend. Lastschriften können über TARGET2 zwischen 7.00 Uhr und 18.00 Uhr verarbeitet werden. Inhaber von PM-Konten, die einen internetbasierten Zugang nutzen, können keine Lastschriftanweisungen ausstellen (sie aber entgegennehmen).

d) Nebensystem-Transaktionen

Zahlungen im Zusammenhang mit der Abwicklung von Nebensystemen: Massenzahlungssysteme, Großbetragszahlungssysteme, Devisenhandelssysteme, Geldmarkthandelssysteme, Clearinghäuser und Wertpapierabwicklungssysteme.

e) Instant-Zahlungen

Instant-Zahlungen werden über TIPS-Geldkonten und TIPS ASTAs abgewickelt. Gemäß der Definition des Europäischen Zahlungsverkehrsrats (European Payments Council – EPC) sind Instant-Zahlungen Zahlungsanweisungen, die 24 Stunden pro Tag an jedem Tag des Jahres ausgeführt werden können und die sofort oder nahezu sofort abgewickelt werden. Der Zahlungspflichtige erhält dabei eine Bestätigung, wenn die Gutschrift auf dem Konto des Zahlungsempfängers eingegangen ist.

f) Positive Rückruf-Antworten

Positive Rückruf-Antworten werden auf den TIPS-Geldkonten und TIPS ASTAs abgewickelt. Gemäß dem SEPA Instant Credit Transfer (SCT^{Inst}) Scheme sind positive Rückruf-Antworten von einem Empfänger einer Rückruf-Anfrage in Reaktion auf eine Rückruf-Anfrage veranlasste Zahlungsaufträge zugunsten des Absenders dieser Rückruf-Anfrage (d. h. eine Mitteilung eines TIPS-Geldkontoinhabers, der die Rückzahlung eines bereits ausgeführten Instant-Zahlungsauftrags verlangt).

g) Liquiditätsübertragungen

Liquidität in Zentralbankgeld kann auf PM-Konten, Heimatkonten, TIPS-Geldkonten und/oder T2S-Geldkonten gehalten werden, wobei die Möglichkeit der Liquiditätsübertragung zwischen den verschiedenen Konten besteht.

Liquiditätsübertragungen im Zusammenhang mit PM-Konten (aber nicht Geldkonten) können über

SWIFTNet FIN MT 202 von 7.00 Uhr bis 18.00 Uhr oder über ICM (im User-to-Application-Modus (U2A-Modus) oder Application-to-Application-Modus (A2A-Modus)) auf der Basis von SWIFTNet InterAct ausgeführt werden. Mittels ICM veranlasste Liquiditätsübertragungen werden während der Betriebszeiten des Zahlungsmoduls bis zum Annahmeschluss für Interbankzahlungen (18.00 Uhr) und ab dem Beginn der Nachtverarbeitung (19.30 Uhr) – mit Ausnahme spezieller Zeitfenster zur Wartung der Gemeinschaftsplattform – sofort nach der Übermittlung ausgeführt.[17]

Informationen zu Liquiditätsübertragungen von PM-Konten auf Geldkonten und umgekehrt sowie zu Liquiditätsübertragungen zwischen T2S-Geldkonten (die derselben Payment Bank gehören oder mit demselben PM-Hauptkonto verlinkt sind) stehen in Abschnitt 2.9 und Abschnitt 2.9.2 zur Verfügung.

h) Geldliche Verrechnung von Wertpapiertransaktionen, die auf T2S-Geldkonten abgewickelt werden:

- Lieferung gegen Zahlung (Delivery versus Payment – DVP) und Erhalt gegen Zahlung (Receive versus Payment – RVP), definiert als Tausch von Wertpapieren gegen Zahlung,

- Lieferung mit Gegenwertverrechnung (Delivery with Payment – DWP), definiert als Wertpapierlieferung von einer zur anderen Partei bei gleichzeitig erfolgender Zahlung,

- Gegenwertverrechnung ohne Lieferung (Payment Free of Delivery – PFOD), die den Tausch von Geld ohne die Lieferung von Wertpapieren darstellen,

- Abwicklungsrestriktionen, die die Blockierung und Reservierung von Geld in einem T2S-Geldkonto ermöglichen.

Es sei angemerkt, dass T2S auch FOP-Transaktionen (Free of Payment) verarbeitet, in denen Wertpapiere geliefert (Delivery Free of Payment – DFOP) oder empfangen (Receive Free of Payment – RFOP) werden können, ohne dass eine Gegenwertverrechnung erfolgt. Definitionsgemäß erfordert diese Transaktionsart allerdings keine Geldbewegungen und wird daher nicht auf der Basis von T2S-Geldkonten abgewickelt.

[17] Zu den Verarbeitungszeiten bei Daueraufträgen vgl. UDFS, Buch 1.

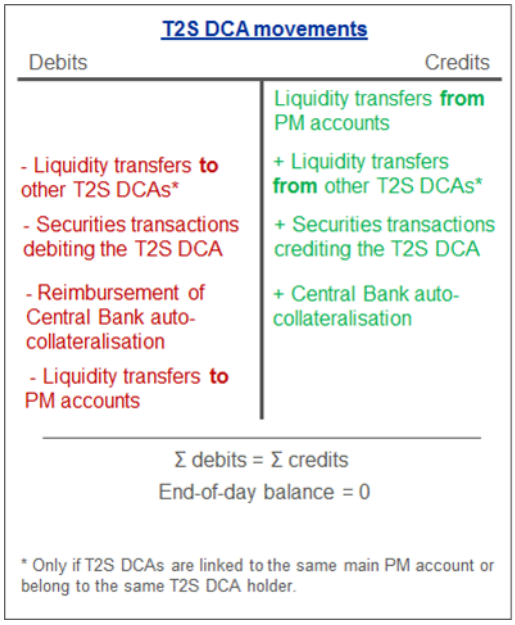


Abbildung 6: Bewegungen auf T2S-Geldkonten

2.8 Liquiditätsübertragungen – in Euro

2.8.1 Liquiditätsübertragungen zwischen PM-Konten und TIPS-Geldkonten

Die Liquiditätsübertragung zwischen PM-Konten und TIPS-Geldkonten ist wie folgt möglich:

1. Liquiditätsübertragungen von PM-Konten auf TIPS-Geldkonten[18]

Die Liquiditätsübertragung von PM-Konten auf TIPS-Geldkonten ist wie folgt möglich:

a) Liquiditätsübertragung per Dauerauftrag

Bei einer Liquiditätsübertragung per Dauerauftrag kann der Inhaber des PM-Kontos einen festen Betrag definieren, der vom PM-Konto auf ein bestimmtes TIPS-Geldkonto übertragen werden soll.

Die Daueraufträge können im Stammdatenmodul der Gemeinschaftsplattform bis spätestens 18.00 Uhr (wirksam ab der nächsten Nachtverarbeitung), über das ICM oder (im A2A-Modus) per XML-Nachricht eingegeben werden. Die Ausführung erfolgt kontinuierlich (bis der Dauerauftrag geändert wird) zu Beginn der Abwicklung der Nachtverarbeitung der Nebensysteme (19.30 Uhr plus 15 Minuten am letzten Tag der Mindestreserve-Erfüllungsperiode).

Ist nicht genügend Liquidität vorhanden, erfolgt eine Teilausführung aller zu diesem Zeitpunkt

18 Liquiditätsübertragungen zwischen TIPS-Geldkonten sind nicht möglich.

anstehenden Daueraufträge (einschließlich solcher mit Abwicklungsverfahren 6 bzw. T2S). Dies geschieht wie folgt:

- **Ermittlung eines Kürzungsfaktors**: bestehende Liquidität / Summe aller Daueraufträge
- **Kürzung der Daueraufträge**: Dauerauftrag **x** Kürzungsfaktor

b) Liquiditätsübertragung per laufendem Auftrag

Ein laufender Auftrag ermöglicht dem Inhaber des PM-Kontos, sofort Liquidität auf ein bestimmtes TIPS-Geldkonto zu übertragen. Diese Aufträge können zwischen dem Beginn der Abwicklung der Nachtverarbeitung der Nebensysteme (19.30 Uhr plus 15 Minuten am letzten Tag der Mindestreserve-Erfüllungsperiode) und dem Annahmeschluss für Interbankzahlungen (18.00 Uhr) über die Gemeinschaftsplattform, konkret über das ICM oder (im A2A-Modus) per XML-Nachricht, initiiert werden.[19]

Ist nicht genügend Liquidität vorhanden, werden die Liquiditätsübertragungen während der Tagverarbeitung der Gemeinschaftsplattform in eine Warteschlange gestellt. Während der Nachtverarbeitung werden sie zurückgewiesen.

2. Liquiditätsübertragungen von TIPS-Geldkonten auf PM-Konten

Die Liquiditätsübertragung von TIPS-Geldkonten auf PM-Konten ist über laufende Aufträge zur Liquiditätsübertragung wie folgt möglich:

a) über die Gemeinschaftsplattform (durch den Inhaber des mit dem TIPS-Geldkonto verbundenen PM-Kontos), und zwar über das ICM oder (im A2A-Modus) per XML-Nachricht. Dabei handelt es sich um sogenannte „Pull"-Liquiditätsübertragungen aus TIPS.

b) in TIPS (durch den Inhaber des TIPS-Geldkontos), über die TIPS GUI oder (im A2A-Modus) per XML-Nachricht.

Solche Liquiditätsübertragungen gemäß a) und b) oben können zwischen dem Beginn der Abwicklung der Nachtverarbeitung der Nebensysteme auf der Gemeinschaftsplattform (19.30 Uhr plus 15 Minuten am letzten Tag der Mindestreserve-Erfüllungsperiode) und dem Annahmeschluss für Interbankzahlungen (18.00 Uhr) initiiert werden.[20]

Ist nicht genügend Liquidität auf dem TIPS-Geldkonto vorhanden, wird die Liquiditätsübertragung

19 Ausnahme: Wartungsfenster der Gemeinschaftsplattform zwischen 22.00 Uhr und 1.00 Uhr.
20 Ausnahme: Wartungsfenster der Gemeinschaftsplattform zwischen 22.00 Uhr und 1.00 Uhr.

zurückgewiesen.

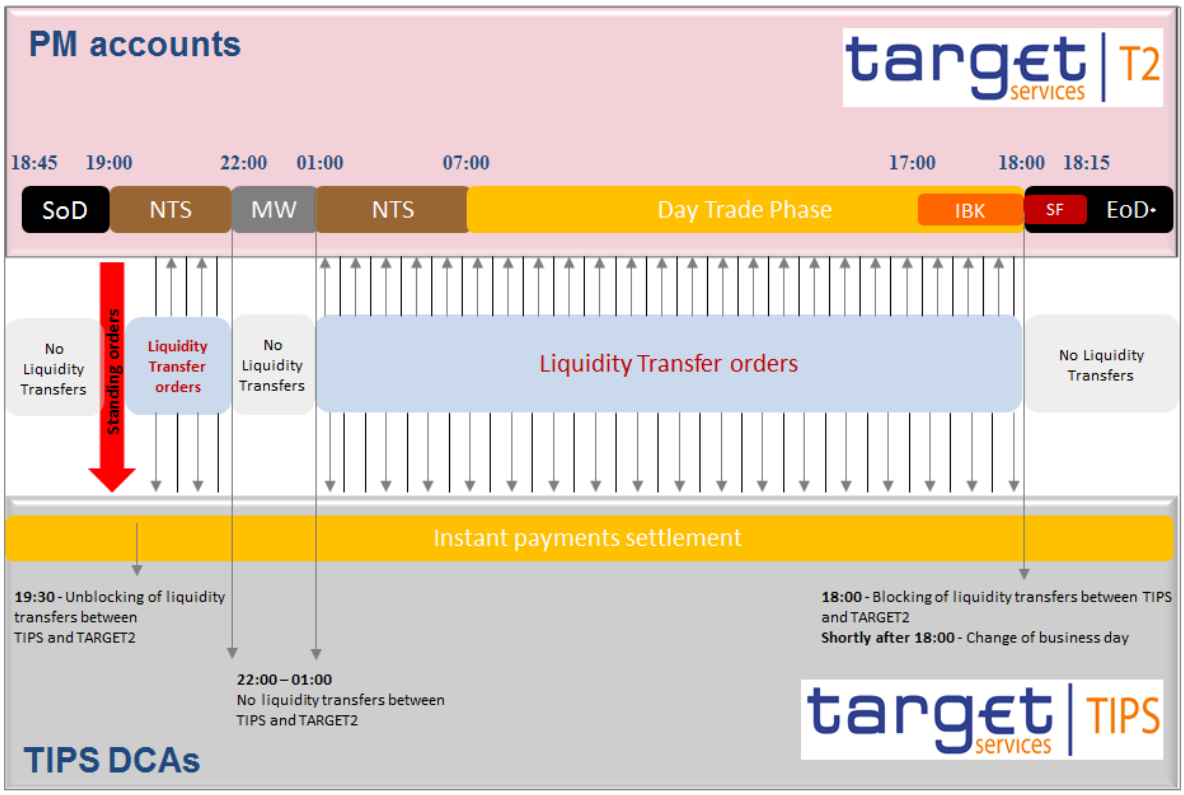


Abbildung 7: Liquiditätsströme zwischen PM-Konten und TIPS-Geldkonten

2.8.2 Liquiditätsübertragungen zwischen TIPS-Geldkonten und technischen Nebensystem-Konten in TIPS

Serviceinterne Liquiditätsübertragungen dienen dazu, Liquidität in derselben Währung im TIPS-System zwischen Geldkonten und technischen Nebensystem-Konten (TIPS ASTAs) zu transferieren. Durch eine serviceinterne Liquiditätsübertragung kann Liquidität zugunsten/zulasten von TIPS ASTAs transferiert werden, damit Nebensysteme Instant Payments abwickeln können. Serviceinterne Liquiditätsübertragungen sind rund um die Uhr an 365 Tagen im Jahr möglich und können im A2A-Modus und im U2A-Modus über eine spezielle Erfassungsmaske in der TIPS-GUI ausgelöst werden. Sie werden sofort ausgeführt. Zu beachten ist, dass serviceinterne Liquiditätsübertragungen zwischen zwei TIPS-Geldkonten oder zwischen zwei TIPS ASTAs nicht möglich sind

a) Eine serviceinterne Liquiditätsübertragung von einem TIPS-Geldkonto auf ein TIPS ASTA kann von einer Zentralbank, einem TIPS-Teilnehmer, einem Nebensystem oder einer einreichenden Partei im Auftrag eines TIPS-Teilnehmers veranlasst werden.

b) Eine serviceinterne Liquiditätsübertragung von einem TIPS ASTA auf ein TIPS-Geldkonto kann von einer Zentralbank, einem Nebensystem oder einer einreichenden Partei im Auftrag eines Nebensystems veranlasst werden.

2.8.3 Liquiditätsübertragungen zwischen PM-Konten und T2S-Geldkonten sowie zwischen T2S-Geldkonten

Es ist möglich, Liquidität von PM-Konten auf T2S-Geldkonten und von T2S-Geldkonten auf PM-Konten zu transferieren. Daneben ist es möglich, Liquidität zwischen T2S-Geldkonten zu übertragen, wenn die beteiligten T2S-Geldkonten mit demselben RTGS-Konto verlinkt sind oder demselben T2S-Geldkontoinhaber gehören.

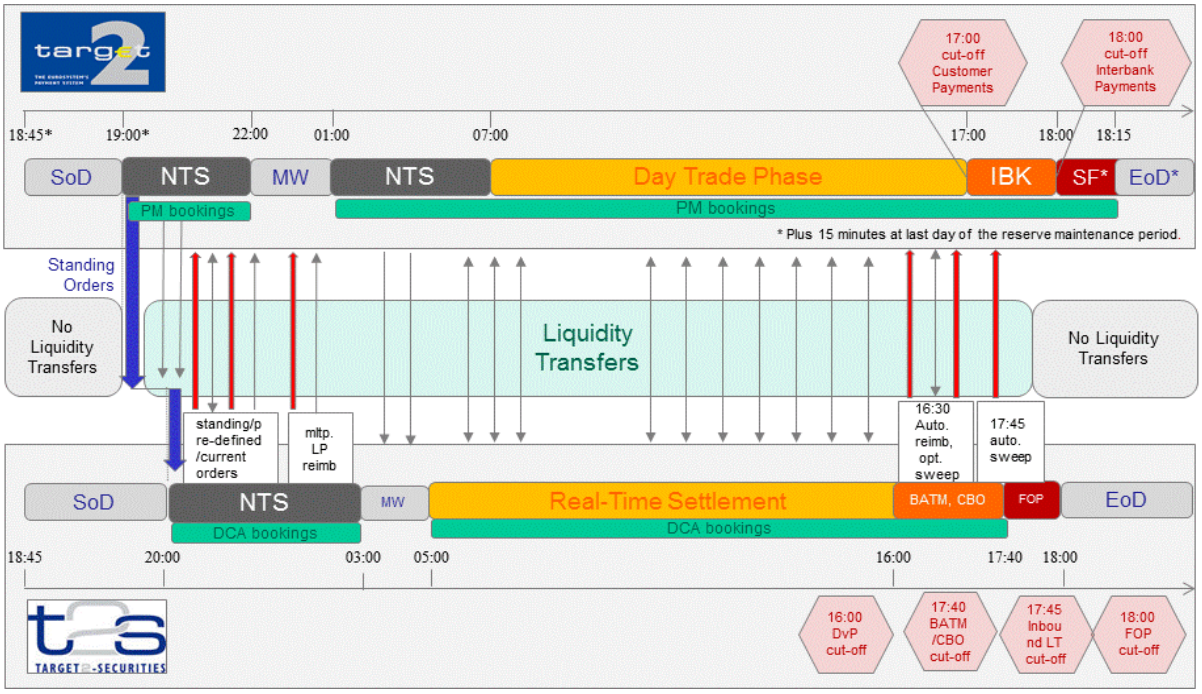


Abbildung 8: Liquiditätsströme zwischen PM-Konten und T2S-Geldkonten

Liquiditätsübertragungen zwischen T2S-Geldkonten sind möglich, wenn die T2S-Geldkonten mit demselben RTGS-Konto verlinkt sind oder demselben T2S-Geldkontoinhaber gehören. In einer Contingency-Situation ist es auch möglich, Liquiditätsübertragungen zwischen den T2S-Geldkonten einer Payment Bank und dem Geldkonto der Zentralbank auszuführen. Eine Teilausführung bei ungenügender Liquidität auf dem T2S-Geldkonto ist lediglich dann möglich, wenn die Liquiditätsübertragung von einer dritten Partei veranlasst wird, die vom T2S-Geldkontoinhaber dazu autorisiert wurde.

Diese Liquiditätsübertragungen können von T2S-Geldkontoinhabern initiiert werden, die im A2A-Modus direkt mit T2S verbunden sind, über ISO 20022-Nachrichten, oder (im U2A-Modus) über die T2S GUI. Sie werden in T2S ab dem ersten Nachtverarbeitungszyklus – Sequenz 0 abgewickelt werden (siehe Abschnitt 4.1.4).

Liquiditätsübertragungen von PM-Konten auf T2S-Geldkonten sind in der SSP zu veranlassen und werden mit Beginn des neuen Geschäftstags von 19.30 Uhr (unterbrochen durch das Wartungsfenster von 22.00 Uhr bis 1.00 Uhr) bis zum Annahmeschluss für Liquiditätsübertragungen auf T2S (17.45 Uhr) durchgeführt. Alle PM-Kontoinhaber mit SWIFT-basiertem Zugang können Liquiditätsübertragungen auf T2S-Geldkonten vornehmen.

Bei **Liquiditätsübertragungen von PM-Konten auf T2S-Geldkonten** lässt sich zwischen folgenden Aufträgen unterscheiden:

a) **Daueraufträge**, die vom Inhaber eines PM-Kontos eingerichtet wurden

Auf der Gemeinschaftsplattform wird ein Dauerauftrag regelmäßig in der angegebenen Höhe ausgeführt, bis er geändert wird. Die Aufträge können bis spätestens 18.00 Uhr (wirksam mit der nächsten Nachtverarbeitung) eingestellt werden. Die Ausführung auf der Gemeinschaftsplattform erfolgt unmittelbar nach der automatischen Durchgabe der Nachricht „Beginn des Verfahrens“ („Start of procedure“) (nur bei der Nachtverarbeitung) bzw. auf der T2S-Plattform während der Sequenz 0 des ersten Nachtverarbeitungszyklus. Bei ungenügender Liquidität auf dem PM-Konto erfolgt eine Teilausführung aller zu diesem Zeitpunkt anstehenden Daueraufträge (d. h. zusammen mit den ASI-Daueraufträgen); siehe Abschnitt 4.1.3.

b) **Laufende Aufträge**, die vom Inhaber eines PM-Kontos generiert wurden

Der Auftrag kann im „Push“-Modus (über die TARGET2-Standardleistungen) erfasst werden. Die laufenden Aufträge, die von einem PM-Kontoinhaber initiiert wurden, werden zurückgewiesen, falls die Liquidität nicht ausreicht (keine Teilausführung).

Auf der T2S-Plattform eingegangene laufende Aufträge können ab dem ersten Nachtverarbeitungszyklus, Sequenz 0 abgewickelt werden. Die Ausführung erfolgt sofort, wenn die Nachtverarbeitung begonnen hat und sie zwischen zwei Sequenzen eingehen. Werden sie während der Verarbeitung einer Sequenz entgegengenommen, so erfolgt die Abwicklung mit der nächstfolgenden Sequenz.

c) **Laufende Aufträge einer autorisierten dritten Partei (T2S-Beteiligter in TARGET2)**[21], die im Auftrag des PM-Kontoinhabers handelt

Die Hinterlegung eines laufenden Auftrags durch einen Dritten für den PM-Konteninhaber beruht auf internationalen Regeln. Diese Aufträge werden sofort ausgeführt, sobald sie abgesandt wurden und die T2S-Nachtverarbeitung begonnen hat. Bei ungenügender Liquidität erfolgt lediglich eine Teilausführung.

Liquiditätsübertragungen von T2S-Geldkonten auf PM-Konten können von T2S-Geldkontoinhabern veranlasst werden, die im A2A-Modus direkt mit T2S verbunden sind, über ISO 20022-Nachrichten, oder (im U2A-Modus) über die T2S GUI. Indirekt an T2S angebundene T2S-Geldkontoinhaber können TARGET2-Zusatzleistungen für T2S nutzen,[22] sodass es ihnen möglich ist, mithilfe von ICM, MT 202-Nachrichten oder einer LiquidityCreditTransfer-Nachricht ohne Business Application Header (BAH) Liquidität von den T2S-Geldkonten abzuziehen und auch die Salden auf den jeweiligen T2S-Geldkonten einzusehen.

Solche Liquiditätsübertragungen werden auf der Gemeinschaftsplattform durchgehend außer während der Tagesende- und Tagesbeginn-Verarbeitung (kurz nach 18.00 Uhr bis 19.30 Uhr) und auch nicht während des technischen Wartungsfensters (22.00 Uhr bis 1.00 Uhr) verarbeitet. Da der Saldo auf den T2S-Geldkonten am Ende des Geschäftstags null betragen muss, müssen alle Liquiditätsübertragungen auf PM-Konten vor der Ausführung des letzten Algorithmus (kurz nach 18.00 Uhr) verarbeitet sein. Dies wird durch den automatisierten „Cash Sweep“ in T2S gegen 17.45 Uhr sichergestellt.

Bei der Liquiditätsübertragung von T2S-Geldkonten auf PM-Konten unterscheidet man zwischen folgenden Varianten:

a) **Dauerauftrag zur Liquiditätsübertragung**, der auf der T2S-Plattform initiiert wurde: In T2S lässt sich bei den Stammdaten ein Dauerauftrag erfassen. Dieser wird regelmäßig bis zu dessen Löschung ausgeführt. Auslöser für den Auftrag kann ein bestimmtes Ereignis oder ein bestimmter Zeitpunkt sein. Der Auftrag kann auf einen bestimmten Teilbetrag oder den gesamten Saldo auf dem T2S-Geldkonto lauten. Es ist möglich, während des Geschäftstags verschiedene Aufträge für unterschiedliche Zeiten oder Ereignisse zu erfassen.

Eine Teilausführung könnte bei unzureichender Liquidität erfolgen; der verbleibende Teil wird nicht

21 Der Zugang als T2S-Beteiligter in TARGET2 ist eine spezielle Zugangsart zu TARGET2, die nur über T2SI und im A2A-Modus erfolgen kann, worüber eine dritte Partei (wie zum Beispiel ein Zentralverwahrer) laufende Aufträge zur Liquiditätsübertragung auf T2S im Namen eines PM-Kontoinhabers generieren kann.

22 Nähere Information finden sich in den UDFS, Buch 1.

ausgeführt (nur Nachtverarbeitung).

b) **Vorab auf der T2S-Plattform erstellter Auftrag zur Liquiditätsübertragung:** Ein vorab festgelegter Liquiditätsauftrag wird nur einmal ausgeführt. Er kann durch ein Ereignis ausgelöst werden oder an einem bestimmten Zeitpunkt erfolgen. Es ist zulässig, mehr als einen vorab erstellten Auftrag für unterschiedliche Zeiten oder Ereignisse einzureichen. Der Auftrag kann auf einen bestimmten Teilbetrag oder den gesamten Saldo auf dem T2S-Geldkonto lauten. Bei ungenügender Liquidität werden vorab erstellte Aufträge zur Liquiditätsübertragung teilausgeführt; für den restlichen Teil, der beim ersten Versuch nicht ausgeführt werden konnte, erfolgt keine weitere Abwicklung.

c) **Sofortige Liquiditätsübertragung**, die direkt in T2S oder über TARGET2-Zusatzleistungen für T2S veranlasst wurde:
Sofortige, auf der T2S-Plattform ausgelöste Liquiditätsübertragungen werden während der Nachtverarbeitung ab dem ersten Zyklus, Sequenz 1 unmittelbar ausgeführt. Gehen sie während der Verarbeitung einer Sequenz ein, werden sie gespeichert. Eine Teilausführung bei ungenügender Liquidität auf dem T2S-Geldkonto ist lediglich dann möglich, wenn die Liquiditätsübertragung von einer dritten Partei veranlasst wird, die vom T2S-Geldkontoinhaber dazu autorisiert wurde. Bei sofortigen Liquiditätsübertragungen, die vom T2S-Geldkontoinhaber selbst veranlasst wurden, erfolgt bei mangelnder Liquidität keine Teilausführung, sondern sie werden zurückgewiesen.

Nachfolgende Tabelle gewährt einen Überblick darüber, **wie die Liquidität zwischen PM-Konten und T2S-Geldkonten sowie zwischen T2S-Geldkonten bewegt werden kann**, d. h. entweder im U2A-Modus (über ICM oder T2S GUI) oder im A2A-Modus:

Art der Liquiditätsübertragung		Teilausführung	Periodizität	Ausführungszeiten
Von PM-Konten auf T2S-Geldkonten	Dauerauftrag	Ja	Jeder Geschäftstag	Tagesbeginn
	Laufender Auftrag	Nein	Einmalig	Bei Anweisung
	Laufender Auftrag durch eine Drittpartei (T2S-Akteur in TARGET2)	Ja	Einmalig	Bei Anweisung
Von T2S-Geldkonten auf PM-Konten	Sofortige Liquiditätsübertragung	Ja	Einmalig	Bei Anweisung
	Vorab erstellter Auftrag zur Liquiditätsübertragung	Ja	Einmalig	Vorab festgelegter Zeitpunkt/vorab festgelegtes Ereignis
	Dauerauftrag zur Liquiditätsübertragung	Ja	Jeder Geschäftstag	Vorab festgelegter Zeitpunkt/vorab festgelegtes Ereignis
Zwischen versch. T2S-Geldkonten	Interne und sofortige Liquiditätsübertragung	Nur bei Anweisung durch eine Drittpartei	Einmalig	Bei Anweisung

Tabelle 3: Liquiditätsübertragungen – Überblick

Kasten 1: Euro- Zwischenkonten

Es gibt zwei Euro-Zwischenkonten für die Abwicklung und das Monitoring aller Liquiditätsübertragungen zwischen der SSP und der T2S-Plattform, d. h. zwischen den PM-Konten und den T2S-Geldkonten. Die Liquiditätsströme einschließlich Zwischenkonten sind in der folgenden Abbildung dargestellt:

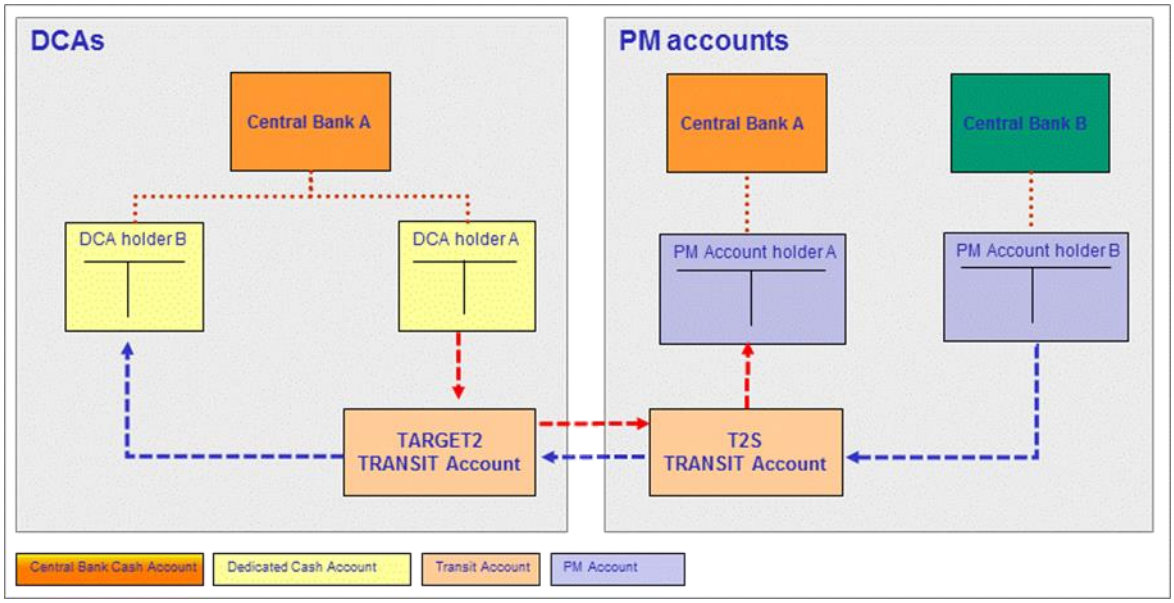


Abbildung 9: Euro-Zwischenkonten

Wie vorstehend illustriert, gibt es ein TARGET2-Zwischenkonto auf der T2S-Plattform (das alle Bewegungen abbildet, die sich auf die T2S-Geldkonten auswirken) und ein T2S-Zwischenkonto auf der SSP (das alle Bewegungen abbildet, die sich auf die PM-Konten auswirken). Die beiden Zwischenkonten haben Spiegelsalden und die Gesamtforderungen und Gesamtverbindlichkeiten ergeben bei Summierung null. Am Tagesende werden die Salden auf beiden Konten in der Regel auf null reduziert (Gesamtverbindlichkeiten = Gesamtforderungen). Zu diesem Zweck werden alle anstehenden Selbstbesicherungen automatisch um 16.30 Uhr zurückgeführt und alle noch verbleibenden Guthaben auf den T2S-Geldkonten über den automatisierten „Cash Sweep“ auf ihre entsprechenden PM-Hauptkonten transferiert; dies findet nach dem Annahmeschluss für eingehende Liquiditätsübertragungen um 17.45 Uhr statt. In Ausnahmesituationen können die Salden über Nacht auf T2S-Geldkonten verbleiben.

2.9 Nachrichtenströme

Es gibt grundsätzlich zwei Arten von Nachrichten: SWIFTNet FIN-Nachrichten (insbesondere Kunden- und Interbankzahlungen sowie Lastschriften) und XML-Nachrichten (InterAct und FileAct; proprietäre und ISO 20022-Nachrichten).

SWIFT-FIN-Nachrichten

Das Zahlungsmodul (PM) der Gemeinschaftsplattform nutzt den SWIFTNet FIN Y-Copy-Service[23] zur Verarbeitung sämtlicher Zahlungen innerhalb einer eigens dafür eingerichteten SWIFT Closed User Group (CUG). Das Zahlungsmodul erhält eine vollständige Kopie jeder Zahlung, um die Abwicklung sowie eine effiziente und umfassende Informationsbereitstellung im Informations- und Steuerungsmodul (Information and Control Module – ICM) zu ermöglichen.

SWIFT-FIN-Nachrichten können bis zu fünf TARGET2-Geschäftstage im Voraus eingereicht werden. In diesem Fall wird die Zahlungsnachricht bis zur Tagverarbeitung der Gemeinschaftsplattform gespeichert („warehoused payments“).

Nutzer, die über einen internetbasierten Zugang mit der Gemeinschaftsplattform verbunden sind, führen den Austausch von Nachrichten mit der SSP nicht über das SWIFT-Netzwerk durch, sondern sie können diese über ICM-Erfassungsmasken erfassen und anzeigen lassen. Eine Verbindung mit dem ICM für solche Nutzer ist nur im User-to-Application-Modus (U2A-Modus) möglich (siehe auch Abschnitt 3.1.7).

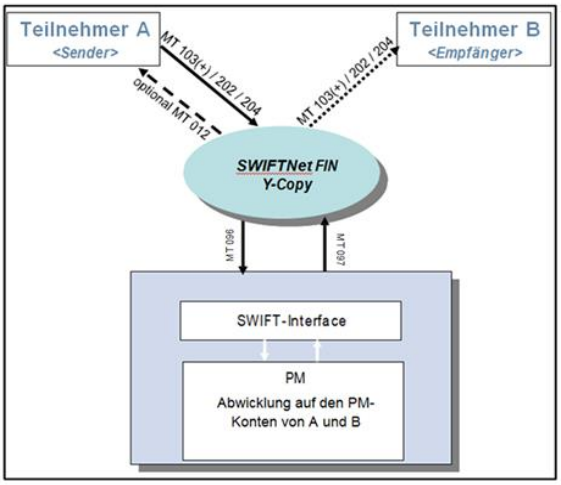


Abbildung 10: Transaktionsfluss in Y-Copy

23 Im HAM wird V-Shape genutzt.

In den TARGET2-UDFS, Buch 1 (siehe 9.1.2.1.1.3 SWIFTNet FIN messages – User header – „Structure when sending a message“ bzw. „Structure when receiving a message“) wird das Feld-Kennzeichen 113 „Banking priority“ erläutert. Wie dort erklärt, bleiben die dritte und die vierte Stelle des Feldes 113 ungenutzt (und werden von der Gemeinschaftsplattform nicht geprüft). TARGET2-Nutzer sollten die nationalen Vereinbarungen zur Verwendung des Feld-Kennzeichens kennen.

XML-Nachrichten

Ist ein Teilnehmer mit dem ICM, der TIPS GUI oder der T2S GUI im Application-to-Application-Modus (A2A-Modus) verbunden, werden SWIFTNet InterAct, SWIFTNet FileAct und SIA genutzt. Die verschiedenen Informations- und Steuerungsoptionen sind als XML-Nachrichten konzipiert.[24] SWIFTNet Browse ermöglicht die Initiierung eines InterAct- oder FileAct-Nachrichtenaustausches über eine sichere Browserverbindung.

SWIFTNet FileAct ermöglicht die Übermittlung von Dateien und wird in der Regel zum stapelweisen Austausch strukturierter Finanznachrichten und umfangreicher Berichte verwendet. SWIFTNet FileAct-Nachrichten werden während der Betriebszeiten des PM jederzeit angenommen, außer wenn die Gemeinschaftsplattform gewartet wird, während der Tagesende- und Tagesbeginn-Verarbeitung und auch nicht, wenn Liquidität bereitgestellt wird.

SWIFTNet InterAct ermöglicht die Übertragung von XML-Anfragen über das Secure IP Network (SIPN) durch SWIFT an das ICM und die Nebensystemschnittstelle (Ancillary System Interface – ASI). XML-Nachrichten werden für Anfragen und Antworten im Zusammenhang mit dem ICM (A2A-Modus) sowie für Geschäftsvorgänge der Nebensysteme genutzt. Die Nachrichten zu Geschäftsvorgängen der Nebensysteme werden wie in den TARGET2-UDFS, Buch 1 erläutert angenommen. Bei ICM-(A2A-)Vorgängen werden die Nachrichten entsprechend dem zugrunde liegenden Geschäftsvorfall angenommen. Während des SSP-Wartungsfensters werden keine SWIFTNet InterAct-Nachrichten angenommen.

Die gemeinsame Systemschnittstelle von TARGET2 und T2S verwendet ebenfalls XML-Nachrichten, die gemäß T2S-Anforderungen im Einklang mit der ISO 20022-Norm stehen. XML-Nachrichten, die von TARGET2-Nutzern im Rahmen der TARGET2-Standard- und -Zusatzleistungen für T2S verwendet werden, basieren ebenfalls auf demselben Standard, doch der Business Application Header ist nicht erforderlich. TIPS-Geldkontoinhaber, erreichbare Parteien (einschließlich der jeweiligen einreichenden Parteien) und T2S-Geldkontoinhaber, die direkt an T2S angebunden sind, müssen gemäß

24 Eine detaillierte Beschreibung der XML-Nachrichten findet sich in den UDFS, Buch 4.

den TIPS- bzw. T2S-Anforderungen auch den Nachrichtenstandard ISO 20022 anwenden.

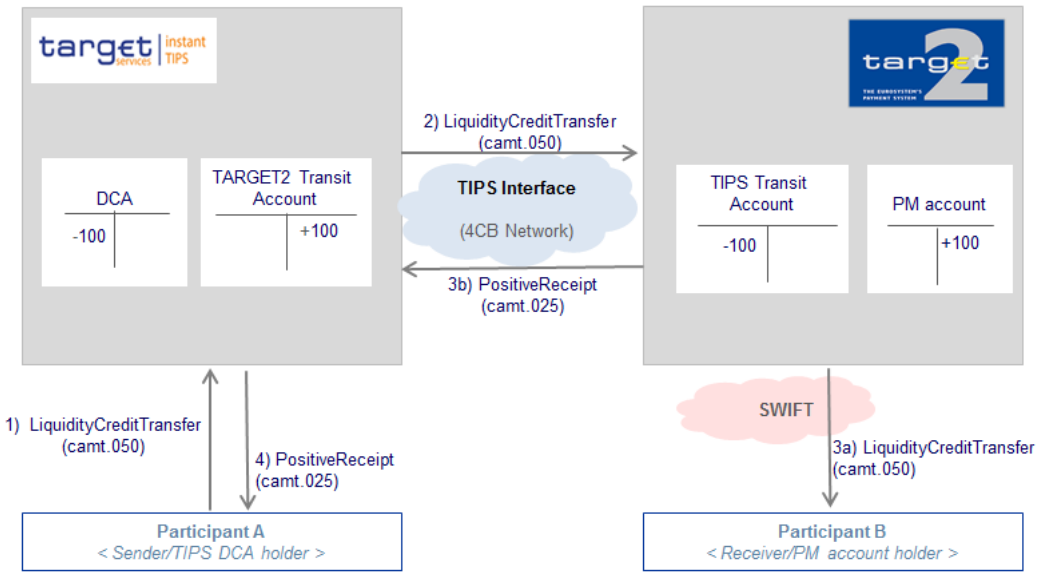


Abbildung 11: Liquiditätsübertragung von TIPS auf TARGET2 (ISO 20022-Nachrichtenströme)

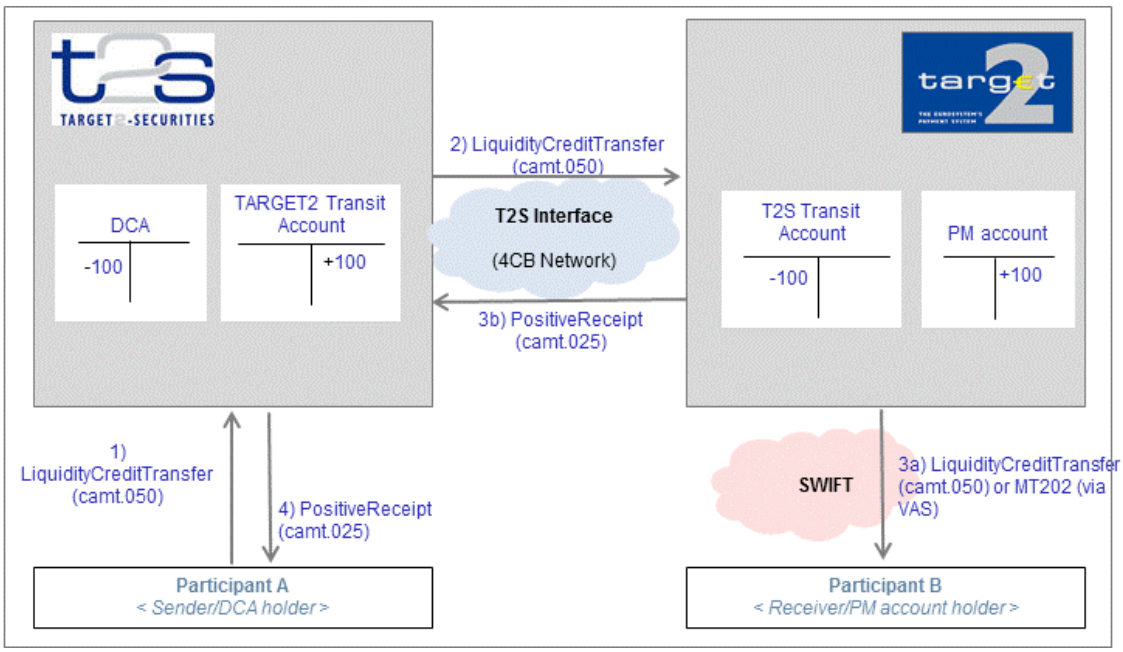


Abbildung 12: Liquiditätsübertragung von T2S auf TARGET2 (ISO 20022-Nachrichtenströme)

2.10 Abwicklung von Nebensystemen[25]

Nebensysteme können auf die Abwicklung innerhalb der SSP sowohl über die Standard-Teilnehmer-Schnittstelle (Participant Interface – PI) als auch über die Nebensystemschnittstelle (ASI) zugreifen. Im ersten Fall können Nebensysteme, die die Voraussetzungen für die Teilnahme als PM-Kontoinhaber erfüllen, die Systemfunktionalitäten wie jeder andere PM-Kontoinhaber nutzen. Insbesondere verfügen sie über ein PM-Konto auf der Plattform. Im zweiten Fall werden die Nebensysteme auf die Gemeinschaftsplattform über eine spezielle Schnittstelle (die ASI) zugreifen, die über eine Reihe spezifischer Merkmale verfügt, die eigens zur Ermöglichung der AS-Abwicklung konzipiert wurden, so z. B. die zentralisierte Steuerung der Autorisierung der Belastung eines bestimmten Kontos, die Nutzung von Mandated Payments, spezielle Abwicklungsverfahren, optionale Mechanismen und die Nutzung bestimmter Kontoarten (technische Konten, Spiegelkonten, Garantiekonten). Ein Nebensystem, das die ASI-Schnittstelle nutzt, kann bei Erfüllung der Teilnahmevoraussetzungen parallel dazu ein PM-Kontoinhaber werden und ein PM-Konto eröffnen. Es könnte somit die ASI für seine Abwicklungsaktivitäten und das PM-Konto für andere Zwecke verwenden. Um unterschiedliche Geschäftsfälle im Zusammenhang mit den verschiedenen Nebensystemen zu unterstützen, bietet das Zahlungsmodul über die ASI sechs generische Abwicklungsverfahren.

Abwicklungsverfahren[26]	**Beschreibung**
Verfahren 1 Liquiditätsübertragung	Liquiditätsübertragung zwischen einem Nebensystem-Teilnehmer und dem PM über ein Spiegelkonto. Die Verrechnung erfolgt im Nebensystem selbst.
Verfahren 2 Abwicklung in Echtzeit	Übertragung zwischen den Konten zweier PM-Kontoinhaber mit dem Ziel, eine im Nebensystem bereits ausgleichsfähige Transaktion endgültig abzuschließen.
Verfahren 3 Bilaterale Abwicklung	Das Nebensystem übermittelt dem PM Belastungen und Gutschriften gleichzeitig. Die beiden Transaktionen („credit leg“ und „debit leg“) werden unabhängig voneinander abgewickelt.
Verfahren 4 Multilaterale Standardabwicklung	Belastungen und Gutschriften werden gleichzeitig an das PM übermittelt. Erst wenn alle Belastungen erfolgreich verarbeitet wurden, werden die Gutschriften verbucht.
Verfahren 5 Simultan-multilaterale Abwicklung	Belastungen und Gutschriften werden gleichzeitig an das PM übermittelt. Sie werden jedoch sämtlich auf ihre Abwicklungsfähigkeit geprüft und können nur nach dem Grundsatz „alles oder nichts“ abgewickelt werden.
Verfahren 6	PM-Kontoinhaber dedizieren Liquidität zur Abwicklung der Nebensystem-

25 Weitere Einzelheiten finden sich in den UDFS, Buch 1, Kapitel 2.8.

26 Integriertes Modell: Die endgültige geldliche Verrechnung findet im Wertpapierabwicklungssystem selbst statt. Schnittstellen-Modell: Die endgültige geldliche Verrechnung findet im Zahlungsmodul statt.

Dedizierte Liquidität und systemübergreifende Abwicklung	Transaktionen entweder auf speziellen Unterkonten oder auf dem technischen Konto. Die Abwicklung erfolgt entweder auf den Unterkonten oder im Nebensystem selbst. Dieses Abwicklungsverfahren eignet sich besonders für das Nachtgeschäft, kann jedoch auch während des Tages verwendet werden.

Tabelle 4: Abwicklungsverfahren

Außerdem können die oben erwähnten obligatorischen Abwicklungsverfahren durch nachstehend aufgeführte Mechanismen den besonderen Bedürfnissen der einzelnen Nebensysteme angepasst werden:

- Informationsfrist zur Vorankündigung einer Abwicklung nach den AS-Verfahren 3, 4 und 5;
- Abwicklungszeitraum für den Saldenausgleich der Nebensysteme, um die Abwicklung anderer Geschäfte nicht zu behindern; sind die Nebensystem-Transaktionen am Ende dieses Zeitraums nicht abgewickelt, werden die entsprechenden Salden entweder zurückgewiesen oder es wird ein Garantiekonto-Verfahren aktiviert, sofern dies vom Nebensystem für die Verfahren 4 und 5 festgelegt wurde.
- Durch ein Garantiekonto-Verfahren wird die erforderliche zusätzliche Liquidität bereitgestellt, wenn Nebensystem-Transaktionen mit der vorhandenen Liquidität der Teilnehmer nicht abgewickelt werden können.
- Der festgelegte Zeitpunkt („scheduled time“) ist ein Mechanismus, der Nebensystem-Transaktionen bis zum festgelegten Abwicklungszeitpunkt speichert.

Nebensysteme, die die Abwicklungsverfahren 3, 4, 5 und 6 einsetzen, können SWIFTNet FileAct nutzen, um die Geldseite von AS-Transaktionen abzuwickeln. Für Abwicklungsverfahren 6 genutzte SWIFTNet FileAct-Nachrichten können grundsätzlich über die gesamte Öffnungszeit des Zahlungsmoduls hinweg verarbeitet werden, d. h. bis zum Annahmeschluss für Interbankzahlungen (18.00 Uhr) und ab dem Beginn der Nachtverarbeitung (19.30 Uhr), ausgenommen die für Wartungsarbeiten an der Gemeinschaftsplattform vorgesehenen Zeitfenster. Für Abwicklungsverfahren 3, 4, und 5 genutzte SWIFTNet FileAct-Nachrichten können während der Tagverarbeitung von 7.00 Uhr bis 18.00 Uhr verarbeitet werden.

3 Teilnahme

3.1 Teilnahme an TARGET2

3.1.1 Zugangskriterien

Das Eurosystem hat die allgemeine rechtliche Struktur und die Grundsätze für die Teilnahme an TARGET2 so gestaltet, dass die TARGET2-Nutzer entscheiden können, in welcher Form sie am System teilnehmen. Der Zugang zum TARGET2-System kann auf verschiedene Weise erfolgen: über die direkte oder eine indirekte Teilnahme, über „erreichbare BIC-Inhaber“[27] oder über den „Multi-Adressaten-Zugang“. Die TARGET2-Nutzer müssen die in Abschnitt 3.7 beschriebenen TARGET2-Sicherheitsanforderungen und -kontrollen erfüllen.

3.1.2 Direkte Teilnahme

Zugelassen für die direkte Teilnahme an TARGET2 sind:

a) Kreditinstitute, die ihren Sitz oder eine ihrer Zweigstellen im Europäischen Wirtschaftsraum (EWR) haben, auch wenn sie über eine im EWR ansässige Zweigstelle handeln

b) Kreditinstitute mit Sitz außerhalb des EWR, sofern sie über eine im EWR ansässige Zweigstelle handeln

c) NZBen der EU-Mitgliedstaaten und die EZB.

Die zuständige Zentralbank kann nach ihrem Ermessen darüber hinaus als direkte Teilnehmer zulassen:

a) (Haupt-)Kassen/(zentrale) Finanzabteilungen von Zentral- oder Regionalregierungen der EU-Mitgliedstaaten

b) öffentliche Stellen von EU-Mitgliedstaaten, die zur Führung von Kundenkonten berechtigt sind

c) Wertpapierfirmen mit Sitz in der EU oder im EWR, auch wenn sie über eine in der EU oder im EWR niedergelassene Zweigstelle handeln, sowie Wertpapierfirmen mit Sitz außerhalb des EWR, sofern sie über eine in der EU oder im EWR niedergelassene Zweigstelle handeln

d) Stellen, die Nebensysteme betreiben und in dieser Funktion handeln

e) Kreditinstitute oder Stellen der unter a) bis d) aufgeführten Art, sofern diese ihren Sitz in einem

[27] Der BIC (Business Identifier Code) ist die international am häufigsten verwendete Art der Identifizierung von Finanzinstituten. In seiner Funktion als ISO-Registrierungsstelle gibt SWIFT an Finanzinstitute und Nicht-Finanzinstitute, die an SWIFT angeschlossen sind, sowie an nicht angeschlossene Institute BICs aus. Der BIC wird für Finanztransaktionen, Datenbanken im Zusammenhang mit Kunden- und Geschäftspartnern, Compliance-Dokumente und sonstige Zwecke genutzt. Die BIC-Struktur basiert auf ISO 9362 (siehe SWIFT-Website).

Land haben, mit dem die Europäische Union eine Währungsvereinbarung getroffen hat, wonach solchen Stellen der Zugang zu Zahlungsverkehrssystemen in der Europäischen Union gestattet ist. Dies gilt nur nach Maßgabe der in der Währungsvereinbarung festgelegten Bedingungen und unter der Voraussetzung, dass die in dem betreffenden Land geltenden rechtlichen Regelungen den einschlägigen Rechtsvorschriften der Europäischen Union entsprechen.

Direkte Teilnehmer sind Stellen, die mindestens ein PM-Konto im Zahlungsmodul (Payment Module – PM) der Gemeinschaftsplattform (Single Shared Platform – SSP) unterhalten (PM-Kontoinhaber) und/oder über ein TIPS-Geldkonto auf der TIPS-Plattform und/oder ein T2S-Geldkonto auf der T2S-Plattform verfügen (TIPS-Geldkontoinhaber bzw. T2S-Geldkontoinhaber). Die PM-Kontoinhaber erhalten über SWIFT oder Internet Zugang zur Gemeinschaftsplattform (jeweils PM-Kontoinhaber mit SWIFT-basiertem Zugang oder PM-Kontoinhaber mit internetbasiertem Zugang). Für den internetbasierten Zugang gelten Sonderregeln, die in Abschnitt 3.1.7 erläutert werden.

Direkte Teilnehmer können:

a) Zahlungen direkt in die/aus der Gemeinschaftsplattform/TIPS-Plattform/T2S-Plattform einreichen/empfangen

b) Zahlungen direkt über ihre Zentralbank abwickeln

c) PM-Sonderkonten für nicht mit dem Zahlungsverkehr zusammenhängende Aktivitäten eröffnen (z. B. für die Erfüllung der Mindestreservepflicht). Diese Sonderkonten werden anhand eines separaten BIC11 identifiziert.

Darüber hinaus sind die PM-Kontoinhaber verantwortlich für alle über ihr Konto eingereichten Zahlungen an Stellen bzw. auf ihrem Konto empfangenen Zahlungen der Stellen, die über sie in TARGET2 registriert sind (indirekte Teilnehmer, Stellen mit Multi-Adressaten-Zugang und erreichbare BIC-Inhaber (siehe unten)).

Gemäß den TARGET2-Bedingungen der jeweiligen Zentralbank wird davon ausgegangen, dass die Teilnehmer Kenntnis von allen für sie geltenden Verpflichtungen aus Rechtsvorschriften zum Datenschutz sowie zur Verhinderung der Geldwäsche und der Terrorismusfinanzierung, proliferationsrelevanter nuklearer Tätigkeiten und der Entwicklung von Trägersystemen für Kernwaffen besitzen und diese erfüllen. Weitere Informationen zu diesen Verpflichtungen können die Teilnehmer den von der jeweiligen Zentralbank veröffentlichten Bedingungen entnehmen.

3.1.3 Indirekte Teilnahme

Kreditinstitute mit Sitz im EWR können jeweils mit (nur) einem PM-Kontoinhaber vertraglich vereinbaren, Zahlungsaufträge einzureichen und/oder Zahlungen zu empfangen, die über das PM-Konto dieses PM-Kontoinhabers verrechnet werden. Zentralbanken erkennen indirekte Teilnehmer durch deren Aufnahme in das TARGET2-Directory an.

Sofern ein PM-Kontoinhaber, bei dem es sich um ein Kreditinstitut handelt, und ein indirekter Teilnehmer derselben Gruppe angehören, kann der PM-Kontoinhaber dem indirekten Teilnehmer ausdrücklich gestatten, das PM-Konto unmittelbar zu nutzen, um im Wege des gruppenbezogenen Multi-Adressaten-Zugangs Zahlungsaufträge einzureichen und Zahlungen zu empfangen.

3.1.4 Multi-Adressaten-Zugang

PM-Kontoinhaber können ihre Zweigstellen oder ihrer Gruppe angehörende Kreditinstitute, die sich in EWR-Ländern befinden, bevollmächtigen, ohne die Mitwirkung des PM-Kontoinhabers Zahlungen über ihr Konto abzuwickeln, indem die Zahlungen direkt in die Gemeinschaftsplattform eingereicht bzw. über diese empfangen werden. Dies bietet den Niederlassungen von Banken oder Bankengruppen effiziente Mechanismen für das Liquiditätsmanagement und Zahlungsverkehrsgeschäft.

Der Multi-Adressaten-Zugang kann wie folgt gewährt werden:

a) Ein Kreditinstitut, das als PM-Kontoinhaber zugelassen wurde, kann einer oder mehreren seiner im EWR ansässigen Zweigstellen zur direkten Einreichung von Zahlungsaufträgen und/oder zum direkten Empfang von Zahlungen Zugang zu seinem PM-Konto gewähren, sofern die betreffende Zentralbank darüber informiert wurde.

b) Wurde eine Zweigstelle eines Kreditinstituts als PM-Kontoinhaber zugelassen, so haben auch die anderen Zweigstellen derselben juristischen Person und/oder die Zentrale – vorausgesetzt, sie sind im EWR ansässig – Zugang zum PM-Konto jener Zweigstelle, sofern die betreffende Zentralbank darüber informiert wurde.

In der Praxis kann eine Bank mit Multi-Adressaten-Zugang ihren Zahlungsverkehr über ihre eigene BIC-Adresse abwickeln. Die Zahlungen werden jedoch auf dem Konto ihres PM-Kontoinhabers verbucht.

3.1.5 Erreichbare BIC-Inhaber

Die erreichbaren BIC-Inhaber in TARGET2 unterliegen keinerlei Systemregelungen. Alle Korrespondenten und Zweigstellen eines PM-Kontoinhabers, die Inhaber eines BIC sind, können unabhängig von ihrem Sitz in das TARGET2-Directory aufgenommen werden. Darüber hinaus wurden vom Eurosystem für diese erreichbaren BIC-Inhaber keine finanziellen oder administrativen Kriterien

ausgearbeitet, sodass die Festlegung einer Vermarktungsstrategie für diesen Status dem PM-Kontoinhaber obliegt. Der PM-Kontoinhaber ist dafür verantwortlich, die für die Aufnahme in das TARGET2-Directory relevanten Informationen an die betreffende Zentralbank weiterzuleiten.

Zahlungsaufträge von/an erreichbare(n) BIC-Inhaber(n) werden immer über einen PM-Kontoinhaber eingereicht bzw. empfangen. Ihre Zahlungen werden über das Konto des PM-Kontoinhabers im Zahlungsmodul der Gemeinschaftsplattform abgewickelt.

		Konto	Einreichung/ Empfang von Zahlungen	Zahlungs-abwicklung	Unterliegt System-regelungen	Aufgeführt im TARGET2-Directory
Direkte Teilnahme	**PM-Konto-inhaber**	PM-Konto	Direkt	Eigenes Konto im PM	Ja	Ja
	TIPS-Geldkonto-inhaber	TIPS-Geldkonto	Direkt	Eigenes Konto auf der TIPS-Plattform	Ja	Nein
	T2S-Geldkonto-inhaber	T2S-Geldkonto	Direkt	Eigenes Konto auf der T2S-Plattform	Ja	Nein
Multi-Adressaten-Zugang		Kein Konto	Direkt	Konto des direkten Teilnehmers	Ja	Ja
Indirekte Teilnahme		Kein Konto	Über den direkten Teilnehmer	Konto des direkten Teilnehmers	Ja	Ja
Erreichbare BIC-Inhaber		Kein Konto	Über den direkten Teilnehmer	Konto des direkten Teilnehmers	Nein	Ja

Tabelle 5: TARGET2-Teilnahmestruktur

3.1.6 Kontengruppe

Den Status „Kontengruppe“ können verschiedene Kategorien von Instituten erlangen:

Kategorie 1: Kreditinstitute, die gemäß den International Accounting Standards (IAS 27) konsolidieren,

Kategorie 2: Kreditinstitute, die nicht oder gemäß anderen Standards konsolidieren, welche jedoch der im IAS 27 enthaltenen Definition entsprechen,

Kategorie 3: bilaterale und multilaterale Netzwerke von Sparkassen und Genossenschaftsbanken, für die satzungsmäßige Regelungen/Kooperationsregelungen gelten, die die nationalen rechtlichen Anforderungen erfüllen.

Dementsprechend wird bei einem Antrag auf Anerkennung des Gruppenstatus folgendermaßen verfahren:

Kategorie 1: Einreichung eines Auszugs aus dem offiziellen konsolidierten Jahresabschluss oder einer beglaubigten Erklärung eines externen Revisors, worin angegeben ist, welche Stellen in die Konsolidierung einbezogen sind.

Kategorie 2: Einreichung einer Erklärung eines externen Revisors, die gegenüber der NZB darlegt, dass die Konsolidierung dem IAS 27 entspricht.

Kategorie 3: Die NZB erstellt zunächst eine Beurteilung, in der dargelegt wird, dass die „Gruppe" mit den nationalen rechtlichen Anforderungen und/oder dem rechtlichen Rahmen im Einklang steht, und dass sie die im TARGET2-Rechtsrahmen festgelegten politischen Vorgaben erfüllt. Darüber hinaus muss der EZB-Rat dem Antrag auf Anerkennung als Gruppe zustimmen.

3.1.7 Internetbasierter Zugang

Der internetbasierte Zugang zu TARGET2 stellt eine alternative Art der Verbindung mit der Gemeinschaftsplattform dar, die einen direkten Zugriff auf die wichtigsten TARGET2-Dienstleistungen bietet,[28] ohne dass eine Verbindung mit dem SWIFT-Netzwerk erforderlich ist. Dementsprechend senden und erhalten Teilnehmer mit internetbasiertem Zugang keine Nachrichten über das SWIFT-Netzwerk, sondern verwenden das ICM, um Zahlungen über die SSP zu veranlassen und Informationen über eingehende Zahlungen sowie Kontoauszüge zu erhalten.

Der internetbasierte Zugang unterstützt folgende Funktionen:

- Überwachung eines PM-Kontos über das ICM, einschließlich der Bereitstellung von Online-Informationen über ein- und ausgehende Zahlungen (final oder schwebend) sowie über die Verrechnung von Nebensystemen und Liquiditätspositionen,
- Erstellung von Überweisungen über spezielle ICM-Erfassungsmasken, einschließlich MT 103/MT 103 STP, MT 202/MT 202 COV und Liquiditätsübertragungen an Teilnehmer mit SWIFT-basiertem oder internetbasiertem Zugang,
- Anzeige eingehender Überweisungen von Teilnehmern mit SWIFT-basiertem Zugang oder internetbasiertem Zugang, einschließlich MT 103/MT 103 STP, MT 202/MT 202 COV und Liquiditätsübertragungen, sowie MT 204 von Teilnehmern mit SWIFT-basiertem Zugang,
- Anzeige von Benachrichtigungen, Informationen und Tagesabschlussnachrichten über das ICM. Am Beginn des nächsten Geschäftstags kann ein Kontoauszug heruntergeladen werden.

[28] Teilnehmer können über einen internetbasierten Zugang auf ein PM-Konto oder ein HAM-Konto zugreifen.

- Verwaltung von Limiten und Reservierungen; Verwaltung von in der Warteschlange stehenden Aufträgen, einschließlich der Änderung von Prioritäten, der Umsortierung von Zahlungsaufträgen, der Änderung von Ausführungsfristen und der Stornierung von Zahlungen in der Warteschlange,
- Abwicklung der Position eines Teilnehmers innerhalb der Verrechnung eines Nebensystems, einschließlich AS-Abwicklungsverfahren 6, für das Unterkonten eröffnet werden können,
- Abwicklung von Zahlungen im Rahmen von Offenmarktgeschäften des Eurosystems,
- Online-Einsicht in das TARGET2-Directory.

Dabei ist Folgendes zu beachten:

- PM-Kontoinhaber mit internetbasiertem Zugang können nur im User-to-Application-Modus (U2A-Modus) auf das ICM zugreifen.
- Im Fall von Kontengruppen, Multi-Adressaten-Zugängen oder erreichbaren BIC-Inhabern ist die Verwendung eines internetbasierten PM-Kontos nicht möglich.
- Teilnehmer mit internetbasiertem Zugang haben keinen Zugriff auf TIPS-Informationen und können keine Daueraufträge oder laufenden Aufträge zur Liquiditätsübertragung an TIPS initiieren.
- Teilnehmer mit internetbasiertem Zugang können nicht zum Inhaber des verknüpften PM-Kontos (LM-Link) bestimmt werden.
- Einem PM-Kontoinhaber mit internetbasiertem Zugang stehen die TARGET2-Zusatzleistungen für T2S nicht zur Verfügung.
- Ein PM-Kontoinhaber mit internetbasiertem Zugang kann nicht zum Inhaber des PM-Hauptkontos für ein T2S-Geldkonto bestimmt werden.
- Aus Sicherheitsgründen steht zwischen 22.00 Uhr und 6.30 Uhr keine Internetverbindung zur Verfügung. Darüber hinaus können von 19.30 Uhr bis 22.00 Uhr sowie zwischen 6.30 Uhr und 6.45 Uhr – mit Ausnahme von Liquiditätsübertragungen – keine Zahlungen getätigt werden.

3.2 Teilnahme an TIPS – in Euro

In diesem Abschnitt werden die verschiedenen Arten der Teilnahme an TIPS beschrieben.

Inhaber von TIPS-Geldkonten

TIPS-Geldkontoinhaber müssen dieselben allgemeinen Voraussetzungen wie für eine Teilnahme an TARGET2 erfüllen. Sie müssen die Vorgaben des SEPA Instant Credit Transfer (SCT^{Inst}) Scheme einhalten.

Sie lassen sich anhand eines BIC11 in TIPS identifizieren und unterhalten TIPS-Geldkonten, die von ihrer zuständigen Zentralbank eröffnet und zur Abwicklung von Instant-Zahlungen, positiven Rückruf-Antworten und Liquiditätsübertragungen genutzt werden. TIPS-Geldkontoinhaber können die mit ihrem TIPS-Geldkonto verbundenen Credit Memorandum Balances (CMBs) sowie die Berechtigungen einreichender Parteien, die in ihrem Auftrag oder im Auftrag erreichbarer Parteien handeln, welche als Nutzer ihrer Konten oder CMBs definiert wurden, festlegen und verwalten. Sie können auch als einreichende Parteien für andere TIPS-Akteure fungieren.

Kontoinhaber von TIPS ASTAs

Die Voraussetzungen für die Eröffnung eines TIPS ASTA sind in der TARGET2-Leitlinie dargelegt.

TIPS ASTAs werden von der zuständigen Zentralbank auf Ersuchen eines Nebensystems eröffnet, das Instant Payments durchführt (TIPS-Nebensystem). Über TIPS ASTAs können Instant Payments, positive Rückruf-Antworten und serviceinterne Liquiditätsübertragungen abgewickelt sowie die von den Nebensystemteilnehmern zur Deckung ihrer Position in den Büchern des Nebensystems bereitgestellten Beträge gesammelt werden.

Kontoinhaber von TIPS ASTAs können Folgendes festlegen und verwalten:

a. Credit Memorandum Balances (CMBs) für ihre eigenen Konten und damit verbundene Limits
b. erreichbare Parteien, d. h. die berechtigten Nutzer ihrer Konten oder CMBs
c. die Konfiguration von einreichenden Parteien, die im eigenen Auftrag handeln

Erreichbare Parteien sind ebenfalls über einen BIC11 identifizierbar, verfügen jedoch über kein TIPS-Geldkonto und können Zahlungen in TIPS nur über das Konto eines TIPS-Geldkontoinhabers abwickeln. Sie können auch als einreichende Parteien auftreten. In diesem Fall können sie direkt mit TIPS interagieren. Erreichbare Parteien müssen das SCT^{Inst} Scheme einhalten.

Neben den beiden bereits erwähnten Teilnahmearten gibt es **einreichende Parteien**. Diese wurden von TIPS-Geldkontoinhabern oder erreichbaren Parteien dazu ermächtigt, in deren Namen Instant-Zahlungen an TIPS zu senden oder aus TIPS zu empfangen. Aus technischer Sicht sind einreichende Parteien sogenannte Distinguished Names, die an TIPS-Geldkontoinhaber und/oder erreichbare Parteien gekoppelt sind.

Zentralbanken können ebenfalls zu eigenen Zwecken TIPS-Geldkonten eröffnen. Sie sind in jedem Fall verantwortlich für die Pflege der Stammdaten der in ihren Zuständigkeitsbereich fallenden Bankengemeinschaft und können in Contingency-Situationen im Auftrag ihrer registrierten Teilnehmer handeln (z. B. Liquiditätsübertragungen einreichen).

Seit der Einführung des Mobile Proxy Lookup (MPL) in TIPS werden Parteien, die TIPS aktiv nutzen (d. h. TIPS-Teilnehmer und erreichbare Parteien in TIPS), automatisch auch als **aktive MPL-Nutzer** erachtet. Überdies ist es technisch möglich, Parteien nur als MPL-Akteure zu definieren, sofern sie TIPS nicht aktiv verwenden wollen.[29]

3.3 Teilnahme an T2S (T2S-Geldkontoinhaber)

T2S-Geldkontoinhaber (auch Payment Banks genannt) besitzen ein Geldkonto in T2S, das sie zur Abwicklung der Geldseite (cash leg) wertpapierbezogener Transaktionen verwenden und das zum Zwecke der Disposition mit einem PM-Konto verbunden ist. Wie TIPS-Geldkontoinhaber müssen auch T2S-Geldkontoinhaber dieselben Kriterien wie für eine Teilnahme an TARGET2 erfüllen. Technisch können T2S-Geldkontoinhaber auf folgende Weise eine Verbindung mit T2S herstellen (und mit T2S interagieren):

- direkt (als Directly Connected Parties – DCPs) über einen Anbieter von Mehrwertnetzwerkdiensten oder
- indirekt (als Indirectly Connected Parties – ICPs); in diesem Fall sind sie auf die Schnittstelle für Zusatzleistungen in TARGET2 angewiesen.

3.4 Konnektivitätsprozess

3.4.1 Anbindung an die Gemeinschaftsplattform von TARGET2

Zur Einrichtung einer Verbindung zur SSP müssen sich PM-Kontoinhaber, die einen SWIFT-basierten Zugang haben möchten, bei SWIFT, und um einen internetbasierten Zugang zu erhalten, bei einer akkreditierten Zertifizierungsstelle registrieren.

[29] Gemäß dem Beschluss des Market Infrastructure Board (MIB) ist die MPL-Nutzung zunächst auf die TIPS-Akteure beschränkt (siehe MIB-19-02-017).

Bei PM-Kontoinhabern mit internetbasiertem Zugang sollte die Registrierung bei einer akkreditierten Zertifizierungsstelle entsprechend den im „User manual internet access for the public key certification service“ (Benutzerhandbuch zur Public-Key-Zertifizierung für den Internetzugang) spezifizierten Verfahren durchgeführt werden. Das Benutzerhandbuch ist auf der TARGET2-Website der Bundesbank verfügbar.

Durch die Registrierung bei SWIFT können PM-Kontoinhaber mit SWIFT-basiertem Zugang die geeigneten SWIFT-Dienste für TARGET2 in Anspruch nehmen. Die Registrierung geschieht über ein von SWIFT entwickeltes, auf TARGET2 zugeschnittenes elektronisches Formular auf der SWIFT-Website (sog. „E-Ordering“), wobei die Aktualisierung der Angaben im BIC-Directory nur einmal pro Monat erfolgt. Im Rahmen des E-Ordering müssen alle Anmeldeanträge zunächst durch die Zentralbanken validiert und genehmigt werden und danach die Zustimmung durch den SSP Service Desk erhalten. Das gesamte Verfahren einschließlich Validierung und Umsetzung durch SWIFT kann zwei bis fünf Wochen in Anspruch nehmen. Zur Gewährleistung übereinstimmender Stammdaten bei SWIFT und auf der SSP sollten PM-Kontoinhaber bei Änderungen jeglicher Art – insbesondere im Bereich der Message Routing Rules (MRR) – vorzugsweise die E-Ordering-Funktion auf www.swift.com nutzen. Verwendet der PM-Kontoinhaber hierzu „myswift.com“, also eine SWIFT Customer Relationship Management Website, sollte die Änderung mit der Zentralbank abgesprochen werden. Die Zentralbank ist vor dem Umsetzungsdatum zu informieren. Weitere Informationen zur Registrierung bei SWIFT stehen auf www.swift.com zur Verfügung.

Zusätzlich zur Registrierung bei SWIFT benötigen PM-Kontoinhaber mit SWIFT-basiertem Zugang eine RMA-Autorisierung mit TRGTXEPM, Inhaber von HAM-Konten eine mit TRGTXEHM, der Co-Manager von HAM-Konten eine mit TRGTXEPM und TRGTXEHM und Zentralbankkunden eine mit TRGTXECB. Dieser Schritt ist für alle PM- und HAM-Kontoinhaber sowie für Zentralbankkunden obligatorisch.

3.4.2 Anbindung an die TIPS-Plattform und an das CRDM über das ESMIG

Der gemeinsame Zugangspunkt für die externe Kommunikation mit TIPS, das gemeinsame Referenzdatenmanagement (CRDM) und den Mobile Proxy Lookup Service (MPL-Service) in TIPS ist das Eurosystem Single Market Infrastructure Gateway (ESMIG). Um eine Verbindung mit dem ESMIG herzustellen, müssen die TIPS-Akteure mindestens einen TIPS-Netzwerkdienstleister auswählen.

Generell stellt der TIPS-Netzwerkdienstleister folgende Leistungen zur Verfügung:

- Netzwerkkonnektivität
- Nachrichtendienste im U2A- und A2A-Modus
- Verwaltung der Public Key Infrastructure (PKI) und der Closed Group of Users (CGU)
- Support und Störungsbehebung

Aus der Perspektive von TIPS ist das **ESMIG** für den A2A- und U2A-Datenverkehr verantwortlich. Es führt grundlegende Prüfungen der eingehenden Nachrichten durch und leitet sie an TIPS weiter. Ebenso übernimmt das ESMIG das Routing der von TIPS ausgehenden Nachrichten an den jeweiligen TIPS-Netzwerkdienstleister. Sämtlicher Nachrichtenverkehr zwischen dem ESMIG und ESMIG-Beteiligten basiert auf XML-Technologie und erfüllt, sofern nötig, den ISO 20022-Standard.

Jeder TIPS-Akteur ist durch einen Distinguished Name identifizierbar (dabei handelt es sich um eine Abfolge von durch Kommata abgetrennte Attribut-Wert-Beziehungen, die eindeutig mit digitalen Zertifikaten verbunden sind), der den individuellen Nutzern (die im U2A-Modus mit TIPS interagieren) oder Anwendungen (die im A2A-Modus mit TIPS interagieren) zugewiesen wird. Die Zertifikate werden von jedem TIPS-Netzwerkdienstleister ausgegeben. Für jeden Antrag, der im U2A- oder A2A-Modus an TIPS übermittelt wird, nimmt der zuständige TIPS-Netzwerkdienstleister eine Authentifizierungsprüfung des Absenders auf Netzwerkinfrastrukturebene vor. Ist die Authentifizierung erfolgreich, leitet der TIPS-Netzwerkdienstleister den Antrag und den Distinguished Name des Absenders an das ESMIG weiter.

Das **CRDM** ermöglicht die Erstellung und Pflege gemeinsamer Referenzdaten für die Konfiguration von Daten im Zusammenhang mit Parteien, Geldkonten, Regeln und Parametern über die CRDM GUI. Stammdaten aus dem CRDM können an andere Dienste wie TIPS weitergegeben werden. Alle Arten von CRDM-Nutzern haben Zugriff auf das gemeinsame Datenmanagement. Je nach ihrem Datenbereich erstreckt sich der Zugang auf unterschiedliche Funktionen und Daten. Zusätzlich ist es mithilfe eines Datenmigrationstools (DMT) möglich, TIPS-Referenzdaten in das CRDM einzugeben.

Zu beachten ist, dass **Informationen, die im CRDM gespeichert werden, allen Teilnehmern des Systems zugänglich sind**. Mit Verweis auf die DSGVO (siehe Abschnitt 12), in der festgelegt ist, wie personenbezogene Daten zu nutzen, zu verarbeiten und zu speichern sind, wird daher davon abgeraten, personenbezogene Daten in das CRDM aufzunehmen. Werden diese Felder dennoch ausgefüllt, so sollten sie ausschließlich nicht personenbezogene Angaben enthalten (z. B. allgemeine Telefonnummern von juristischen Personen usw.).

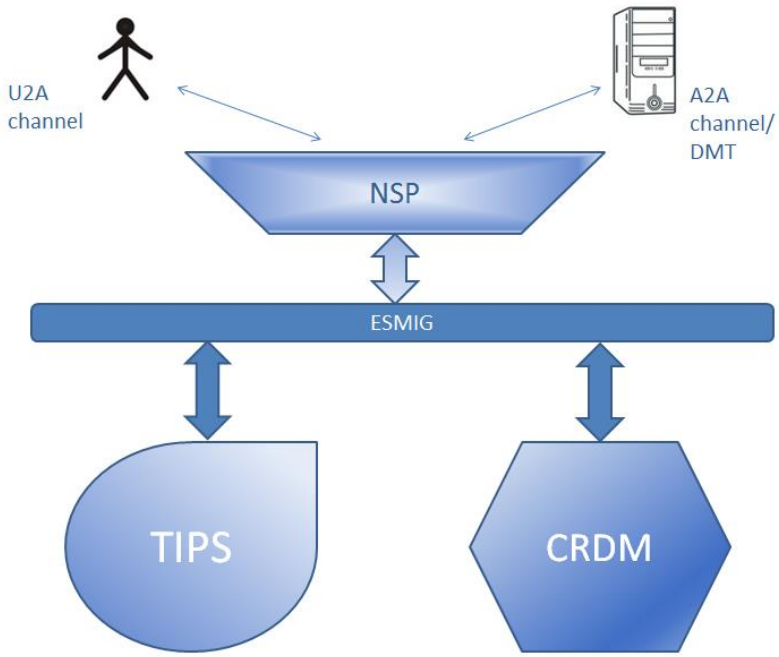


Abbildung 13: Anbindung an die TIPS-Plattform und an das CRDM über das ESMIG

3.4.3 Anbindung an die T2S-Plattform

Zur Einrichtung einer direkten Verbindung zur T2S-Plattform müssen die T2S-Geldkontoinhaber (**direkt angeschlossene T2S-Geldkontoinhaber**) einen[30] für T2S lizenzierten Anbieter von Mehrwertnetzwerkdiensten auswählen und die T2S-Verbindungsdienste über die VA-NSP-Website abonnieren. Der Antrag muss zunächst von der Zentralbank und danach vom T2S Service Desk geprüft und genehmigt werden. Der T2S-Geldkontoinhaber wird per E-Mail über jede sich in Bezug auf den Status des Antrags ergebende Änderung informiert. Bei Ablehnung des Antrags wird der jeweilige Grund genannt. Bei Annahme des Antrags erfolgt nach Festlegung des Umsetzungsdatums eine abschließende Bestätigung. Am Umsetzungsdatum stellt der Anbieter der Mehrwertnetzwerkdienste die Dienstleistungen in der beantragten Form bereit und übermittelt dem T2S-Geldkontoinhaber eine abschließende Bestätigung.

Dabei ist Folgendes zu beachten: Ist ein T2S-Geldkontoinhaber auch Kunde eines Zentralverwahrers oder einer anderen Zentralbank, so muss dieser Schritt nur einmal durchgeführt werden. Auf Anfrage kann der T2S Service Desk einer Zentralbank mitteilen, ob der T2S-Geldkontoinhaber bereits für die T2S-Verbindungsdienste registriert ist oder nicht.

[30] Direkt angeschlossene T2S-Geldkontoinhaber können beide Netzdienstanbieter in Anspruch nehmen, z. B. aus Gründen der Business Continuity.

Zusätzlich zu den T2S-Verbindungsdiensten sollte der T2S-Geldkontoinhaber beim Anbieter der Mehrwertnetzwerkdienste auch die Ausstellung digitaler Zertifikate für Authentifizierungs- und Signaturzwecke beantragen. Diese Zertifikate können auf USB-Token für den U2A-Zugriff durch Endnutzer oder auf dem Hardware-Sicherheitsmodul (HSM) für den A2A-Zugriff durch Anwendungen zur Verfügung gestellt werden.

Weitere Informationen finden sich in der VA-NSP-Dokumentation und in den folgenden Dokumenten: T2S Connectivity Licences and Licence Agreement und T2S Connectivity Guide.

Bei **indirekt angeschlossenen T2S-Geldkontoinhabern** ist keine Registrierung über einen Anbieter von Mehrwertnetzwerkdiensten erforderlich. Es reicht aus, wenn der Inhaber des PM-Hauptkontos die TARGET2-Zusatzleistungen für T2S anhand der SSP-Registrierungsformulare abonniert (siehe Abschnitt unten).

3.5 Erhebung von Stammdaten

Jeder Nutzer muss der Zentralbank seine Stammdaten zur Verfügung stellen. An die Gemeinschaftsplattform angebundene Nutzer verwenden hierzu die SSP-Formulare, TIPS-Geldkontoinhaber verwenden die TIPS-Formulare, und T2S-Geldkontoinhaber die entsprechenden T2S-Formulare. Die Formulare können die Nutzer auf dem mit ihrer Zentralbank vereinbarten Weg beim jeweiligen National Service Desk einreichen.

Die Zentralbanken geben die Formularangaben der an die Gemeinschaftsplattform angebundenen Nutzer über das ICM, die Angaben der TIPS-Geldkontoinhaber über das CRDM, und die Angaben der T2S-Geldkontoinhaber über die T2S GUI ein.[31]

Aus verfahrenstechnischer Sicht sind vier Schritte einzuhalten:

- **Analyse**

Der Nutzer analysiert im Rahmen seines Change-Management-Verfahrens die nötigen Änderungen und füllt die entsprechenden Formulare aus, die anschließend der betreffenden Zentralbank übermittelt werden.

Änderungen an den Stammdaten nimmt der Nutzer überwiegend in eigener Regie vor. Er definiert seine Anforderungen, wobei er vielfach mit SWIFT und/oder dem TIPS-Netzwerkdienstleister und/oder dem Anbieter von Mehrwertnetzwerkdiensten und/oder der Zentralbank in Kontakt steht, um sich über die Durchführbarkeit zu informieren. Vor allem bei komplexen Änderungen ist eine vorherige

[31] Weitere Informationen und ausführliche Erläuterungen zu den Formularen sind dem Dokument „Reference and static data registration user guide“ zu entnehmen.

Kommunikation mit der Zentralbank notwendig. Dabei sollten die Nutzer mit der Darstellung ihrer geplanten Änderung beginnen. Die Dauer der Analyse hängt von der Organisation des Nutzers ab.

Der Nutzer übermittelt seiner Zentralbank die Registrierungsformulare und gegebenenfalls:

- eine Darstellung der Änderung und des Verfahrens (z. B. Kontokonfiguration, technische Änderungen, Bedarf an spezifischen Tests und Support),
- eine einschlägige Rechtsdokumentation (z. B. Ländergutachten),
- eine technische Dokumentation (z. B. zur Ausfallsicherheit).

- **Bewertung und Validierung**

Im Falle umfangreicher Änderungen sollte die zuständige Zentralbank in die oben beschriebene Analyse einbezogen werden. Diese prüft die Formulare in rechtlicher und technischer Hinsicht nach Maßgabe ihrer nationalen Bestimmungen. Ferner kontrolliert die Zentralbank, ob die Registrierung bei SWIFT/beim TIPS-Netzwerkdienstleister/beim Anbieter von Mehrwertnetzwerkdiensten mit den Angaben in den Stammdatenformularen übereinstimmt.

Die Prüfungen durch die Zentralbank zielen auf die Gewährleistung der rechtlichen und operationellen Sicherheit des gesamten TARGET2-Systems ab.

Die Zentralbank muss überprüfen, ob die Nutzerzertifizierung unter den neuen Voraussetzungen noch gültig ist. Andernfalls muss eine neue Zertifizierungsphase (die inhaltlich vom gegenwärtigen Zertifizierungsstatus und der Art der anstehenden Änderung abhängt) geplant[32] und erfolgreich durchgeführt werden. Ein Nutzer kann zudem beantragen, dass zunächst in der Testumgebung getestet wird, bevor der Live-Betrieb erfolgt. Die Prüfungen umfassen auch die Validierung der Registrierungsformulare.

Abschließend validiert die Zentralbank den Antrag oder lehnt ihn ab.

- **Durchführung der Stammdatenerhebung**

Nach der Validierung gibt die Zentralbank die Angaben aus den Formularen über das ICM, die CRDM GUI für TIPS und/oder die T2S GUI ein. Ergeben sich Auswirkungen auf das TARGET2-Directory, ist die Frist für dessen wöchentliche Aktualisierung zu berücksichtigen.

TIPS-Änderungen im CRDM, die am nächsten Geschäftstag aktiviert werden sollen, müssen vor dem Annahmeschluss um 17.00 Uhr eingegeben werden.

32 Je nach Änderung kann es sein, dass die geplante Modifizierung auch im Testumfeld vorgenommen werden muss.

- **Abschließende Prüfung**

Anhand des ICM, der CRDM GUI oder der T2S GUI sollte der betreffende Nutzer die Richtigkeit des neuen Stammdateneintrags/der Änderung überprüfen.

3.5.1 Konfliktäre Registrierung von erreichbaren BIC-Inhabern und indirekten Teilnehmern

Das TARGET2-Directory erlaubt pro BIC[33] lediglich eine Anmeldung und nur eine Beziehung zwischen einem erreichbaren BIC-Inhaber/indirekten Teilnehmer und dem PM-Kontoinhaber, der den Zugang zu TARGET2 ermöglicht. Aus diesem Grund ist es möglich, dass zwei oder mehrere Teilnehmer konfliktäre Registrierungsformulare an ihre Zentralbank senden. Daher sollten die Banken, bevor sie ein Registrierungsformular an ihre Zentralbank schicken, um einen erreichbaren BIC-Inhaber zu registrieren, im TARGET2-Directory nachprüfen, ob der BIC, mit dem sie den erreichbaren BIC-Inhaber/indirekten Teilnehmer anmelden möchten, bereits bei einem anderen PM-Kontoinhaber registriert wurde.

Ist der erreichbare BIC-Inhaber/indirekte Teilnehmer (Bank X) schon im TARGET2-Directory bei einem anderen PM-Kontoinhaber B registriert, muss sich der antragstellende PM-Kontoinhaber A mit dem anderen PM-Kontoinhaber B in Verbindung setzen, um diesen darüber zu informieren, dass sich die Routing-Anweisungen für den erreichbaren BIC-Inhaber/indirekten Teilnehmer (Bank X) ändern werden.

Der PM-Kontoinhaber B, über den gegenwärtig die Verbindung der Bank X besteht, muss dann ein Formular ausfüllen und die Löschung der bestehenden Registrierung beantragen. Dieses Formular reicht er bei seiner Zentralbank und dem PM-Kontoinhaber A ein.

Der PM-Kontoinhaber A leitet daraufhin sein eigenes Formular für die Registrierung des erreichbaren BIC-Inhabers/indirekten Teilnehmers (Bank X) mit einer Kopie des vom anderen PM-Kontoinhaber B unterzeichneten Formulars für die Aufhebung der früheren Verbindung an seine Zentralbank weiter.

Falls der erreichbare BIC-Inhaber/indirekte Teilnehmer zu dem Zeitpunkt, zu dem der PM-Kontoinhaber die Überprüfung durchführt, nicht im TARGET2-Directory aufgeführt ist, aber in der gleichen Woche ein anderer PM-Kontoinhaber die Anmeldung desselben BIC-Inhabers als erreichbaren BIC-Inhaber/indirekten Teilnehmer beantragt, wird einer der Zentralbankanträge abgelehnt. Die betreffende Zentralbank muss dann die Banken von den konfliktären Registrierungsaufträgen in Kenntnis setzen. Es obliegt den Banken, eine Vereinbarung zu erzielen, welche Bank der PM-Kontoinhaber sein soll, der den Korrespondenten vertritt.

[33] BIC mit elf Stellen.

3.5.2 Directorys

3.5.2.1 TARGET2-Directory

Das TARGET2-Directory unterstützt das Routing von Zahlungsaufträgen. Es verwendet mit SWIFT zusammenhängende Informationen in Verbindung mit TARGET2-spezifischen Informationen, die die PM-Kontoinhaber im Rahmen der SSP-Registrierung bereitstellen. Das TARGET2-Directory ist die Datenbank, der die BICs für das Routing von Zahlungsaufträgen entnommen werden können.

Sofern vom TARGET2-Nutzer nicht anders gewünscht, werden die BICs im TARGET2-Directory veröffentlicht.[34]

Der Inhalt des TARGET2-Directory basiert auf den Stammdaten der Gemeinschaftsplattform, wie sie bei den PM-Kontoinhabern mittels dafür vorgesehener Formulare erhoben wurden. Diese Formulare werden von den PM-Kontoinhabern verwendet, um die Eröffnung ihres Kontos/ihrer Konten zu beantragen und alle anderen vom System benötigten Informationen einzuholen. Der PM-Kontoinhaber ist insbesondere für die Anmeldung seiner indirekten Teilnehmer, Stellen mit Multi-Adressaten-Zugang oder erreichbaren BIC-Inhaber verantwortlich und für alle dabei auftretenden Fehler oder missbräuchlichen Verwendungen haftbar.

Das TARGET2-Directory enthält Informationen zu allen Kreditinstituten, die über TARGET2 erreicht werden können. Es enthält außer dem BIC des Teilnehmers auch den BIC des Empfängers (d. h. den BIC, der zum Empfang und zum Versand von Zahlungen verwendet wird), des Kontoinhabers (d. h. den BIC des PM-Kontos), den Namen des Instituts, die Anschrift sowie die nationale Bankleitzahl (sofern vorhanden). Die folgende Tabelle ist ein Beispiel für einen Eintrag eines PM-Kontoinhabers im TARGET2-Directory:

Feld im TARGET2-Directory	Beispiel
BIC	BANKBEBBXXX
Addressee	BANKBEBBXXX
Account holder	BANKBEBBXXX
Institution name	Bank S.A. Brussels
City heading	Brussels
National sorting code	-
Main BIC flag	Yes
Type of change	A

[34] Die nicht im TARGET2-Directory veröffentlichten BICs werden jedoch im BIC-Directory von SWIFT publiziert.

Valid from	20080218
Valid until	99991231
Type of participation	01

Tabelle 6: TARGET2-Directory

Das TARGET2-Directory wird nur an PM-Kontoinhaber ausgegeben.[35] Die Verteilung erfolgt über SWIFTNet FileAct (für das gesamte Directory nur im „Pull"-Modus, für Aktualisierungen im „Pull"- und „Push"-Modus). Das Herunterladen des gesamten Inhalts ist in erster Linie für das erste Laden des Directory oder für den Fall vorgesehen, dass eine Wiederherstellung des Directory erforderlich ist. Aufgrund der Dateigröße wird eine Komprimierung nachdrücklich empfohlen. Des Weiteren können PM-Kontoinhaber das TARGET2-Directory zentral herunterladen und es intern verteilen. Sie dürfen das TARGET2-Directory nur an ihre Zweigstellen und Stellen mit Multi-Adressaten-Zugang weitergeben. Die Weitergabe an sonstige Dritte auf anderem Wege ist ihnen nicht gestattet.

Das TARGET2-Directory erscheint nicht in Papierform. Es wird wöchentlich aktualisiert. Die Aktualisierungen werden in der Nacht von Donnerstag auf Freitag bereitgestellt und gelten ab dem darauffolgenden Montag. Die vollständige Version steht ab Freitagmorgen zur Verfügung. PM-Kontoinhabern wird dringend empfohlen, ihren Zentralbanken Änderungsanträge frühzeitig zukommen zu lassen und dabei möglichst ein künftiges Aktivierungsdatum zu nennen. Für Änderungen der Stammdaten, die das TARGET2-Directory betreffen, ist es ratsam, einen Montag als Aktivierungsdatum zu wählen, um die Übereinstimmung der Stammdaten mit dem TARGET2-Directory sicherzustellen. Aus Gründen der Konsistenz ist es außerdem ratsam, den ersten Montag nach der monatlichen Aktualisierung des SWIFT BICPlusIBAN-Directory zu wählen.

3.5.2.2 TIPS-Directory

Das TIPS-Directory ist die Datenbank, der die BICs für die Unterstützung des Routing von Instant-Zahlungen in TIPS entnommen werden können. Es verwendet SWIFT-bezogene Informationen (BIC11) in Verbindung mit TIPS-spezifischen Informationen, die die TIPS-Geldkontoinhaber im Rahmen ihrer Registrierung bereitstellen. Das TIPS-Directory umfasst ein Verzeichnis aller BICs von TIPS-Geldkontoinhabern und erreichbaren Parteien[36], die innerhalb von TIPS adressiert werden können, samt Angaben zur maximalen Betragshöhe, bis zu welcher diese eingehende Instant-Zahlungen

35 Teilnehmer mit internetbasiertem Zugang können das TARGET2-Directory online einsehen.

36 Erreichbare Parteien, die nicht mit einem TIPS-Geldkonto verbunden sind, werden nicht in das TIPS-Directory aufgenommen.

entgegennehmen.

Die verschiedenen Arten der Teilnahme an TIPS lassen sich dem TIPS-Directory entnehmen (TIPS-Geldkontoinhaber oder erreichbare Partei). Außerdem enthält das TIPS-Directory den Nutzer-BIC, den Namen des Instituts, den BIC der Partei, den Kontoinhaber-BIC, die Art der Änderung (A, M, D, U), Angaben zum Gültigkeitsbeginn und –ende und zur maximalen Betragshöhe von Instant-Zahlungen (weitere Informationen finden sich in Abschnitt 1.4.4.2 der User Detailed Functional Specifications (UDFS) des gemeinsamen Referenzdatenmanagements (CRDM)). Ein BIC11 kann nur einmal als Nutzer-BIC für einen bestimmten Gültigkeitszeitraum aufgenommen werden.

Das CRDM generiert ein TIPS-Directory für jede Währung, die über TIPS abgewickelt wird. Für den Euro generiert es täglich um 17.00 Uhr eine Voll- und eine Deltaversion des TIPS-Directory. Unmittelbar nach Abschluss dieses Vorgangs leitet das CRDM beide Versionen zur Verteilung im „Push"- und „Pull"-Modus an TIPS weiter.

TIPS-Akteure können auf folgende Arten auf das TIPS-Directory zugreifen:

c) **„Push"-Modus**: Täglich nach Erhalt der Tagesabschlussnachricht von TARGET2 sendet TIPS die Vollversion oder die Deltaversion des TIPS-Directory an alle TIPS-Akteure, die eine entsprechende Berichtskonfiguration vorgenommen haben.

d) **„Pull"-Modus**: Die TIPS-Akteure können sich während der Geschäftszeiten des CRDM jederzeit die Voll- oder die Deltaversion des TIPS-Directory über die CRDM GUI herunterladen.

Die TIPS-Geldkontoinhaber dürfen das TIPS-Directory nur an ihre Zweigstellen, die von ihnen benannten erreichbaren Parteien und ihre einreichenden Parteien verteilen. Erreichbare Parteien dürfen das TIPS-Directory nur an ihre Zweigstellen weitergeben.

3.5.3 Verwaltung der Zugriffsrechte von TIPS-Geldkontoinhabern

3.5.3.1 Registrierungsprozess und TIPS-Formulare – für Verrechnungen in Euro

Allgemeine Informationen zum Registrierungsprozess und zu den Formularen sind dem Dokument „Reference and static data registration user guide" zu entnehmen.

3.5.3.2 Zugriffsrechte

Die Autorisierung von Anfragen bestimmter Nutzer (d. h. Einzelpersonen oder Anträge, die über einen Distinguished Name (DN) identifiziert werden) erfolgt in TIPS auf der Grundlage der jeweiligen Zugangsrechteprofile. Jede Interaktion mit TIPS, die entweder im A2A-Modus mittels einer Nachricht (z. B. Versendung einer Instant-Zahlung) oder im U2A-Modus über den TIPS-GUI-Bildschirm

(z. B. Erfragung des Saldos eines TIPS-Geldkontos) ausgelöst werden kann, ist als TIPS-Nutzerfunktion definiert. Das Recht, eine bestimmte TIPS-Nutzerfunktion auszulösen, wird über eine damit verbundene Berechtigung gewährt.

Alle für TIPS relevanten Berechtigungen sind im CRDM definiert und gespeichert. Das CRDM bietet außerdem die Möglichkeit, verschiedene Berechtigungen in Rollen zusammenzufassen. Jede dieser Rollen definiert eine spezifische Geschäftsrolle, die TIPS-Akteure für die Interaktion mit TIPS nutzen. Je nach Anforderungen werden den TIPS-Nutzern eine oder mehrere Rollen im CRDM zugeordnet, und diese Rollen bestimmen die Konfiguration ihrer Zugriffsrechte.

Die Rollen werden dann Nutzern zugewiesen, die durch spezifische Distinguished Names identifiziert werden. Somit kann der mit der Rolle verbundene Distinguished Name Nutzerfunktionen in TIPS auslösen, indem er die in der Rolle enthaltenen Berechtigungen ausübt.

Die Nutzerrollen sind innerhalb des Eurosystems harmonisiert.

Der komplette Konfigurationsprozess der Zugriffsrechte wird im CRDM ausgeführt: Die CRDM-Dokumentation liefert weitere Details zu diesen Aspekten.

3.5.3.3 Einrichtung und Änderung von LM- und RM-/SF-Links

Jedes TIPS-Geldkonto muss über einen LM-Link mit einem PM-Konto und über einen RM-/SF-Link mit einem PM-/Heimatkonto verbunden sein. Zentralbanken können diese Links über das ICM in den Stammdaten des Teilnehmers einrichten, verändern und einsehen.

Liquiditätssteuerungsverbindung (LM-Link)

Der LM-Link ermöglicht den Teilnehmern, über das ICM auf Liquiditätssteuerungsfunktionen zuzugreifen (im Allgemeinen kann von jedem TIPS-Geldkonto auf jedes PM-Konto Liquidität übertragen werden und umgekehrt) und besteht zwischen einem TIPS-Geldkonto und einem PM-Konto. Außerdem werden die Gebühren für TIPS dem verknüpften PM-Konto belastet. Jedes TIPS-Geldkonto muss mit einem PM-Konto verbunden sein.[37] Eine Änderung des LM-Links zu einem anderen PM-Konto ist möglich.

Es gilt zu beachten, dass maximal zehn TIPS-Geldkonten[38] zu Liquiditätssteuerungszwecken mit einem PM-Konto verbunden werden können und dass die Liquiditätsübertragungsfunktion Teilnehmern mit internetbasiertem Zugang nicht zur Verfügung steht. Die verantwortliche Zentralbank stellt sicher, dass das verknüpfte TIPS-Geldkonto bereits im CRDM angelegt wurde.

37 Die Verbindung zu genau einem PM-Konto ist technisch vorgegeben.

38 Die maximale Anzahl von zehn verbundenen TIPS-Geldkonten ist technisch vorgegeben.

Der LM-Link kann zwischen Konten eingerichtet werden, die von unterschiedlichen juristischen Personen und bei unterschiedlichen Zentralbanken gehalten werden (d. h., grenzüberschreitende Verbindungen sind erlaubt).

Verbindung mit dem Modul für die Mindestreserveverwaltung und dem Modul für die ständigen Fazilitäten (RM-/SF-Link)

Zur Berechnung der Mindestreserven, zur Verzinsung von Übernachtguthaben und zur automatisierten Inanspruchnahme der Spitzenrefinanzierungsfazilität (Übernachtkredit)[39] muss der TIPS-Geldkontoinhaber sein TIPS-Geldkonto über den RM-/SF-Link an ein PM-/Heimatkonto anbinden, das er **bei derselben Zentralbank** hält (d. h., grenzüberschreitende Verbindungen sind nicht erlaubt). Der RM-/SF-Link kann nur zwischen TIPS-Geldkonten und PM-/Heimatkonten derselben Institution eingerichtet werden. Die Verbindung kann auch bei Teilnehmern mit internetbasiertem Zugang eingesetzt werden.

Der RM-/SF-Link ist vollständig unabhängig vom LM-Link. Die Zahl der TIPS-Geldkonten, die zu Zwecken der Mindestreserveverwaltung mit einem PM-Konto oder Heimatkonto verknüpft werden können, ist nicht begrenzt.

Die für die Berechnung der Mindestreserve, für die Verzinsung von Übernachtguthaben und für die automatisierte Inanspruchnahme der Spitzenrefinanzierungsfazilität (Übernachtkredit) notwendigen Daten werden nach Abschluss der letzten Algorithmen in TARGET2 (i. d. R. kurz nach 18.00 Uhr) über eine Hauptbuchdatei („General Ledger File“) von TIPS an TARGET2 übertragen.

3.5.3.4 Registrierung erreichbarer Parteien − für Euro-Zahlungen

Das TIPS-Directory ermöglicht nur eine einzige Beziehung zwischen einer erreichbaren Partei und einem TIPS-Geldkontoinhaber, der den Zugang zu TIPS bereitstellt. Alle erreichbaren Parteien werden im TIPS-Directory veröffentlicht. Erreichbare Parteien müssen das SEPA Instant Credit Transfer (SCT^{Inst}) Scheme einhalten und das SEPA Instant Credit Transfer Adherence Agreement unterzeichnen.

Erreichbare Parteien werden von der Zentralbank des jeweiligen direkten Teilnehmers registriert.

Es ist möglich, dass zwei oder mehrere Teilnehmer konfliktäre Registrierungsanfragen an ihre jeweilige Zentralbank senden. Konfliktäre Anfragen können folgende Aspekte betreffen:

- einen bestehenden Eintrag im TIPS-Directory oder

[39] Die TIPS-Salden in TARGET2 am Tagesschluss (sofern verfügbar) werden entsprechend den mittels RM-/SF-Links übermittelten Informationen berücksichtigt und zum Zwecke der Mindestreserveanforderungen, der Verzinsung von Übernachtguthaben und der automatisierten Inanspruchnahme der Spitzenrefinanzierungsfazilität (Übernachtkredit) zum Saldo des entsprechenden TARGET2-Teilnehmers hinzuaddiert.

- eine neue erreichbare Partei im TIPS-Directory.

Zentralbanken erhalten Anfragen von ihrem Markt (d. h. ihren TIPS-Geldkontoinhabern) und veranlassen die für die Registrierung erreichbarer Parteien notwendigen Schritte.

Geht eine Anfrage für eine bereits registrierte Partei ein und hat dieser Eintrag kein Gültigkeitsende (End of Validity Date, z. B. 31/12/9999), muss die Zentralbank den Konflikt dadurch lösen, dass sie den TIPS-Geldkontoinhaber und gegebenenfalls die andere Zentralbank kontaktiert.

3.5.3.5 Einrichtung von MPL-Akteuren

Die Einrichtung von Akteuren im Mobile Proxy Lookup Service (MPL-Service) erfolgt in der Komponente Gemeinsames Referenzdatenmanagement (CRDM). Der TIPS-Betreiber ist für die Einrichtung und die Pflege der Referenzdaten für alle Zentralbanken als Parteien im MPL-Service zuständig. Die Zentralbanken sind für die Einrichtung und Pflege der Referenzdaten ihrer nationalen Teilnehmer und MPL-Teilnehmer für die Einrichtung und Konfiguration ihrer eigenen Nutzer verantwortlich.

MPL-Teilnehmer sind hier zu verstehen als Institute, die im MPL-Service Elemente in Proxy-IBAN-Mapping-Tabellen eintragen und pflegen. Sie werden durch einen BIC11 eindeutig identifiziert und können:

- Suchanfragen im MPL-Service starten, um die IBAN herauszufinden, die einem gegeben Proxy Digest (zum Beispiel einer Rufnummer) entspricht,

- eine Erreichbarkeitsprüfung veranlassen, um zu prüfen, ob ein gegebener Proxy Digest (zum Beispiel eine Rufnummer) einer IBAN zugeordnet wurde.

3.5.4 Verwaltung der Zugriffsrechte von direkt angeschlossenen T2S-Geldkontoinhabern

Die Verwaltung der Zugriffsrechte in T2S ist dezentral organisiert und folgt dem dreistufigen Hierarchie-Modell der T2S-Parteien (siehe nachstehende Abbildung). Gemäß diesem Modell ist der Betreiber von T2S (4ZB) die auf der obersten Hierarchieebene angesiedelte Partei. Zentralbanken und Zentralverwahrer befinden sich auf der zweiten Ebene, während ihre Teilnehmer (jeweils T2S-Geldkontoinhaber und CSD-Teilnehmer) die dritte Ebene bilden.

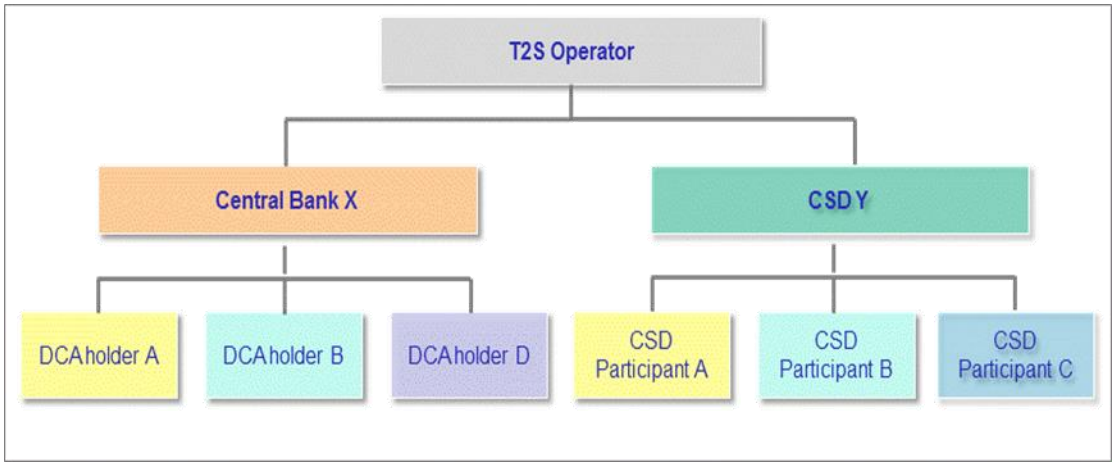


Abbildung 14: Hierarchie-Modell der T2S-Partei

Auf dieser Grundlage definiert der Betreiber von T2S über die Verwaltung der Zugriffsrechte die verschiedenen T2S-Funktionen, die von den Zentralbanken und Zentralverwahrern verwendet werden können. Die Zentralbanken und Zentralverwahrer wiederum definieren die verschiedenen T2S-Funktionen, die ihre Teilnehmer verwenden können. Der Umfang der Daten (Stamm- und transaktionsbezogene Daten), über die jede Einrichtung/Partei verfügt, wird durch das Hierarchie-Modell der T2S-Parteien bestimmt.

Ferner basiert die Verwaltung der Zugriffsrechte auf dem Konzept von Berechtigungen, Rollen und Partei-Administratoren. Unter Berechtigung ist das Recht zu verstehen, eine gewisse T2S-Funktion auszulösen (z. B. eine vorgegebene Abfrage auszuführen). Berechtigungen können in Rollen zusammengefasst werden. Das Zugangsrechteprofil eines bestimmten Nutzers ergibt sich aus den ihm übertragenen Rollen und Berechtigungen.

Jede Einrichtung/Partei muss über mindestens einen Partei-Administrator verfügen, d. h. einen Nutzer, der Rollen und Berechtigungen zuteilen darf, sofern sie der Einrichtung übertragen wurden, der er angehört. Der Partei-Administrator kann über eine Berechtigung verfügen, sobald sie eingeräumt wurde. Ab diesem Zeitpunkt kann er die Berechtigung weitergeben. Nachdem die Zugangsrechte für eine Partei auf der Ebene dieser Partei konfiguriert wurden, kann der Partei-Administrator/können die Partei-Administratoren die Konfiguration diese Rechte auf Nutzerebene vornehmen, um allen Nutzern der Partei die geeigneten Rollen und Berechtigungen zuzuweisen.[40]

Rollen und Berechtigungen werden von den Partei-Administratoren der einzelnen Stellen dezentral wie

[40] Wie im Dokument „Reference and static data registration user guide“ angegeben, können die von den Zentralbanken bestimmten Administratoren für die T2S-Geldkontoinhaber dem Zwei-Augen- oder dem Vier-Augen-Prinzip unterworfen werden. Im Falle des Vier-Augen-Prinzips ist ein spezielles Verfahren anzuwenden. Um nähere Informationen zu erhalten, sollten die T2S-Geldkontoinhaber daher ihre jeweilige Zentralbank kontaktieren.

folgt gemäß dem Hierarchie-Modell der T2S-Parteien vergeben:

a) Der Administrator einer Zentralbank: 1) erstellt neue Rollen, einschließlich der verfügbaren Berechtigungen, 2) verwaltet die verfügbaren Rollen und Berechtigungen und weist sie den Nutzern zu, 3) legt die ersten Administratoren seiner T2S-Geldkontoinhaber an, 4) ordnet die verfügbaren Rollen und Berechtigungen seinen T2S-Geldkontoinhabern zu,

b) Der Administrator eines T2S-Geldkontoinhabers: 1) verwaltet die Nutzer seines Instituts, 2) weist den Nutzern die verfügbaren Rollen und Berechtigungen zu.

3.5.4.1 Auf der T2S-Plattform aufgeführte externe RTGS-Konten

Auf der T2S-Plattform wird eine Liste externer RTGS-Konten geführt, anhand derer das Konto des Begünstigten bei ausgehenden Liquiditätsübertragungen (von einem T2S-Geldkonto auf ein PM-Konto) überprüft wird. Ist ein als Konto des Begünstigten angegebenes PM-Konto nicht in der Liste externer RTGS-Konten zu finden, wird die Liquiditätsübertragung zurückgewiesen. Hierbei ist zu beachten, dass die auf dieser Liste stehenden Kontonummern für die direkt an T2S angeschlossenen T2S-Geldkontoinhaber sichtbar sind. Es wird jedoch weder der BIC noch der Name des Instituts angezeigt, das das Konto unterhält, es sei denn, diese können von der RTGS-Kontonummer abgeleitet werden.[41]

Dabei sind alle TARGET2-PM-Konten, die gegebenenfalls Liquiditätsübertragungen von einem T2S-Geldkonto empfangen können, in die T2S-Liste externer RTGS-Konten aufzunehmen, d. h., es werden alle Konten aufgeführt, mit Ausnahme von Spiegel-/technischen Konten, PM-Konten von Teilnehmern mit internetbasiertem Zugang sowie von unveröffentlichten Konten (unveröffentlichten BICs)[42].

Jede Zentralbank ist dafür verantwortlich, die T2S-Liste externer RTGS-Konten zu aktualisieren, wenn ein PM-Konto auf der Gemeinschaftsplattform eingerichtet, geändert oder gelöscht wird (mit Ausnahme eines Spiegel-/technischen Kontos, eines PM-Kontos eines Teilnehmers mit internetbasiertem Zugang sowie eines unveröffentlichten Kontos).

3.5.4.2 Informationsfluss zwischen Zentralbanken, T2S-Geldkontoinhabern und Zentralverwahrern

Die Einrichtung und Schließung eines T2S-Geldkontos erfolgt durch die verantwortliche Zentralbank auf Basis der vom T2S-Geldkontoinhaber vorgelegten Stammdatenformulare. Nach Eröffnung des T2S-Geldkontos kann der T2S-Geldkontoinhaber seine(n) Zentralverwahrer kontaktieren, um die Kontokonfiguration abzuschließen und die Verbindung vom T2S-Geldkonto zum Wertpapierkonto/zu

41 Jeder T2S-Geldkontoinhaber kann nur die Daten zu den RTGS-Konten einsehen, über die seine jeweilige Zentralbank verfügt.

42 Unveröffentlichte PM-Konten und PM-Konten von Teilnehmern mit internetbasiertem Zugang können von der Zentralbank auf Antrag des Teilnehmers in die Liste aufgenommen werden.

den Wertpapierkonten herzustellen.

Beabsichtigt ein T2S-Geldkontoinhaber, ein T2S-Geldkonto zu schließen, hat er seine Zentralbank und seine(n) Zentralverwahrer hiervon in Kenntnis zu setzen. Anschließend hat er seine(n) Zentralverwahrer aufzufordern, die Verbindung(en) zwischen dem T2S-Geldkonto und dem Wertpapierkonto/den Wertpapierkonten aufzuheben. Nachdem alle Verbindungen gelöscht wurden, kann er die Schließung des T2S-Geldkontos bei der Zentralbank beantragen. Nach der Schließung ist es nicht mehr möglich, das T2S-Geldkonto für die Wertpapierabwicklung oder Liquiditätsübertragungen zu verwenden.

Es ist keine formelle Kommunikation zwischen den Zentralbanken und den Zentralverwahrern im Zusammenhang mit der Registrierung von T2S-Geldkontoinhabern vorgesehen. Bei der Eröffnung oder Schließung eines T2S-Geldkontos ist der T2S-Geldkontoinhaber dafür verantwortlich, die Einrichtung oder Aufhebung der Verbindung(en) zwischen dem T2S-Geldkonto und dem Wertpapierkonto/den Wertpapierkonten beim jeweiligen Zentralverwahrer/bei den jeweiligen Zentralverwahrern zu beantragen.

Tritt eine Sondersituation ein, wie beispielsweise die Insolvenz eines T2S-Geldkontoinhabers, die eine Zentralbank gegebenenfalls zur Sperrung des T2S-Geldkontos veranlasst, informiert die Zentralbank den/die Zentralverwahrer per GUI-Nachricht.

3.6 Zertifizierungstests

Jeder TARGET2-Nutzer muss, abhängig von den von der betreffenden Zentralbank gewählten SSP-Modulen und den vom Nutzer gewählten Funktionen der SSP und/oder der TIPS-Plattform und/oder der T2S-Plattform, eine Reihe von Zertifizierungstests durchführen. Ein weiterer Faktor, der sich auf Art und Anzahl der durchzuführenden Tests auswirkt, ist beispielsweise die Teilnahme an verschiedenen Nebensystemen.

Die Zertifizierung lässt sich unterteilen in die technische Zertifizierung und die Feststellung der Betriebsbereitschaft:

- Die technische Zertifizierung der PM-Kontoinhaber und der Nebensysteme besteht aus dem erfolgreichen Abschluss einer gewissen Anzahl an Connectivity- und Interoperability-Tests. Die Feststellung der Betriebsbereitschaft wird auf Basis der Teilnahme an Country- und Business-Day-Tests geprüft.
- Die technische Zertifizierung der direkt angeschlossenen T2S-Geldkontoinhaber besteht aus dem erfolgreichen Abschluss einer gewissen Anzahl an Connectivity-, Certification- und Authorisation-Tests. Die Feststellung der Betriebsbereitschaft wird auf Basis der Teilnahme an Community- und Business-Day-Tests geprüft.

- Die technische Zertifizierung der indirekt angeschlossenen T2S-Geldkontoinhaber besteht aus dem erfolgreichen Abschluss einer gewissen Anzahl an Interoperability- und Authorisation-Tests. Die Feststellung der Betriebsbereitschaft wird auf Basis der Teilnahme an Community- und Business-Day-Tests geprüft.

Weitere Informationen über die von den PM-Kontoinhabern, Nebensystemen und T2S-Geldkontoinhabern durchzuführenden Tests sind im „Guide to TARGET2 User Testing“ zu finden.

Bei TIPS besteht das Ziel der Zertifizierungstests darin, den Nachweis dafür zu liefern, dass eine Interaktion des TIPS-Geldkontoinhabers oder der erreichbaren Partei mit TIPS möglich ist. Die TIPS-Zertifizierungstests sollen eine oder mehrere der folgenden Fähigkeiten demonstrieren:

- Versand und Empfang spezifischer Nachrichten im A2A-Modus
- Erfolgreiche Anmeldung bei der U2A-Schnittstelle
- Abonnement und Empfang spezifischer Berichte.

TIPS-Tester müssen ihre Zertifizierungs-Testfälle ausführen. Nach Abschluss der Zertifizierungstests müssen die Tester dem Eurosystem einen Abschlussbericht zur Prüfung einreichen, in dem der erfolgreiche Abschluss der relevanten Testfälle belegt wird. Weitere Angaben zu den Testverfahren für TIPS finden sich auf der Website der EZB.

Das Testumfeld des Nutzers sollte der künftigen Produktionsumgebung so weit wie möglich entsprechen. Jede verwendete Komponente sollte bereits ein internes Zulassungsverfahren durchlaufen haben.

Die zuständige Zentralbank muss schriftlich von allen während oder nach den Zertifizierungstests auftretenden Änderungen des Testumfelds und/oder der künftigen Produktionsumgebung des Nutzers in Kenntnis gesetzt werden. Dazu gehören alle technischen Änderungen (z. B. an technischen Komponenten oder der Software) sowie sämtliche mit der Interaktion mit TARGET2 zusammenhängenden betrieblichen Änderungen. Unter einer betrieblichen Änderung ist eine Änderung der Kontenstruktur bzw. die Nutzung optionaler Funktionen zu verstehen, die in der Vergangenheit nicht genutzt wurden und deshalb nicht Teil eines früheren Zertifizierungsverfahrens waren. Die Mitteilung sollte neben einer eindeutigen Beschreibung von Art und Umfang der Änderung sowie der damit verbundenen Risiken einen Vorschlag enthalten, welche Testfälle aufgrund der Änderung erneut durchzuführen sind (Non-Regression-Tests). Die Zentralbank prüft diesen Vorschlag. Grundsätzlich sind während der technischen Zertifizierung Änderungen möglich; während der Feststellung der Betriebsbereitschaft sollten Änderungen vermieden werden. Änderungen nach der Zertifizierung eines TARGET2-Nutzers sind nicht mehr gestattet; sie würden ein neues Zertifizierungsverfahren erforderlich machen. Zur Wahrung der notwendigen Flexibilität können die Zentralbanken allerdings Ausnahmen

von diesen Grundsätzen zulassen, sofern diese gerechtfertigt sind.

Der technische Aufbau der SSP und/oder der TIPS-Plattform und/oder der T2S-Plattform und/oder des PHA kann sich im Zuge der jährlichen Releases, nach Notfalländerungen und „Hot Fixes“ (z. B. zur Fehlerbehebung) ändern. In solchen Fällen schätzen die Zentralbanken ab, welche Auswirkungen diese Veränderungen auf das bereits von den TARGET2-Nutzern durchgeführte Zertifizierungsverfahren haben werden und informieren diese entsprechend. Unter Umständen kann es erforderlich sein, dass einige Zertifizierungstests wiederholt werden müssen (Non-Regression-Tests). Solche Aufforderungen zur Durchführung von Non-Regression-Tests werden auf das absolute Minimum begrenzt.

3.7 Maßnahmen zur Gewährleistung der Sicherheit und operationellen Zuverlässigkeit von TARGET2-Nutzern

3.7.1 Aufgaben und Zuständigkeiten

Folgende vier Hauptaufgaben und -zuständigkeiten sollen die Sicherheit und die operationelle Zuverlässigkeit der Nutzer gewährleisten:[43]

- Festlegung des Rahmenwerks durch das Eurosystem: Verfassen von Richtlinien, an die sich alle beteiligten Parteien halten müssen, und Spezifizierung einheitlicher Anforderungen, die die Nutzer zu erfüllen haben
- Überprüfung auf Einhaltung durch die Zentralbanken („Compliance Check“): Überprüfung, ob die Nutzer die im Rahmenwerk festgelegten Maßnahmen einhalten
- Bereitstellung von Informationen durch Nutzer: Versorgung der Zentralbanken mit relevanten Informationen wie im Rahmenwerk festgelegt
- Überwachung und Folgemaßnahmen durch die Zentralbanken: Aufdeckung von Schwachstellen und Überwachung der Folgemaßnahmen, die diese Schwachstellen beseitigen sollen

Um sicherzustellen, dass alle Nutzer dieselben Kriterien erfüllen müssen und um eine harmonisierte Durchführung der „Compliance Checks“ zu erleichtern, sind einheitliche und effektive Richtlinien sowie Verfahren erforderlich. Für die Festlegung und Einhaltung dieses Rahmenwerks ist das Eurosystem zuständig.

Was die „Compliance Checks“ anbelangt, so gilt der Grundsatz, dass die Kundenbeziehung vollständig in den Zuständigkeitsbereich der Zentralbank fällt, die mit dem Nutzer in einer Rechtsbeziehung steht. Hierbei spielt es keine Rolle, ob der Nutzer seinen Sitz innerhalb oder außerhalb des Euro-

[43] Inwieweit das Selbstzertifizierungsrahmenwerk auch für TIPS-Akteure gilt, wird derzeit noch erörtert. Bezüglich TIPS ist damit zu rechnen, dass das Rahmenwerk im Jahresverlauf 2019 angepasst wird.

Währungsgebiets hat. Vielmehr ist zu berücksichtigen, ob sich eine Zentralbank im TARGET2-Gebiet befindet.[44]

Beispiele: Dänemark hat den Euro nicht eingeführt, aber die dänische Zentralbank nimmt an TARGET2 teil. Folglich gehen direkte Teilnehmer, deren Hauptsitz sich in Dänemark befindet, in der Regel mit der dänischen Zentralbank eine Rechtsbeziehung ein. Im Fall von direkten Teilnehmern mit Hauptsitz im Vereinigten Königreich ist dies anders. Die Bank of England hat sich entschieden, nicht an TARGET2 teilzunehmen. Deshalb müssen direkte Teilnehmer aus dem Vereinigten Königreich eine an TARGET2 teilnehmende Zentralbank auswählen, mit der sie eine Rechtsbeziehung eingehen.

Anhand der folgenden Fragen können die Zentralbanken feststellen, ob sie für das Einholen der relevanten Informationen bei einem bestimmten Nutzer zuständig sind.

Unterhält der Nutzer eine eigene technische Infrastruktur für das Routing von Zahlungen nach TARGET2?

- Lautet die Antwort „Ja“: Die Zentralbank dieses direkten Teilnehmers ist die zuständige Zentralbank.
- Lautet die Antwort „Nein“: Befindet sich die für das Routing von Zahlungen nach TARGET2 verwendete Infrastruktur, die von einem anderen direkten Teilnehmer unterhalten wird, in einem anderen Land (z. B. Mitglied/Konzentrator, Zweigstelle/Tochter, Zentrale eines direkten Teilnehmers)?
  - Lautet die Antwort „Ja“: Die Zentralbank des direkten Teilnehmers, der die technische Infrastruktur unterhält, ist zuständig.
  - Lautet die Antwort „Nein“: Bietet das Institut, das die Infrastruktur unterhält, den gleichen Service auch anderen direkten Teilnehmern an (z. B. Servicebüro)?
    - Lautet die Antwort „Ja“: Die Zentralbank, die mit dem betragsmäßig größten, diese Infrastruktur verwendenden direkten Teilnehmer in einer Rechtsbeziehung steht, ist zuständig.
    - Lautet die Antwort „Nein“: Die Zentralbank, die mit dem direkten Teilnehmer in einer Rechtsbeziehung steht, ist zuständig.

Die folgende Tabelle bietet direkten Teilnehmern, die feststellen möchten, welche Zentralbank für ihr Institut zuständig ist, eine Orientierungshilfe:

44 Das TARGET2-Gebiet umfasst die Länder aller an TARGET2 teilnehmenden Zentralbanken.

Beschreibung der Gegebenheiten	Zuständige Zentralbank
Hauptsitz (Zentrale) befindet sich innerhalb/außerhalb[45] des TARGET2-Gebiets; keine Zweigstellen/Töchter	Zentralbank, die eine Rechtsbeziehung mit der Zentrale hat
Hauptsitz (Zentrale) und Zweigstellen/Töchter befinden sich innerhalb/außerhalb des TARGET2-Gebiets; beide sind direkte Teilnehmer, und das Routing des Zahlungsverkehrs nach TARGET2 erfolgt über die technische Infrastruktur der Zentrale	Zentralbank, die eine Rechtsbeziehung mit der Zentrale hat
Hauptsitz (Zentrale) und Zweigstellen/Töchter befinden sich innerhalb/außerhalb des TARGET2-Gebiets; beide sind direkte Teilnehmer, verfügen jedoch über ihre eigene technische Infrastruktur für das Routing von Zahlungen zu TARGET2	Jeweilige Zentralbank, die eine Rechtsbeziehung mit der Zentrale und den Zweigstellen/Töchtern hat
Es besteht keine Rechtsbeziehung zwischen der innerhalb/außerhalb des TARGET2-Gebiets gelegenen Zentrale und einer TARGET2-Zentralbank, aber das Routing des Zahlungsverkehrs erfolgt über eine Zweigstelle/Tochter, die ein direkter Teilnehmer ist (unabhängig davon, wo die technische Infrastruktur angesiedelt ist).	Zentralbank, die eine Rechtsbeziehung mit der Zweigstelle/Tochter hat
Serviceprovider, der in keiner Rechtsbeziehung steht (unabhängig davon, ob er sich innerhalb oder außerhalb des TARGET2-Gebiets befindet), unterhält die technische Infrastruktur für Finanzinstitute, die direkte Teilnehmer sind	Zentralbank, die eine Rechtsbeziehung mit dem Finanzinstitut hat, das betragsmäßig den größten Umsatz über diese technische Infrastruktur nach TARGET2 einliefert

Tabelle 7: Zuständigkeit der Zentralbank für direkte Teilnehmer

Wie aus der oben stehenden Tabelle hervorgeht, kann in Bezug auf die Servicebüros eine Ausnahmeregelung gelten (siehe Abschnitt 3.7.2.3). Denkbar ist eine gemeinsame Nutzung der von einer solchen Institution bereitgestellten technischen Infrastruktur durch einige in verschiedenen Ländern ansässige direkte Teilnehmer (mit geringem Umsatzvolumen). Servicebüros gehen jedoch keine Rechtsbeziehung mit einer Zentralbank ein. Vielmehr stehen sie lediglich mit Kunden in einer Rechtsbeziehung, die ihre technische Infrastruktur zum Routing von Transaktionen nach TARGET2 nutzen. Allerdings sind direkte Teilnehmer, die ein Servicebüro nutzen, aufgrund der Harmonisierten Bedingungen rechtlich verpflichtet, ihre Zentralbank von Ausfällen bei einem solchen Unternehmen in

45 Falls die Zentrale nicht im TARGET2-Gebiet ansässig ist, muss sie sich aber innerhalb des EWR befinden.

Kenntnis zu setzen.[46] In einem solchen Fall und um die Erhebung von identischen Daten über verschiedene direkte Teilnehmer zu vermeiden, obliegt es der Zentralbank, die mit dem betragsmäßig größten direkten Teilnehmer[47] aller dasselbe Servicebüro nutzenden Teilnehmer in einer Rechtsbeziehung steht, die Einhaltung der im Rahmenwerk zur Gewährleistung der Sicherheit und operationellen Zuverlässigkeit der Nutzer festgelegten Maßnahmen zu überprüfen (siehe Abschnitt 3.7.2).

Wenn die direkten Teilnehmer ein Mitglied/einen Konzentrator nutzen,[48] gibt es zwei Möglichkeiten: Entweder ist das Mitglied/der Konzentrator selbst ein direkter Teilnehmer, dann übernimmt die Zentralbank, die mit diesem direkten Teilnehmer in einer Rechtsbeziehung steht, die in diesem Leitfaden beschriebenen Zuständigkeiten; oder das Mitglied/der Konzentrator ist lediglich ein Verbindungsdienstleister (der nicht in einer Rechtsbeziehung mit einer Zentralbank steht); in diesem Fall ist die Zentralbank, die mit dem betragsmäßig größten, dasselbe Mitglied/denselben Konzentrator nutzenden direkten Teilnehmer in einer Rechtsbeziehung steht, für die Überprüfung der Einhaltung der relevanten Sicherheitsanforderungen zuständig.

Um eine effektive Durchführung dieser Tests zu gewährleisten, müssen die direkten Teilnehmer ihrer Zentralbank auf Anfrage die notwendigen Informationen und Dokumente zur Verfügung stellen.

Jede entdeckte Schwachstelle muss auf der Grundlage eines harmonisierten Ansatzes genau untersucht werden. Anschließend muss die weitere Vorgehensweise zur Beseitigung dieser Schwachstellen abgestimmt und die Umsetzung der beschlossenen Maßnahmen überwacht werden. Diese Aufgabe fällt ebenfalls in den Zuständigkeitsbereich der Zentralbanken.

Schließlich sollten sich die von den Zentralbanken in Verbindung mit diesem Rahmenwerk wahrgenommenen Aufgaben und die von anderen Regulierungsbehörden, z. B. der Bankenaufsicht oder der Zahlungsverkehrsüberwachung, durchgeführten Maßnahmen nicht überschneiden.

3.7.2 Kritische und nichtkritische Teilnehmer

Ungeachtet der zentralen Anforderung, die Wettbewerbsgleichheit zwischen den Nutzern zu gewährleisten, sind sich alle Beteiligten bewusst, dass Sicherheitsmängel, die die Systeme der Finanzinstitute betreffen, je nach wertmäßigem Marktanteil und/oder Art der abgewickelten

46 Harmonisierte Bedingungen, Artikel 28 Absatz 2: „Die Teilnehmer informieren die [zuständige Zentralbank] über alle sicherheitsrelevanten Vorfälle in ihrer technischen Infrastruktur und, sofern dies angemessen erscheint, über sicherheitsrelevante Vorfälle in der technischen Infrastruktur von Drittanbietern."

47 Welcher unter diesen direkten Teilnehmern der größte ist, kann sich ändern, beispielsweise im Zuge einer Fusion. In einem solchen Fall muss die weitere Vorgehensweise geprüft werden.

48 Gleiches gilt, wenn die TARGET2-Nutzer andere Vereinbarungen für die gemeinsame Nutzung von IT-Infrastruktur treffen, z. B. durch die Auslagerung der Zahlungsabwicklung an ein darauf spezialisiertes Unternehmen (in einigen Fällen ein Joint Venture mit anderen TARGET2-Nutzern).

Transaktionen (z. B. bei Zahlungsvorgängen in systemisch wichtigen Nebensystemen) in ihren Auswirkungen variieren können. Eingedenk dessen ist zwischen *kritischen Teilnehmern* und *nichtkritischen Teilnehmern* zu unterscheiden.[49]

Es steht eine Reihe grundlegender Instrumente zur Verfügung, die sowohl auf kritische als auch auf nichtkritische Teilnehmer anwendbar sind. Damit der entscheidenden Bedeutung der kritischen Teilnehmer für das reibungslose Funktionieren des TARGET2-Systems Rechnung getragen wird, müssen diese Nutzer jedoch einige zusätzliche Maßnahmen umsetzen.

Im Folgenden werden die TARGET2-Nutzer in Kreditinstitute, Nebensysteme und Servicebüros/Konzentratoren unterteilt. Für jede Gruppe wird erläutert, welche Teilnehmer als kritisch und welche als nichtkritisch gelten.

3.7.2.1 Kreditinstitute

Allgemeine Überlegungen und Grundsätze

Bei der Festlegung der Bestimmungskriterien für die Einstufung eines Kreditinstituts als kritisch oder nichtkritisch gilt der Grundsatz, dass neben den Instituten mit einem ausreichenden betragsmäßigen Marktanteil auch solche als kritisch gelten, bei denen ein Ausfall bei der Erfüllung ihrer Verpflichtungen dazu führen könnte, dass auch andere Teilnehmer oder Finanzinstitute in anderen Bereichen des Finanzsystems nicht mehr in der Lage sind, ihren Verpflichtungen bei Fälligkeit nachzukommen.[50] Dies bedeutet insbesondere, dass eine Betriebsstörung[51] zu einer Liquiditätsansammlung auf dem Konto eines TARGET2-Nutzers führen könnte, die wiederum die Ausführung von Zahlungen durch andere Systemnutzer verhindern und eventuell systemische Risiken verursachen könnte.

Bestimmungskriterien

Die Festlegung von Kriterien zur Unterscheidung zwischen kritischen und nichtkritischen Kreditinstituten sollte logischerweise vom betragsmäßigen Anteil des jeweiligen Kreditinstituts am Gesamtumsatz abhängen.

49 Dies entspricht auch dem vom EZB-Rat am 31. Mai 2006 verabschiedeten Dokument „Business continuity oversight expectations for systemically important payment systems (SIPS)“, worin festgelegt ist, dass kritische Teilnehmer von SIPS-Betreibern als solche eingestuft werden.

50 Prinzipien für Finanzmarktinfrastrukturen (Principles for Financial Market Infrastructures), Bank für Internationalen Zahlungsausgleich, April 2012.

51 Im Gegensatz zu Bilanzproblemen.

Das Eurosystem betrachtet ein Kreditinstitut grundsätzlich als kritischen TARGET2-Teilnehmer, wenn es im ersten Jahresquartal im arbeitstäglichen Durchschnitt betragsmäßig mindestens 1 % des TARGET2-Umsatzes[52] abwickelt (ausgenommen Transaktionen, die von Dritten, z. B. Nebensystemen, vorgenommen werden, Zahlungen, die über MT 204 ausgeführt werden, und Übertragungen zwischen den Konten desselben Teilnehmers). Die Einstufung hängt sowohl für kritische als auch nichtkritische Teilnehmer außerdem von der Einstufung im Vorjahr ab. Das bedeutet, dass ein Teilnehmer, der einmal als kritisch eingestuft wurde, diese Klassifizierung für mindestens zwei Jahre beibehält.

Dieses Kriterium wird regelmäßig überprüft. Anhand der in Abschnitt 3.7.8 beschriebenen Überprüfungsklausel wird gewährleistet, dass das Kriterium im Sinne der beim Betrieb des TARGET2-Systems gewonnenen Erfahrungen an die Geschäftspraxis angepasst wird.

Möglicherweise nutzen zwei oder mehr Kreditinstitute die technische Infrastruktur für die Teilnahme am TARGET2-System gemeinsam. Wenn der Gesamtwert der von diesen Kreditinstituten im gemeinsamen Umfeld abgewickelten Transaktionen betragsmäßig gleich oder größer als 1 % ist, wird die Organisation, die die Infrastruktur im rechtlichen Sinne betreibt (z. B. eine Transaktionsbank), als kritischer Teilnehmer klassifiziert.

Daneben wendet das Eurosystem Simulationstechniken an, um die Folgen des technischen Ausfalls eines Teilnehmers anhand messbarer Kriterien zu beurteilen.[53] Dabei werden ein technischer Ausfall des Kreditinstituts simuliert und die Auswirkungen gemessen, die dieser Ausfall auf die Abwicklung von TARGET2-Zahlungen haben könnte. Grundsätzlich kann ein Kreditinstitut (wieder) als kritischer Teilnehmer eingestuft werden, wenn die Simulation ergibt, dass bei einem Ausfall der technischen Infrastruktur des betreffenden Teilnehmers im Schnitt 1,5 % des gesamten TARGET2-Umsatzes nicht abgewickelt werden könnten.

Zu beachten ist, dass die Zentralbanken zusätzlich zu den oben genannten, vom Eurosystem gemeinsam vereinbarten Hauptkriterien bei der Einstufung der Kreditinstitute, mit denen sie eine Geschäftsbeziehung unterhalten, spezifische nationale Besonderheiten berücksichtigen können. Infolgedessen können die Zentralbanken sogar vorschlagen, direkte Teilnehmer als kritisch einzustufen, die dieses Hauptkriterium nicht erfüllen. Die betreffende Zentralbank muss die EZB über diese Neuklassifizierung informieren und die Gründe dafür erläutern. Die EZB wird dann eine Stellungnahme darüber abgeben, ob die Neuklassifizierung angemessen ist.

52 Der TARGET2-Umsatz beinhaltet auch Übertragungen an/von T2S-Geldkonten, nicht aber die Abwicklung von Wertpapieren (z. B. Lieferung gegen Zahlung).

53 Für die Simulationen wird der TARGET2-Simulator verwendet, der von der finnischen Zentralbank in Zusammenarbeit mit den 3ZB entwickelt wurde. Weitere Informationen zum TARGET2-Simulator finden sich im TARGET-Newsletter (Ausgabe 7, Q4 2013, abrufbar unter www.target2.eu).

Die von der EZB abgegebene Stellungnahme wird dem betreffenden Gremium[54] des Eurosystems zur weiteren Prüfung vorgelegt.

3.7.2.2 Nebensysteme

Die Gruppe der Nebensysteme setzt sich aus Organisationen/Institutionen aus dem Bereich Wertpapierverrechnung und -abwicklung, Massenzahlungsverkehrssysteme – systemrelevante Massenzahlungsverkehrssysteme (Systemically Important Retail Payment Systems – SIRPS), besonders bedeutsame Massenzahlungsverkehrssysteme (Prominently Important Retail Payment Systems – PIRPS) und andere Massenzahlungsverkehrssysteme – sowie sonstigen Großbetragszahlungssystemen (z. B. CLS und EURO1) zusammen.

Wie bei den Kreditinstituten gibt es bei den Nebensystemen keine empirischen Belege für die genauen Ursachen von systemischen Risiken. Deshalb wurden die Kriterien zur Einstufung der Nebensysteme anhand der Ergebnisse einer Konsultation der betreffenden Stellen des Eurosystems und der verfügbaren Dokumente festgelegt.

Massen- und Großbetragszahlungssysteme

Großbetragszahlungssysteme werden per Definition als systemrelevant klassifiziert. Da durch eine Nichtabwicklung von Zahlungen für diese Systeme über TARGET2 Schocks innerhalb des gesamten Finanzsystems (und im Fall von CLS sogar weltweit) übertragen werden könnten, werden diese Systeme als kritische Teilnehmer eingestuft.

Aus demselben Grund werden SIRPS, die über TARGET2 abwickeln, ebenfalls als kritische Teilnehmer klassifiziert.

Was PIRPS und andere Massenzahlungssysteme anbelangt, so ist davon auszugehen, dass es keine systemischen Auswirkungen für das TARGET2-System oder seine Teilnehmer hätte, wenn die Salden nicht mit Zentralbankgeld ausgeglichen würden. Daher werden diese Systeme als nichtkritische Teilnehmer eingestuft.

Organisationen/Institutionen aus dem Bereich Wertpapierverrechnung und -abwicklung

Organisationen/Institutionen aus dem Bereich Wertpapierverrechnung und -abwicklung sind Zentralverwahrer (Central Securities Depositories – CSDs), internationale Zentralverwahrer (International Central Securities Depositories – ICSDs) und zentrale Kontrahenten (Central Counterparties – CCPs).

54 Dabei handelt es sich um das Market Infrastructure Board (MIB), welches die Beschlussorgane des Eurosystems bei der Erfüllung der grundlegenden Aufgaben des ESZB unterstützt, insbesondere bei der Förderung des reibungslosen Betriebs der Zahlungssysteme.

Nach Auffassung des Eurosystems haben alle diese Systeme systemische Bedeutung, und der Ausfall eines (I)CSD/CCP würde sich gravierend auf das reibungslose Funktionieren von TARGET2 auswirken. Demzufolge gelten alle Organisationen/Institutionen aus dem Bereich Wertpapierverrechnung und -abwicklung als kritische Teilnehmer.

Zur Vermeidung einer Überregulierung muss die betreffende Zentralbank eventuell von Fall zu Fall prüfen, ob eine bestimmte Organisation/Institution aus diesem Bereich tatsächlich als kritischer Teilnehmer eingestuft werden sollte. Würde sich dabei herausstellen, dass der Ausfall einer solchen Organisation/Institution keine systemischen Auswirkungen für das TARGET2-System oder seine Teilnehmer hätte, könnte die betreffende Zentralbank diese als nichtkritischen Teilnehmer klassifizieren. Die betreffende Zentralbank muss die EZB über diese Neuklassifizierung informieren und die Gründe dafür erläutern. Die EZB wird dann eine Stellungnahme darüber abgeben, ob die Neuklassifizierung angemessen ist. Diese Stellungnahme wird dem betreffenden Eurosystem-Ausschuss zur weiteren Prüfung vorgelegt. Der Ausschuss kann beschließen, dass die von der Zentralbank zur Neuklassifizierung angewandten Kriterien allgemein zugrunde gelegt werden sollen.

3.7.2.3 „Servicebüro“ und „Mitglied/Konzentrator“

Neben der gemeinsamen Nutzung der SWIFTNet-Verbindung eines anderen SWIFT-Kunden bestehen für einen Nutzer zwei weitere Möglichkeiten, sich indirekt[55] mit SWIFTNet zu verbinden:

- Auslagerung des Tagesgeschäfts an einen Dritten, ein sogenanntes „Servicebüro“[56]
- Inanspruchnahme eines „Mitglieds/Konzentrators“ (neben der technischen Anbindung im vorherigen Punkt), das/der zusätzliche Dienstleistungen anbietet, z. B. die Übernahme der SWIFT-Administration und die Rechnungsstellung im Namen des Nutzers.

Kreditinstitute und eventuell auch Nebensysteme können beschließen, eines dieser Verbindungsmodelle zu nutzen. Sie erhalten einen BIC8 für die Adressierung über SWIFT und übernehmen die Verantwortung für ihre Nachrichten, weshalb sie als direkte Teilnehmer eingestuft werden, obgleich sie nur indirekt verbunden sind. Da das Routing des Zahlungsverkehrs mehrerer Nutzer über eine indirekte Verbindung erfolgen würde, hätte ein Ausfall der technischen Infrastruktur des Servicebüros oder des Mitglieds/Konzentrators möglicherweise systemische Auswirkungen.

55 Eine indirekte Verbindung mit SWIFTNet wird in der Regel von kleineren Instituten, die nach einer kostengünstigen SWIFTNet-Connectivity-Lösung suchen, genutzt.

56 Hierbei handelt es sich definitionsgemäß um: „*A SWIFT user or non-user organisation registered under the Shared Infrastructure Programme that provides services to connect SWIFT users that are not affiliated with such organisation.*“ (SWIFT-Glossar, Ausgabe September 2019).

Das Eurosystem hat zwar vorläufig beschlossen, dass Servicebüros zum gegenwärtigen Zeitpunkt nicht per se als kritische Teilnehmer gelten, aber es erscheint ratsam, diese wie kritische Teilnehmer zu behandeln, wenn der gesamte Zahlungsverkehr, dessen Routing über ein solches Unternehmen erfolgt, das 1 %-Kriterium für Kreditinstitute übersteigt. Wie bei Kreditinstituten hängt die Kritikalität auch von der Einstufung im Vorjahr ab: Servicebüros und Mitglieder/Konzentratoren, die als kritische Teilnehmer eingestuft werden, behalten diesen Status mindestens zwei Jahre bei.

Da zwischen den Servicebüros sowie den Mitgliedern/Konzentratoren und dem Eurosystem keine Rechtsbeziehung besteht, kann die Rechtsgrundlage für die Erfüllung der in diesem Leitfaden enthaltenen Vorschriften durch solche Unternehmen lediglich über die direkten Teilnehmer hergestellt werden.

3.7.3 Maßnahmen zur Gewährleistung der Sicherheit und operationellen Zuverlässigkeit von Nutzern

Der Ausschuss für Zahlungsverkehr und Marktinfrastrukturen (Committee on Payments and Market Infrastructures – CPMI) und die Internationale Organisation der Wertpapieraufsichtsbehörden (International Organization of Securities Commissions – IOSCO) haben Prinzipien für Finanzmarktinfrastrukturen (Principles for Financal Market Infrastructures – PFMI) herausgegeben.[57] Diese enthalten eine Reihe von Vorgaben, die die Betreiber von Zahlungssystemen erfüllen müssen. So bezieht sich etwa Prinzip 17 auf Aspekte der Sicherheit und der Zuverlässigkeit des Betriebs von Finanzmarktinfrastrukturen wie beispielsweise systemrelevanten Zahlungssystemen.

Um die teilnehmerbezogenen Betriebsrisiken zu steuern, besagt Prinzip 17: „*FMIs sollten die Einführung betrieblicher Mindestanforderungen für die Teilnehmer erwägen. Beispielsweise könnten je nach Rolle und Systemrelevanz der Teilnehmer unterschiedliche Betriebs- und Business-Continuity-Anforderungen definiert werden.“* Die Anforderungen haben zum Ziel, potenzielle teilnehmerbezogene betriebliche Schwachstellen für die FMIs zu beseitigen und im Einklang mit der entsprechenden CPMI-Strategie das mit der Endpunktsicherheit zusammenhängende Betrugsrisiko bei Großbetragszahlungen zu verringern.[58]

Die Maßnahmen zur Gewährleistung der Sicherheit und operationellen Zuverlässigkeit der Nutzer sollten im Verhältnis zu deren Systemrelevanz stehen. In den vorherigen Abschnitten wurden die Kriterien zur Bestimmung kritischer Teilnehmer erläutert. In Abschnitt 3.7.3.1 werden die Maßnahmen beschrieben, die sowohl für kritische als auch für nichtkritische Teilnehmer gelten. In Abschnitt 3.7.3.2 folgen die nur für kritische Teilnehmer anzuwendenden Verfahren.

57 Eine vollständige Beschreibung der internationalen Standards für Finanzmarktinfrastrukturen ist auf der Website der BIZ zu finden (www.bis.org/cpmi/info_pfmi.htm).

58 Eine vollständige Beschreibung der CPMI-Strategie zur Verringerung des mit der Endpunktsicherheit zusammenhängenden Betrugsrisikos bei Großbetragszahlungen ist auf der Website der BIZ zu finden (www.bis.org/cpmi/publ/d178.htm).

3.7.3.1 Für kritische und nichtkritische Teilnehmer anzuwendende Maßnahmen

Eine Maßnahme zur generellen Adressierung von Sicherheitsfragen ist die Aufnahme einer Klausel in die zwischen den Zentralbanken und den Nutzern getroffenen rechtlichen Vereinbarungen.

In Artikel 28 der Harmonisierten Bedingungen für die Teilnahme an TARGET2 werden die sicherheitsbezogenen Anforderungen definiert. Daraus geht klar hervor, dass die Gewährleistung eines angemessenen Schutzes der Vertraulichkeit, Integrität und Verfügbarkeit der Systeme der Nutzer in deren alleiniger Verantwortung liegt (siehe Artikel 28 Absatz 1).

Zudem legt Artikel 31 Absatz 4 dieser Bedingungen unter anderem fest, dass die Zentralbanken keine Haftung übernehmen, wenn ein Schaden von einem TARGET2-Teilnehmer verursacht wurde. Dies bedeutet, dass der TARGET2-Systembetreiber gegenüber einem TARGET2-Nutzer keinerlei Haftung übernimmt, wenn das reibungslose Funktionieren von TARGET2 aufgrund einer Störung beeinträchtigt wird, die durch eine Fehlfunktion des Systems dieses Nutzers verursacht wurde. Der Nutzer, der das Problem verursacht hat, muss jedoch die Zentralbank entschädigen (gemäß den in den Harmonisierten Bedingungen festgelegten Vorgaben und nach dem jeweils geltenden Recht), wenn diese aufgrund der Störung andere Nutzer schadlos halten musste.

Jährliche Selbstzertifizierung

Prinzip 17 der Prinzipien für Finanzmarktinfrastrukturen des CPSS und der IOSCO besagt: *„Eine Finanzmarktinfrastruktur (FMI) kann bei der Ausgestaltung ihres Steuerungsrahmens für Betriebsrisiken verschiedene internationale, nationale und branchenspezifische Standards, Richtlinien oder Empfehlungen zugrunde legen.“* Die Einhaltung solcher Geschäftsstandards kann dazu beitragen, ein hohes Maß an Sicherheit und Zuverlässigkeit des Betriebs zu gewährleisten.

Unter Berücksichtigung dessen fordert das Eurosystem die TARGET2-Nutzer mit eigenem TARGET2-Zugang/TARGET2-Anschluss dazu auf, selbst zu bescheinigen, dass sie die vom Eurosystem definierten Sicherheitsanforderungen erfüllen und dass innerhalb ihres Unternehmens Sicherheitsfragen in Übereinstimmung mit international anerkannten Standards wie beispielsweise dem Leitfaden für das Informationssicherheitsmanagement (Code of practice for information security management) (ISO 27001) adressiert werden. Die Einhaltung anderer Standards, deren Schwerpunkt auf der Informationssicherheit liegt, könnte ebenfalls akzeptabel sein.

Das Eurosystem benötigt eine Bestätigung, dass die Komponenten der TARGET2-Nutzer weiterhin die vom Eurosystem festgelegten Sicherheitsanforderungen erfüllen, auch wenn neue Gefährdungen, neue geschäftliche Anforderungen oder neu entdeckte Schwachstellen das Risikoprofil eines bestimmten selbstbetriebenen internen Systems des Nutzers ändern. Deshalb fordert das Eurosystem die TARGET2-

Nutzer auf, einmal pro Jahr selbst zu bescheinigen, dass die Anforderungen des Eurosystems eingehalten werden.

Dazu reicht eine Führungskraft auf Vorstands- oder vergleichbarer Ebene des TARGET2-Nutzers eine Selbstzertifizierungserklärung bei der zuständigen Zentralbank ein (siehe Anhang III). Aus dieser Erklärung soll hervorgehen, inwieweit die Anforderungen des Eurosystems erfüllt werden und welcher Standard zugrunde gelegt wurde. Die Zentralbanken senden die Selbstzertifizierungserklärung an ihre TARGET2-Nutzer, die bis zum Ende des jeweiligen Kalenderjahres bescheinigen, inwieweit sie die Anforderungen des Eurosystems eingehalten haben.

Ein TARGET2-Teilnehmer kann bei seiner jeweiligen Zentralbank eine eigene Selbstzertifizierungserklärung einreichen und gleichzeitig auch im Auftrag anderer TARGET2-Teilnehmer deren Umsetzungsgrad melden. Meldungen im Auftrag anderer Teilnehmer sind möglich, wenn die beiden folgenden Bedingungen erfüllt sind:

a) Alle Teilnehmer gehören zur selben „Gruppe“ im Sinne der Definition in Anhang II („Harmonisierte Bedingungen für die Teilnahme an TARGET2“) der TARGET2-Leitlinie und nutzen dieselbe Infrastruktur, um Zahlungen einzureichen.

b) Alle Teilnehmer, die durch eine einzige Selbstzertifizierungserklärung erfasst werden, setzen sämtliche anwendbaren Anforderungen vollständig um.

Weitere Einzelheiten bezüglich der Meldung im Auftrag anderer TARGET2-Teilnehmer finden sich in Anhang III der TARGET2-Leitlinie.

Im Fall einer Nichteinhaltung der Anforderungen des Eurosystems fügen die TARGET2-Nutzer der Selbstzertifizierungserklärung eine Beschreibung der größten Risiken bei, die sich daraus ergeben. Darüber hinaus müssen sie einen Aktionsplan zur Behebung der Situation erstellen und Fristen für die Umsetzung der einzelnen Maßnahmen festlegen. Die zuständige Zentralbank bewertet die Verbesserungsmaßnahmen und beurteilt auch, inwieweit die TARGET2-Nutzer die Anforderungen erfüllen. Für Nutzer, die in einem bestimmten Jahr die Selbstzertifizierungsanforderungen nicht vollständig erfüllen, können Maßnahmen ergriffen werden, die einen Anreiz bieten sollen, zeitnah eine vollständige Erfüllung zu erreichen.

Anforderungen der Netzwerkdienstleister an die Endpunktsicherheit

Die Teilnehmer ermöglichen ihrer jeweiligen Zentralbank dauerhaft Zugriff auf ihre Bestätigung der Einhaltung der Anforderungen ihres Netzwerkdienstleisters an die Endpunktsicherheit. Verweigert der Teilnehmer den dauerhaften Zugriff auf diese Bestätigung, dann wird dies als „gravierende Nichtumsetzung“ eingestuft.

Regelungen zur TARGET2-Selbstzertifizierung

Die Teilnehmer stellen ihrer jeweiligen Zentralbank einmal im Jahr eine TARGET2-Selbstzertifizierungerklärung in der Form zur Verfügung, wie sie für die von ihnen gehaltenen Konten erforderlich ist und entsprechend auf der Website der jeweiligen Zentralbank und der EZB auf Englisch veröffentlicht wurde. Stellt der Teilnehmer die TARGET2-Selbstzertifizierung nicht bereit (oder stellt eine veraltete Bestätigung bereit), dann wird dies als „gravierende Nichtumsetzung" eingestuft.

Monitoring und Störungsberichte

Für das reibungslose Funktionieren des TARGET2-Systems ist von entscheidender Bedeutung, dass ein Nutzer in der Lage ist, eine Kumulierung von Liquidität auf seinem Konto zu verhindern. Deshalb sind das Monitoring der Verfügbarkeit einer TARGET2-Komponente sowie Störungsberichte zwei Maßnahmen, die – längerfristig – zur Stabilität und Sicherheit des TARGET2-Systems beitragen können.

Sobald ein Nutzer am System teilnimmt, unterliegt er dem Monitoring[59] der zuständigen Zentralbank. Ist ein Nutzer von einer Störung betroffen, sind die zuständigen Mitarbeiter angehalten, die betreffende Zentralbank auf eigene Initiative unverzüglich zu informieren. Sobald der Nutzer den Betrieb wieder aufgenommen hat, kann ihm die Zentralbank ein Formular für einen Störungsbericht (Anhang II) zukommen lassen. In diesem Bericht muss der Nutzer die grundlegende Ursache des Problems, die Auswirkungen, die Schritte, die zur Lösung unternommen wurden, sowie die Maßnahmen, die ein erneutes Auftreten der Störung verhindern sollen, beschreiben.

Eine kleinere Betriebsstörung kann zwar zu Schwierigkeiten bei der Zahlungsabwicklung führen, gilt aber als unbedenklich, wenn sie bei kritischen Teilnehmern nicht länger als 30 Minuten[60] dauert. Solange die Dauer einer Störung diesen Zeitraum nicht überschreitet, ist kein Störungsbericht[61] erforderlich. Bei nichtkritischen Teilnehmern entscheidet die betreffende Zentralbank, ob ein solcher Bericht benötigt wird. Hierbei ist ausschlaggebend, ob die Störung Auswirkungen auf das reibungslose Funktionieren von TARGET2 oder auf andere Nutzer hatte. In diesem Zusammenhang ist anzumerken, dass kein Störungsbericht erforderlich ist, wenn ein Nutzer bewusst beschließt, die Zahlungsabwicklung für einen bestimmten Zeitraum auszusetzen, obgleich es keine technischen Probleme gibt. Um Irritationen zu vermeiden, ist der Nutzer gehalten, seine jeweilige Zentralbank so bald wie möglich über die Aussetzung zu informieren.

---

59 Grundprinzip VII (7.7.4): Die Systembetreiber sollten auch die „*Sicherheit und Zuverlässigkeit der Teilnehmer (...) überwachen, z. B. die Verfügbarkeit ihrer Komponenten während der üblichen Geschäftszeiten*".

60 Berechnet ab dem Zeitpunkt, an dem die Störung bemerkt wurde, bis zur erneuten Betriebsbereitschaft des Systems.

61 Störungsberichte für Nebensysteme, die auf T2S umsteigen, sind bis zum Migrationstermin auf T2S zu erstellen.

Wie oben erwähnt wird kein formeller Störungsbericht benötigt, wenn die Betriebsstörung nicht länger als 30 Minuten dauert oder eine bewusste Entscheidung, die Zahlungsabwicklung auszusetzen, getroffen wurde. Beobachtet eine Zentralbank jedoch wiederholt kurze Betriebsstörungen, setzt sie sich mit ihrem Nutzer in Verbindung und bittet diesen um Klärung, was letztendlich eine formelle Stellungnahme erforderlich machen könnte.

Die Nutzer müssen den ausgefüllten Störungsbericht innerhalb von zwei Geschäftstagen nach Auftreten der Störung an die betreffende Zentralbank zurücksenden. Es gibt zwei Arten von Störungsberichten:

- Wenn die Störung zu diesem Zeitpunkt bereits ausgewertet wurde, wird der erste Störungsbericht als abschließender Auswertungsbericht erachtet.
- Wenn die Störung noch untersucht wird, sollten die ursprünglichen Informationen, die bereits zur Verfügung gestellt werden können, als Zwischenbericht betrachtet werden. Der abschließende Auswertungsbericht, der die im Zwischenbericht enthaltenen Informationen vervollständigt, sollte dann spätestens einen Monat nach Auftreten der Störung an die Zentralbank geschickt werden.

Sobald der Störungsbericht abgeschlossen ist, wird er überprüft, analysiert und in einer Störungsübersicht vermerkt. Birgt das Verhalten eines Nutzers Risiken für das reibungslose Funktionieren von TARGET2 oder andere Nutzer, müssen angemessene Maßnahmen ergriffen werden; beispielsweise sollte die Führungsebene des Nutzers auf das Problem aufmerksam gemacht werden.

Störungen, die die Verfügbarkeit des Nutzers betreffen, sind wahrscheinlich die einzigen, die vom Systembetreiber selbst erkannt werden können, indem dieser die gegenwärtige Zahlungsabwicklung mit dem normalen Verlaufsmuster vergleicht. Bemerkt eine Zentralbank eine Abweichung vom normalen Verlauf und vermutet, dass der Nutzer möglicherweise schwerwiegende Probleme hinsichtlich der Verfügbarkeit hat, über die sie nicht informiert wurde, wird der betreffende Nutzer kontaktiert und um eine Erklärung gebeten. Allerdings werden die Nutzer dazu ermutigt, regelmäßig, und wenn möglich auch im Tagesverlauf, Kontenabstimmungen durchzuführen. Sie sollten dabei unterschiedliche systemseitig bereitgestellte Instrumente und Funktionen verwenden, wie z. B. tägliche Kontoauszüge (MT 940/950) und Senderbenachrichtigungen (MT 012).

Außerdem sollten sich die Teilnehmer über marktgängige Tools zur Identifizierung und Verhinderung betrügerischer Zahlungen informieren und diese auch einsetzen. Solche Tools werden beispielsweise von Nachrichtennetzen sowie von anderen Dritten angeboten.

Darüber hinaus werden die Nutzer darum gebeten, Sicherheitsprobleme, die die Vertraulichkeit und Integrität betreffen, unverzüglich und auf eigene Initiative ihrem National Service Desk zu melden. Werden Informationen über solche Probleme öffentlich gemacht, könnte sich dies negativ auf die

Reputation des gesamten TARGET2-Systems auswirken. Daher ist die schnellstmögliche Meldung solcher Fälle unerlässlich, um sicherzustellen, dass eine aussagekräftige und präzise Kommunikation vorbereitet und möglicherweise andere Maßnahmen zur Beruhigung der Finanzmärkte und der Öffentlichkeit eingeleitet werden können.

Wie in Abschnitt 9.2 dargelegt kann der National Service Desk den Teilnehmer darüber hinaus im Bedarfsfall auch bei der Behebung der Störung unterstützen, etwa bei der Umsetzung von Maßnahmen, die es ermöglichen, die Gelder der Nutzer zu schützen und eine Fortsetzung/Ausweitung der betrügerischen Tätigkeiten zu verhindern.

3.7.3.2 Nur für kritische Teilnehmer anzuwendende Maßnahmen

Business Continuity (Aufrechterhaltung des Geschäftsbetriebs):

Am 31. Mai 2006 verabschiedete der EZB-Rat die Überwachungsanforderungen zur Gewährleistung der Business Continuity bei systemrelevanten Zahlungssystemen (Business continuity oversight expectations for systemically important payment systems – SIPS) (im Folgenden „Oversight Expectations"). Es handelt sich dabei um erweiterte Anforderungen der Zahlungsverkehrsüberwachung an die Vorkehrungen zur Aufrechterhaltung des Geschäftsbetriebs von Euro-Zahlungsverkehrssystemen, die für die Stabilität des Finanzsystems von Bedeutung sind.

Die „Oversight Expectations" enthalten einen Abschnitt, der die Teilnehmer von SIPS betrifft, denn „ein technischer Ausfall der kritischen Systemteilnehmer kann zu systemischen Risiken führen." Gemäß diesem Dokument müssen Teilnehmer, die vom Systembetreiber als kritisch eingestuft wurden, bestimmte Mindestanforderungen erfüllen, damit die Aufrechterhaltung des Betriebs im Falle einer Störung sichergestellt ist. Laut den „Oversight Expectations" obliegt dem Systembetreiber die Verantwortung dafür, die Erfüllung dieser Anforderungen zu überprüfen.

Die kritischen Teilnehmer müssen vor allem bestätigen, dass:

- Business-Continuity-Pläne erstellt werden und Verfahren zu deren Einhaltung verfügbar sind
- ein Ausweichstandort vorhanden ist
- das Risikoprofil des Ausweichstandorts sich von dem des Primärstandorts unterscheidet. Dies bedeutet, dass sich der Ausweichstandort in deutlicher Entfernung vom Primärstandort befinden muss und nicht von denselben Komponenten der physischen Infrastruktur[62] abhängen darf.

[62] Zu beachten ist, dass keine Verpflichtung zur Nutzung unterschiedlicher Hardware-Marken und/oder Software-Komponenten besteht, z. B. zur Installation von MS Windows am (eigentlichen) Primärstandort und von UNIX-Systemen am Ausweichstandort. Die Aussage „*nicht von denselben Komponenten der physischen Infrastruktur abhängen*" unterstreicht, dass Ausweichstandorte nicht auf die Infrastrukturkomponenten (z. B. Transport, Telekommunikation,

Dadurch wird das Risiko, dass beide von derselben Störung betroffen sind, minimiert. So sollte beispielsweise der Ausweichstandort an ein anderes Energieversorgungsnetz und eine andere Hauptfernmeldeleitung als der Primärstandort angeschlossen sein.[63]

In diesem Zusammenhang wird berücksichtigt, dass die kritischen Teilnehmer lediglich für Dinge, die in ihren direkten Einflussbereich fallen, verantwortlich sein können. Sie sind zum Teil von den Anbietern abhängig und nicht haftbar, wenn sich die Ausfallsicherheit eines von Dritten bereitgestellten Dienstes als weniger verlässlich erweist als erwartet. Die kritischen Teilnehmer sollten jedoch bestrebt sein, die Festlegung einer angemessenen Ausfallsicherheit in dem mit den Anbietern geschlossenen Vertrag sicherzustellen. So sollte sich z. B. ein Telekommunikationsanbieter im Rahmen der vertraglichen Vereinbarungen verpflichten, mehrere Routing-Einrichtungen bereitzustellen.

- Im Falle einer größeren Betriebsstörung, die dazu führt, dass auf den Primärstandort nicht zugegriffen werden kann und/oder für den Betrieb notwendige Mitarbeiter nicht verfügbar sind, ist der kritische Teilnehmer in der Lage, den normalen Betrieb vom Ausweichstandort aus wiederaufzunehmen und so den Geschäftstag ordnungsgemäß abzuschließen und den folgenden Geschäftstag wieder zu beginnen.
- Um die für die Verlagerung vom Primärstandort auf den Ausweichstandort benötigte Zeit zu überbrücken, gibt es Verfahren, die die Durchführung der kritischsten Transaktionen gewährleisten.
- Die Fähigkeit, Störungen zu bewältigen, wird mindestens einmal jährlich geprüft, und wichtige Mitarbeiter werden angemessen geschult.

Die kritischen Teilnehmer sollten im Wege der Selbstzertifizierung erklären, inwieweit sie den „Oversight Expectations“ entsprechen (siehe Abschnitt 3.7.3). Die Zentralbanken überprüfen dann, ob die „Oversight Expectations“ erfüllt werden. Anhand von Tests wird überprüft, ob die zur Aufrechterhaltung des Geschäftsbetriebs getroffenen Vorkehrungen effektiv sind (siehe Abschnitt 10).

Wasser- und Energieversorgung) angewiesen sein sollten, die am Primärstandort genutzt werden.

63 Basierend auf den „High-level principles for business continuity“, erarbeitet von: The Joint Forum, Bank für Internationalen Zahlungsausgleich, August 2006.

Tests

Um zu kontrollieren, ob die Business-Continuity-Verfahren wirksam sind, müssen diese regelmäßig getestet werden.

Das Prinzip 17 der PFMI legt fest, dass auch die Systemteilnehmer in die Tests der klar dokumentierten Business-Continuity-Verfahren einbezogen werden sollten.

Grundsätzlich können die Tests in zwei Szenarien unterteilt werden. Das erste Szenario beinhaltet die bilaterale Prüfung der zwischen dem kritischen Teilnehmer und seiner Zentralbank vereinbarten Contingency-Verfahren. Diese Prüfung ist bereits integraler Bestandteil des Test-Programms für Nutzer, das diese vor ihrer Teilnahme an TARGET2 durchlaufen müssen.

Die Teilnahme an den Tests ist für kritische Teilnehmer obligatorisch. Der erfolgreiche Verlauf wird von den betreffenden Zentralbanken überwacht.

Unterzeichnung der Selbstzertifizierungserklärung durch die (interne oder externe) Revision

Wie in Abschnitt 3.7.23.1 beschrieben, muss die Selbstzertifizierungserklärung von einer Führungskraft auf Vorstands- oder vergleichbarer Ebene unterzeichnet werden. Kritische TARGET2-Teilnehmer müssen die Selbstzertifizierungserklärung zusätzlich von einem (internen oder externen) Revisor unterzeichnen lassen.

3.7.4 Umsetzung

3.7.4.1 Rechtliche Durchsetzbarkeit

In den Harmonisierten Bedingungen für die Teilnahme an TARGET2, vor allem in Artikel 28 (Sicherheitsanforderungen), werden die Sicherheitsmaßnahmen generell erläutert und somit das Rahmenwerk für die rechtliche Durchsetzbarkeit der in diesem Leitfaden beschriebenen detaillierten Maßnahmen festgelegt. Die praktische und rechtliche Umsetzung, durch die die einzelnen Maßnahmen für Nutzer verbindlich werden, liegt jedoch in der nationalen Zuständigkeit jeder Zentralbank. Demzufolge obliegt es den Zentralbanken zu entscheiden, wie sie die Sicherheitsmaßnahmen für Nutzer in die rechtlichen Vereinbarungen mit ihren Nutzern integrieren (z. B. durch einen Vertragsanhang, eine Veröffentlichung auf der Website mit einem Verweis im Vertrag, ein Schreiben der Zentralbank usw.). Da sich die Gesetzgebung je nach Land unterscheidet und um sicherzustellen, dass die Maßnahmen in allen an TARGET2 teilnehmenden Ländern auf ähnliche Weise und im Einklang mit den Harmonisierten Bedingungen für die TARGET2-Teilnahme rechtlich umgesetzt werden, haben die Zentralbanken darüber Bericht erstattet, auf welche Weise dies erreicht wurde.

3.7.4.2 Übergangsphase

Die Maßnahmen für kritische Teilnehmer definieren die Zugangskriterien, die diese im Idealfall vor der Teilnahme an TARGET2 erfüllen sollten. Neue kritische Teilnehmer müssen selbst bescheinigen, dass die Informationssicherheit im Einklang mit international anerkannten Standards behandelt wird und die im Abschnitt „Business Continuity“ beschriebenen Business-Continuity-Anforderungen erfüllt werden. Darüber hinaus müssten Business-Continuity-Verfahren gemäß dem festgelegten Testprogramm (siehe Abschnitt 10) erfolgreich getestet werden.

Einem kritischen Teilnehmer steht zur Erfüllung der spezifischen Anforderungen hinsichtlich der Sicherheit und der Zuverlässigkeit des Betriebs eine Zeitspanne von 18 Monaten zur Verfügung. Dieser Zeitraum beginnt mit dem Datum seiner Einstufung als kritischer Teilnehmer.

Ferner sollten die betreffenden Zentralbanken einen kritischen Teilnehmer kontaktieren, sobald dieser ermittelt wurde, und ihn bitten, den Stand seiner Vorbereitungen im Hinblick auf die oben beschriebene Umsetzungsfrist anzugeben. Unterscheidet sich in dieser Einführungsphase die tatsächliche Situation stark von den in diesem Leitfaden erläuterten Anforderungen, sollte ein Arbeitsplan erstellt und dieser von der entsprechenden Zentralbank überwacht werden, damit die erforderlichen Maßnahmen innerhalb der oben erwähnten Frist umgesetzt werden können.

3.7.4.3 Konstruktiver Ansatz

Es sollte ausdrücklich darauf hingewiesen werden, dass das Ziel des Rahmenwerks nicht darin besteht, Kreditinstitute von der Teilnahme an TARGET2 abzuhalten. Die beschriebenen Maßnahmen zielen vielmehr darauf ab, die Ausfallsicherheit und Stabilität des gesamten TARGET2-Systems zu stärken und dadurch zur Stabilität der Finanzmärkte beizutragen.

Wenn ein TARGET2-Nutzer eine der Anforderungen nicht erfüllt, wird die zuständige Zentralbank diesen Teilnehmer auf die aus den festgestellten Schwachstellen resultierenden Risiken hinweisen. In enger Zusammenarbeit mit dem betreffenden TARGET2-Nutzer entwickelt die zuständige Zentralbank ein Programm zur schrittweisen Verbesserung der Situation. Falls eine solche schrittweise Verbesserung durch einen anhaltenden Mangel an Bereitschaft oder in böser Absicht verhindert wird, sollte der TARGET2-Nutzer normalerweise aus dem TARGET2-System ausgeschlossen werden. Eine endgültige Entscheidung hierüber wird aber erst nach eingehender Prüfung der Sachlage auf Eurosystem-Ebene getroffen.

3.7.5 Kommunikation und Koordinierung

Für eine effektive und vertrauensvolle Kommunikation und Koordinierung zwischen den Zentralbanken und ihren Nutzern in Sicherheitsfragen ist eine klare Organisationsstruktur unabdingbar. Es obliegt der Verantwortung aller Zentralbanken und ihrer Nutzer, die ordnungsgemäße und effiziente Durchführung

der notwendigen Maßnahmen innerhalb der betreffenden Unternehmen sicherzustellen. Wenn zwischen den beteiligten Parteien sicherheitsempfindliche Informationen ausgetauscht werden, muss gewährleistet sein, dass diese Informationen ordnungsgemäß gekennzeichnet und angemessen geschützt werden.

3.7.6 Vertraulichkeit

Sämtliche von den Nutzern zur Verfügung gestellten Informationen werden vom Eurosystem vertraulich behandelt und lediglich dazu verwendet zu überprüfen, ob die Nutzer die Vorgaben des Eurosystems einhalten, damit dieses seiner Verantwortung als Systembetreiber im Sinne der PFMI gerecht wird.

Falls Nutzer sicherheitsempfindliche Informationen im Zusammenhang mit dem Rahmenwerk erhalten, sind diese selbstredend vertraulich zu behandeln.

3.7.7 Berichterstattung

Die Zentralbanken sind für die Erhebung der erforderlichen Informationen und die Überwachung aller Folgemaßnahmen verantwortlich. Wurden beispielsweise die Vorkehrungen eines Nutzers zur Aufrechterhaltung des Geschäftsbetriebs als ineffektiv eingeschätzt, ist zu erörtern, wie die festgestellten Mängel behoben und bis wann die Abhilfemaßnahmen umgesetzt werden können.

Da das Eurosystem als Ganzes die Verantwortung als Systembetreiber trägt, müssen die von den Zentralbanken gesammelten Informationen über Störungen, die sich auf das reibungslose Funktionieren von TARGET2 auswirken könnten, dem zuständigen Ausschuss auf Eurosystem-Ebene zur Verfügung gestellt werden. Angesichts der Sensibilität der Informationen ist deren streng vertrauliche Behandlung von größter Wichtigkeit. Es könnte sogar in Betracht gezogen werden, die Informationen anonymisiert darzustellen.

Der Ausschuss muss die Informationen prüfen und von Fall zu Fall erwägen, welche Maßnahmen getroffen werden sollten, damit gewährleistet ist, dass ein bestimmter Nutzer kein Risiko für das reibungslose Funktionieren von TARGET2 und für die anderen Nutzer darstellt.

Das Meldeformat und das genaue Verfahren zur Übermittlung von Informationen an den zuständigen Ausschuss werden auf Eurosystem-Ebene festgelegt. Diese internen Verfahren des Eurosystems sollen sicherstellen, dass Zentralbanken, die nicht direkt an der Datenerhebung beteiligt sind, Zugang zu diesen Daten erhalten und die Informationen effektiv und einheitlich ausgetauscht werden.

3.7.8 Überprüfungsklausel

Damit das allgemeine Rahmenwerk weiterhin angemessen bleibt, muss es regelmäßig überprüft werden.

So sind z. B. die zur Bestimmung der kritischen Teilnehmer angewandten Kriterien nicht in Stein

gemeißelt. Es obliegt dem Eurosystem, die Kriterien unter Berücksichtigung der während des TARGET2-Betriebs gewonnenen Erfahrungen oder angesichts neuer Forschungsergebnisse zu systemischen Risiken entsprechend anzupassen.

Weiterhin könnte der von einzelnen Kreditinstituten erzeugte Zahlungsverkehr Veränderungen unterliegen. Wenn ein Kreditinstitut z. B. nach einer Fusion plötzlich mehr als 1 % des Transaktionswerts über TARGET2 abwickelt, müsste dieses Kreditinstitut möglicherweise als kritischer Teilnehmer eingestuft werden und die für diese Unternehmen festgelegten Anforderungen erfüllen. Analog gilt: Sinkt der Wert der Zahlungen eines kritischen Teilnehmers signifikant und liegt lange genug unter dem Schwellenwert, könnte der Teilnehmer als nichtkritischer Teilnehmer eingestuft werden.

Deshalb werden die Kriterien zur Bestimmung kritischer Teilnehmer sowie deren Einstufung mindestens einmal jährlich überprüft, wobei bei Bedarf auch eine anlassbezogene Aktualisierung der Einstufung erfolgen kann. Darüber hinaus sind die Nutzer verpflichtet, die Zentralbanken frühzeitig von wesentlichen Änderungen ihrer Geschäftspraktiken in Kenntnis zu setzen.

3.7.9 Handlungsrahmen zur Gewährleistung der Umsetzung der Anforderungen

3.7.9.1 Methodik in Bezug auf die Umsetzung der Anforderungen

Bei der Beurteilung der Frage, inwieweit PM-Kontoinhaber und Nebensysteme die TARGET2-Selbstzertifizierungserklärung insgesamt umgesetzt haben, legen die Zentralbanken einen quantitativen Ansatz zugrunde (die Umsetzung der Business-Continuity-Anforderungen wird nur bei kritischen Teilnehmern geprüft). Dementsprechend werden die Teilnehmer den folgenden drei Umsetzungsstufen zugeordnet:

- **Vollständige Umsetzung:** Die PM-Kontoinhaber und Nebensysteme erfüllen 100 % der Anforderungen (d. h. alle 15 Anforderungen an die Informationssicherheit und − nur bei kritischen Teilnehmern − alle 6 Business-Continuity-Anforderungen).
- **Geringfügige Nichtumsetzung:** Die PM-Kontoinhaber und Nebensysteme erfüllen weniger als 100 %, aber mindestens 66 % der Anforderungen (d. h. mindestens 10 Anforderungen an die Informationssicherheit und − nur bei kritischen Teilnehmern − mindestens 4 Business-Continuity-Anforderungen).
- **Gravierende Nichtumsetzung:** Die PM-Kontoinhaber und Nebensysteme erfüllen weniger als 66 % der Anforderungen (d. h. weniger als 10 Anforderungen an die Informationssicherheit oder − nur bei kritischen Teilnehmern − weniger als 4 Business-Continuity-Anforderungen).

Können PM-Kontoinhaber oder Nebensysteme nachweisen, dass eine bestimmte Anforderung nicht auf sie anwendbar ist, dann gilt die betreffende Anforderung im Rahmen der obigen Beurteilung als umgesetzt.

Verweigert der Teilnehmer den dauerhaften Zugang zur Bestätigung über die Einhaltung der Anforderungen des Netzwerkdienstleisters an die Endpunktsicherheit oder stellt die TARGET2-Selbstzertifizierungerklärung nicht zur Verfügung, dann wird dies als „gravierende Nichtumsetzung“ eingestuft.

3.7.9.2 Implementierungsmaßnahmen

Kann ein PM-Kontoinhaber oder ein Nebensystem die Anforderungen TARGET2-Selbstzertifizierungserklärung nicht vollständig umsetzen, wenden die Zentralbanken die in diesem Abschnitt beschriebenen Implementierungsmaßnahmen an. Zu beachten ist jedoch, dass es sich beim vorliegenden Handlungsrahmen nicht um eine Standardlösung handelt, die die Zentralbanken automatisch auf alle PM-Kontoinhaber und Nebensysteme anwenden können, welche nicht alle Anforderungen vollständig umsetzen. Es handelt sich vielmehr um eine Orientierungshilfe bezüglich der Maßnahmen, die bei einem Teilnehmer, der gewisse Anforderungen nicht umgesetzt hat, nach einer Analyse des jeweiligen Falles angewendet werden können.

Aktiver Dialog (moralische Appelle)

Diese Maßnahme betrifft die formelle und informelle Kontaktaufnahme der Zentralbank mit einem Teilnehmer, der gewisse Anforderungen nicht umgesetzt hat. Ziel ist es, dass der Teilnehmer frühestmöglich eine vollständige Umsetzung der Anforderungen erreicht. Folgende Schritte können dabei u. a. ergriffen werden:

- Der Teilnehmer wird aufgefordert, einen Aktionsplan vorzulegen, in dem die Maßnahmen dargelegt sind, durch die die Situation behoben wird. Dieser Aktionsplan sollte auch die geplanten Fristen für die Implementierung der einzelnen Maßnahmen enthalten. Die Zentralbank wird die vom Teilnehmer dargelegten Maßnahmen prüfen und ggf. um eine zusätzliche Klarstellung oder weitere Informationen bitten.
- Die Zentralbank wendet sich mit einem offiziellen Schreiben, das von einem leitenden Beamten unterzeichnet wurde, an eine Führungskraft auf Vorstands- oder vergleichbarer Ebene des Teilnehmers. Dieses Schreiben soll den Teilnehmer an seine Verantwortung und Verpflichtung erinnern, seine (für die Einreichung von Transaktion an TARGET2 genutzte) lokale Infrastruktur hochgradig sicher und zuverlässig zu betreiben.

Darin sollten auch die zusätzlichen Implementierungsmaßnahmen aufgeführt werden, die die Zentralbank ergreifen kann, falls die im Aktionsplan aufgeführten Maßnahmen zur Erzielung einer vollständigen Umsetzung der Anforderungen nicht angemessen erscheinen oder die Fristen für deren Implementierung den Erwartungen des Eurosystems nicht entsprechen. In diesem Zusammenhang sollte auch daran erinnert werden, welche Folgen eine Suspendierung/Beendigung der Teilnahme nach sich ziehen würde.

Die Zentralbank sollte die Führungskraft auf Vorstands- oder vergleichbarer Ebene darüber hinaus jedes Mal erneut mittels eines offiziellen Schreibens informieren, wenn der Umsetzungsgrad zusätzliche Implementierungsmaßnahmen erfordert.

- Die Zentralbank informiert die zuständige Aufsichtsbehörde über den Umsetzungsgrad des Teilnehmers. Die Aufsichtsbehörde sollte dann auch jedes Mal informiert werden, wenn aufgrund des Umsetzungsgrads die Einführung zusätzlicher Implementierungsmaßnahmen notwendig wird.

Verstärktes Monitoring

Teilnehmer berichten monatlich an die NZB über die erreichten Fortschritte in Bezug auf ihren Aktionsplan. Diese Meldung hat schriftlich zu erfolgen und ist von einer Führungskraft auf Vorstands- oder vergleichbarer Ebene zu unterzeichnen.

Neben dem Monitoring des Aktionsplans führt die Zentralbank auch ein verstärktes Monitoring der TARGET2-Aktivität des Teilnehmers (in Bezug auf den Wert und das Volumen der von ihm durchgeführten Transaktionen) durch, um Veränderungen im Zahlungsverhalten des Teilnehmers früher erkennen zu können. Wie genau das verstärkte Monitoring des Teilnehmers durchgeführt wird, liegt im Ermessen der jeweiligen Zentralbank. Hierbei spielen auch die Größe und das Geschäftsmodell des Teilnehmers eine Rolle.

Wird ein PM-Kontoinhaber oder ein Nebensystem unter verstärktes Monitoring gestellt, dann wird eine monatliche Strafgebühr in Höhe der monatlichen festen Gebühren für TARGET2 erhoben. Somit richtet sich die Strafgebühr nach der relativen Größe des PM-Kontoinhabers oder des Nebensystems. Die Gebühr dient zwei Zwecken: Erstens stellt sie einen finanziellen Anreiz für PM-Kontoinhaber und Nebensysteme dar, frühestmöglich eine vollständige Umsetzung der Anforderungen zu erreichen. Zweitens dient sie der Entschädigung der betreffenden Zentralbank für den erforderlichen Zusatzaufwand, der sich aus dem verstärkten Monitoring ergibt.

Suspendierung von TARGET2-Kontoinhabern

Im Falle einer Suspendierung muss die Zentralbank jede Zahlung, die der suspendierte Teilnehmer in TARGET2 erhält und/oder sendet, separat genehmigen. Diese Genehmigung basiert auf einer gesonderten Bestätigung, die die Zentralbank vom Teilnehmer über die auf lokaler Ebene vereinbarten Kommunikationswege erhält (z. B. telefonische Bestätigung, E-Mail-Verifizierung usw.).

Ein Teilnehmer, der von der Teilnahme an TARGET2 suspendiert ist, muss eine monatliche Strafgebühr in doppelter Höhe der monatlichen festen Gebühren für das RTGS-System entrichten. Die Gebühr stellt einen finanziellen Anreiz für den Teilnehmer dar, frühestmöglich eine vollständige Umsetzung der Anforderungen zu erreichen. Zudem dient sie als Entschädigung der betreffenden Zentralbank für den erforderlichen Zusatzaufwand, der sich aus der Suspendierung ergibt (d. h., die Gebühr unterliegt nicht der Aufteilung der Umsatzerlöse zwischen den Zentralbanken des Eurosystems).

Angesichts der massiven wirtschaftlichen Folgen, die eine Suspendierung für die betroffene Partei mit sich brächte, wird eine Entscheidung über eine Suspendierung unter Beachtung des Grundsatzes der Verhältnismäßigkeit getroffen.

Beendigung der TARGET2-Teilnahme

Wird ein TARGET2-Teilnehmer suspendiert, dann spricht die betreffende Zentralbank gleichzeitig mit dreimonatiger Frist die Kündigung für dessen TARGET2-Konto oder -Konten aus, falls der Teilnehmer keine deutlichen Fortschritte in Richtung einer vollständigen Umsetzung der Anforderungen macht.

Bei Beendigung der TARGET2-Teilnahme und einer entsprechenden Kontenschließung fällt eine einmalige Strafgebühr von 1 000 € an. Diese dient der Entschädigung der betreffenden Zentralbank für den erforderlichen Zusatzaufwand, der sich aus der Beendigung ergibt.

Angesichts der massiven wirtschaftlichen Folgen, die eine Beendigung der TARGET2-Teilnahme für die betroffene Partei mit sich brächte, wird eine entsprechende Entscheidung unter Beachtung des Grundsatzes der Verhältnismäßigkeit getroffen.

3.7.9.3 Zeitrahmen für die Umsetzung der Maßnahmen

Die Implementierungsmaßnahmen gelten für Teilnehmer, die die Anforderungen nicht vollständig umgesetzt haben. Die Implementierung erfolgt stufenweise, wobei berücksichtigt wird, welchen Umsetzungsgrad der Teilnehmer erreicht hat. In der nachfolgenden Tabelle wird zwischen den Implementierungsmaßnahmen für die Teilnehmer der Kategorien „geringfügige Nichtumsetzung“ und „gravierende Nichtumsetzung“ unterschieden.

Die erste Stufe der Maßnahmen tritt am Ende des Jahres in Kraft, in dem die betreffende Erhebung stattgefunden hat (z. B. Ende 2021 im Hinblick auf das Ergebnis der Überprüfung der Endpunktsicherheit 2021). Die zweite Stufe würde dann am Ende des Folgejahres wirksam werden (z. B. Ende 2022 im Hinblick auf das Ergebnis der Erhebung über die Endpunktsicherheit 2021).

	Erste Stufe der Implementierungsmaßnahmen 31. Dezember des Jahres *X*	Zweite Stufe der Implementierungsmaßnahmen 31. Dezember des Jahres *X+1*
Geringfügige Nichtumsetzung	**Aktiver Dialog** →	**Verstärktes Monitoring**
Gravierende Nichtumsetzung	**Aktiver Dialog** →	**Suspendierung** **+** **Beendigung der Teilnahme***

Beim vorliegenden Rahmen handelt es sich nicht um eine Standardlösung, die die Zentralbanken automatisch bei allen PM-Kontoinhabern und Nebensystemen, welche noch keine vollständige Umsetzung erzielt haben, anwenden können. Vielmehr dient er als Orientierungshilfe im Hinblick auf die Maßnahmen, die bei einem Teilnehmer, der gewisse Anforderungen nicht umgesetzt hat, nach einer Analyse des jeweiligen Falles zur Anwendung kommen können. Dies gilt insbesondere dann, wenn es um die Suspendierung eines PM-Kontoinhabers oder eines Nebensystems bzw. um die Beendigung von deren Teilnahme an TARGET2 geht. Bei der Entscheidung, welche Maßnahmen in Bezug auf die vollständige Umsetzung der Anforderungen angewendet werden sollten, sollte auch berücksichtigt werden, inwieweit ein Teilnehmer die Anforderungen seines Netzwerkdienstleisters an die Endpunktsicherheit erfüllt.

3.8 Beendigung der Teilnahme, Suspendierung von Teilnehmern und Behandlung von Teilnehmern, die sich in Abwicklung befinden

Im Einklang mit der TARGET2-Leitlinie erfolgt eine **fristlose Beendigung der Teilnahme oder Suspendierung** eines Teilnehmers (PM-Kontoinhaber, TIPS-Geldkontoinhaber oder T2S-Geldkontoinhaber) an einem TARGET2-Komponentensystem durch eine Zentralbank ohne vorherige Ankündigung, wenn:

a) ein Insolvenzverfahren über das Vermögen des Teilnehmers eröffnet wird, und/oder

b) der Teilnehmer die Zugangsvoraussetzungen für die Teilnahme am betreffenden Komponentensystem nicht mehr erfüllt.

Die Zentralbank **kann** die Teilnahme eines Teilnehmers an einer TARGET2-Komponente ohne vorherige Ankündigung **beenden oder diesen suspendieren**, wenn:

a) ein oder mehrere Ausfallereignisse (außer den oben genannten) eintreten,

b) der Teilnehmer erheblich gegen die Harmonisierten Bedingungen für die Eröffnung und Führung eines PM-Kontos oder die Harmonisierten Bedingungen für die Eröffnung und Führung eines TIPS-Geldkontos oder eines T2S-Geldkontos verstößt,

c) der Teilnehmer wesentlichen Pflichten gegenüber der Zentralbank nicht nachkommt,

d) der Teilnehmer aus einer TARGET2 Closed User Group (CUG) oder, im Falle direkt angeschlossener T2S-Geldkontoinhaber, von einer T2S Closed Group of Users (CGU) ausgeschlossen wird oder dieser aus anderen Gründen nicht mehr angehört,

e) der TIPS-Geldkontoinhaber keine gültige Vereinbarung mit einem TIPS-Netzwerkdienstleister mehr besitzt, der ihm die notwendige Verbindung mit der TIPS-Plattform herstellt,

f) ein anderes Ereignis im Zusammenhang mit einem Teilnehmer eintritt, das nach Ansicht der Zentralbank die Stabilität insgesamt, die Solidität oder die Sicherheit ihrer TARGET2-Komponente oder eines anderen TARGET2-Komponentensystems gefährden oder die Zentralbank in der Erfüllung ihrer Aufgaben, wie sie in den entsprechenden nationalen Gesetzen sowie in der Satzung des Europäischen Systems der Zentralbanken und der Europäischen Zentralbank dargelegt sind, beeinträchtigen würde, und/oder unter Risikoerwägungen eine Gefahr darstellt,

g) eine NZB einen Teilnehmer gemäß Anhang III Nummer 12 der TARGET2-Leitlinie vorläufig oder endgültig vom Zugang zu Innertageskrediten ausschließt.

Wird ein TIPS-Geldkontoinhaber von einer Zentralbank suspendiert oder seine Teilnahme an

TARGET2 von einer Zentralbank beendet, muss die Zentralbank die anderen Zentralbanken und PM-Kontoinhaber in allen TARGET2-Komponentensystemen sofort per ICM-Nachricht darüber informieren. Eine solche Nachricht ist einer Nachricht gleichgestellt, die von der Heimatzentralbank des PM-Kontoinhabers, der die Nachricht erhält, versendet wurde.

Inhaber von verknüpften PM-Konten sind verpflichtet, die mit ihnen verbundenen TIPS-Geldkontoinhaber zu informieren, sobald ein TIPS-Geldkontoinhaber suspendiert oder seine Teilnahme an TARGET2 beendet wurde.

3.8.1 Auswirkungen der Suspendierung eines PM-Kontoinhabers

- Das PM-Konto und die Unterkonten werden unverzüglich entsprechend gekennzeichnet.
- Die automatische Abwicklung von Zahlungen über diese Konten ist nicht mehr möglich.
- In einem laufenden Abwicklungsprozess (Algorithmus) befindliche Zahlungen sind von der Suspendierung nicht betroffen.
- Die Zentralbank muss Zahlungen in der Warteschlange über das ICM explizit bestätigen, bevor diese über das PM-Konto abgewickelt werden.
- Vom suspendierten PM-Kontoinhaber nach dessen Suspendierung gesendete Zahlungen werden zur Bestätigung durch die Zentralbank über das ICM „geparkt“.
- An den suspendierten PM-Kontoinhaber nach dessen Suspendierung gesendete Zahlungen werden zur Bestätigung durch die Zentralbank über das ICM „geparkt“.
- Auf welcher Grundlage die Zentralbank die Zahlungen bestätigt, ist von den nationalen Bestimmungen abhängig.

Die **Beendigung der Teilnahme eines PM-Kontoinhabers** führt zur Löschung dieses Teilnehmers aus dem System.

Dabei ist Folgendes zu beachten:
- Was die Vereinbarungen zum Liquiditätspooling betrifft, so tauschen die Zentralbanken, die Vertragspartei einer Vereinbarung über die Aggregierung von Deckungsmitteln (aggregated liquidity – AL) sind und für die PM-Kontoinhaber, die eine solche AL-Vereinbarung geschlossen haben und an ihrer TARGET2-Komponente teilnehmen, als Geschäftspartner fungieren, sämtliche Informationen, die für die Erfüllung ihrer Aufgaben und Pflichten im Rahmen einer AL-Vereinbarung erforderlich sind, aus. Diese Zentralbanken benachrichtigen unverzüglich die leitendende Zentralbank, wenn sie einen Verwertungsfall im Zusammenhang mit der AL-Gruppe oder einem AL-Gruppenmitglied, einschließlich der Zentrale und deren Zweigstellen, bemerken.

- Im Falle der Suspendierung eines PM-Kontoinhabers kann die Zentralbank wählen, ob der suspendierte Teilnehmer weiterhin im TARGET2-Directory veröffentlicht werden soll oder nicht. Aus dem Eintrag im TARGET2-Directory ist nicht ersichtlich, ob ein PM-Kontoinhaber suspendiert wurde. Die ausführlichen Informationen in den TARGET2-Stammdaten, die über das ICM angezeigt werden können, enthalten jedoch einen entsprechenden Vermerk.

- Handelt es sich bei dem PM-Kontoinhaber, dessen Teilnahme beendet oder suspendiert wurde, um den Leiter einer Kontengruppe, kann dieser ab dem Zeitpunkt, an dem die Beendigung oder Suspendierung wirksam wird, nicht mehr in dieser Funktion auftreten. Ist der suspendierte PM-Kontoinhaber der **Co-Manager** für HAM-Konten, kann er nach der Suspendierung nicht mehr in dieser Funktion agieren. Es obliegt den betroffenen HAM-Kontoinhabern, einen neuen Co-Manager zu benennen. Standardmäßig kann die Zentralbank diese Aufgabe übernehmen.

- Ist der PM-Kontoinhaber, dessen Teilnahme beendet oder der suspendiert wurde, ein AS-Verrechnungsinstitut, wird er gemäß den für PM-Kontoinhaber geltenden Regeln behandelt. Die Zentralbank des Verrechnungsinstituts muss die Transaktionen bestätigen.

- Ein vom Zahlungsmodul ausgeschlossenes oder suspendiertes Nebensystem (AS) wird gemäß den für PM-Kontoinhaber geltenden Regeln behandelt. Die Zentralbank des Nebensystems muss die Transaktionen bestätigen.

- Sind ein oder mehrere TIPS-Geldkonten über einen LM-Link mit dem PM-Kontoinhaber, dessen Teilnahme beendet oder der suspendiert wurde, verknüpft, und werden die TIPS-Geldkonten nicht von derselben juristischen Person wie das PM-Konto unterhalten, müssen die TIPS-Geldkonten spätestens am Tag der Suspendierung/Beendigung der Teilnahme mit einem anderen PM-Konto verknüpft werden, das vom TIPS-Geldkontoinhaber zu benennen ist.

- Sind ein oder mehrere T2S-Geldkonten mit dem PM-Kontoinhaber, dessen Teilnahme beendet oder der suspendiert wurde, verbunden (PM-Hauptkonto), und werden die T2S-Geldkonten nicht von derselben juristischen Person wie das PM-Konto unterhalten oder gibt es keinen Grund, die verbundenen T2S-Kontoinhaber zu suspendieren/ihre Teilnahme zu beenden, müssen die T2S-Geldkonten am Tag der Suspendierung/Beendigung der Teilnahme des PM-Hauptkontos spätestens vor dem automatisierten „Cash Sweep“ um 17.45 Uhr mit einem anderen PM-Konto verbunden werden, das vom T2S-Geldkontoinhaber zu benennen ist.

3.8.2 Auswirkungen der Suspendierung eines TIPS-Geldkontoinhabers

Liegen die Gründe für die Suspendierung eines TIPS-Geldkontoinhabers vom TARGET2-Komponentensystem einer Zentralbank außerhalb des Geltungsbereichs von Artikel 26 Absatz 1 Buchstabe a Anhang IIb der TARGET2-Leitlinie, muss die Zentralbank des suspendierten TIPS-

Geldkontoinhabers entweder:

a) alle eingehenden Zahlungsaufträge zurückweisen,

b) alle ausgehenden Zahlungsaufträge zurückweisen, oder

c) sowohl eingehende als auch ausgehende Zahlungsaufträge zurückweisen.

Liegen die Gründe für die Suspendierung innerhalb des Geltungsbereichs von Artikel 26 Absatz 1 Buchstabe a Anhang IIb der TARGET2-Leitlinie, muss die Zentralbank des suspendierten TIPS-Geldkontoinhabers alle eingehenden und ausgehenden Zahlungsaufträge zurückweisen.

Die zuständige Zentralbank muss Aufträge für Instant-Zahlungen eines TIPS-Geldkontoinhabers, der gemäß Artikel 26 Absatz 1 oder 2 Anhang IIb der TARGET2-Leitlinie von der Teilnahme am betreffenden TARGET2-Komponentensystem suspendiert oder dessen Teilnahme daran beendet wurde und für den die Zentralbank gemäß Artikel 18 Absatz 3 Buchstabe b vor der Suspendierung oder Beendigung der Teilnahme Beträge auf einem TIPS-Geldkonto reserviert hat, verarbeiten.

3.8.3 Auswirkungen der Suspendierung eines in TIPS aktiven Nebensystems

Wird ein TIPS-Nebensystem vom TARGET2-Komponentensystem einer Zentralbank suspendiert und liegen die Gründe dafür außerhalb des Geltungsbereichs von Artikel 26 Absatz 1 Buchstabe a Anhang IIb der TARGET2-Leitlinie, dann muss die Zentralbank des suspendierten TIPS-Nebensystems entweder:

a) alle eingehenden Zahlungsaufträge zurückweisen,

b) alle ausgehenden Zahlungsaufträge zurückweisen oder

c) sowohl eingehende als auch ausgehende Zahlungsaufträge zurückweisen.

Liegen die Gründe für die Suspendierung innerhalb des Geltungsbereichs von Artikel 26 Absatz 1 Buchstabe a Anhang IIb der TARGET2-Leitlinie, muss die Zentralbank des suspendierten TIPS-Nebensystems alle eingehenden und ausgehenden Zahlungsaufträge zurückweisen.

Aufträge für Instant-Zahlungen eines TIPS-Nebensystems, das von der Teilnahme am betreffenden TARGET2-Komponentensystem suspendiert oder dessen Teilnahme daran beendet wurde und für das die Zentralbank gemäß Artikel 8 Absatz 3 Buchstabe b vor der Suspendierung oder Beendigung der Teilnahme Beträge auf einem TIPS ASTA reserviert hat, müssen von der zuständigen Zentralbank bearbeitet werden.

3.8.4 Auswirkungen der Suspendierung eines T2S-Geldkontoinhabers

- Das Limit für die Zentralbank-Selbstbesicherung wird auf null gesetzt. Jegliche zuvor gewährte Zentralbank-Selbstbesicherung ist zurückzuzahlen.

- Für das T2S-Geldkonto wird eine Innertages-Beschränkung festgelegt, damit keine Verrechnung stattfindet.
- Das PM-Hauptkonto ist nun das PM-Konto der Zentralbank, es sei denn, das PM-Hauptkonto wird von der juristischen Person unterhalten, die auch das T2S-Geldkonto unterhält, und wurde ebenfalls suspendiert.
- Die zur Veranlassung von Liquiditätsübertragungen in T2S gewährten Berechtigungen werden widerrufen.
- Vorab festgelegte Aufträge und Daueraufträge für Liquiditätsübertragungen werden gelöscht.
- Die am Tag der Suspendierung auf dem T2S-Geldkonto verbleibende Liquidität wird durch den automatisierten „Cash Sweep“ auf das PM-Hauptkonto übertragen.

3.8.5 Auswirkungen der Suspendierung eines HAM-Teilnehmers

- Die Suspendierung wird sofort wirksam.
- Zahlungen können nicht mehr automatisch über die HAM-Konten des Teilnehmers abgewickelt werden.
- Von einem suspendierten Teilnehmer gesendete Zahlungen werden zur Bestätigung durch die Zentralbank „geparkt“.
- An einen suspendierten Teilnehmer gesendete Zahlungen werden zur Bestätigung durch die Zentralbank „geparkt“.
- Hinsichtlich der Co-Management-Funktion[64] gilt Folgendes: Ist der suspendierte PM-Teilnehmer ein Co-Manager für HAM-Konten, kann er nicht mehr in dieser Funktion agieren, nachdem die Suspendierung wirksam geworden ist. Es obliegt den betroffenen HAM-Kontoinhabern, einen neuen Co-Manager zu benennen. In der Zwischenzeit kann die jeweilige Zentralbank auf Wunsch diese Aufgabe übernehmen. Wird ein HAM-Teilnehmer ausgeschlossen, dessen Konto von einem Co-Manager mit verwaltet wird, so bleibt die Beziehung zwischen dem betreffenden HAM-Kontoinhaber und dem Co-Manager bestehen. Dem HAM-Konto dieses Teilnehmers zu belastende oder gutzuschreibende Transaktionen sind von der Zentralbank auszuführen.

64 Ein HAM-Konto kann von einem PM-Kontoinhaber mit SWIFT-basiertem Zugang als Co-Manager mit verwaltet werden. Co-Management soll kleinen Banken ermöglichen, ihre Bestände zur Erfüllung der Mindestreservepflicht direkt zu steuern, das Cashflow-Management jedoch an andere Banken zu delegieren.

3.8.6 Behandlung von Teilnehmern, die sich in Abwicklung befinden

Gemäß dem vom Finanzstabilitätsrat (FSB) am 6. Juli 2017 veröffentlichten Leitfaden über die Kontinuität des Zugangs von in Abwicklung befindlichen Unternehmen zu Finanzmarktinfrastrukturen (FMIs)(„Guidance on Continuity of Access to Financial Market Infrastructures (FMIs) for a Firm in Resolution“, im Folgenden „FSB-Leitfaden“) *„sollten Anbieter kritischer FMI-Dienste geeignete Schritte einleiten, um das Zusammenspiel zwischen den Abwicklungsregimes der Nutzer ihrer FMI-Dienste und ihrem eigenen Risikomanagementrahmenwerk zu überdenken und zu planen. Dabei sollte geklärt werden, welche Maßnahmen sie in einem Abwicklungsszenario ergreifen könnten, um Unternehmen und Behörden bei der Verbesserung der Bereitschaft im Abwicklungsfall zu unterstützen“.*

Im Einklang mit dem FSB-Leitfaden ist in der TARGET2-Leitlinie festgelegt, dass das Ergreifen von Krisenpräventionsmaßnahmen oder Krisenmanagementmaßnahmen im Sinne der Richtlinie 2014/59/EU (BRRD) gegen den Inhaber eines PM-Kontos/T2S-Geldkontos/TIPS-Geldkontos nicht automatisch mit der Eröffnung eines Insolvenzverfahrens gemäß Richtlinie 98/26/EG (Finalitätsrichtlinie) oder der TARGET2-Leitlinie gleichzusetzen ist. Das bedeutet, dass ein in Abwicklung befindliches Unternehmen nicht automatisch suspendiert oder seine Teilnahme an TARGET2 beendet würde. Der Betreiber von TARGET2 behält sich allerdings das Recht vor, nach eigenem Ermessen und nach Prüfung der besonderen Umstände des jeweiligen Einzelfalls einen Kontoinhaber gemäß Artikel 34 Absatz 2 der TARGET2-Leitlinie zu suspendieren oder seine Teilnahme zu beenden. Dieses Vorgehen steht im Einklang mit dem FSB-Leitfaden, der vorsieht, dass FMIs ihr Risiko selbst steuern und ihre Teilnehmer vor einem Ansteckungsrisiko schützen müssen. Es entspricht auch Prinzip 18 der PFMIs des Ausschusses für Zahlungsverkehr und Marktinfrastrukturen (CPMI) und der Internationalen Organisation der Wertpapieraufsichtsbehörden (IOSCO).

Die TARGET2-Leitlinie schafft nicht automatisch verbindliche Rechte, Pflichten oder Verfahren in Bezug auf einen Teilnehmer, bei dem eine Abwicklung ansteht. Teilnehmer sind jedoch verpflichtet, ihre zuständige Zentralbank umgehend zu informieren, wenn sie Gegenstand von Krisenpräventionsmaßnahmen oder Krisenmanagementmaßnahmen im Sinne der BRRD werden. Es obliegt den einzelnen Zentralbanken, ihre Teilnehmer über etwaige Handlungsanleitungen (sofern sie sich auf FMI-Teilnehmer erstrecken) sowie sonstige Verfahren und Informationsanforderungen, die sie für Abwicklungsereignisse festgelegt haben, in Kenntnis zu setzen. Überdies wurde die TARGET2-Leitlinie geändert, um sie mit dem FSB-Leitfaden in Einklang zu bringen. Die Zentralbanken dürfen nun neben den Aufsichts- und Überwachungsbehörden auch Abwicklungsbehörden von Mitgliedstaaten und der Union (einschließlich anderen Zentralbanken) Zahlungs-, technische oder organisatorische Informationen eines Teilnehmers in dem Umfang offenlegen, der für die Durchführung ihrer öffentlichen Aufgaben notwendig ist, und stets unter der Voraussetzung, dass die Offenlegung nicht anwendbarem Recht zuwiderläuft.

3.9 Beschränkung oder vorläufiger oder endgültiger Ausschluss des Zugangs zu Innertageskrediten und/oder Selbstbesicherungsfazilitäten

Eine Zentralbank schließt eine Stelle vorläufig oder endgültig von Innertageskrediten/Selbstbesicherungsfazilitäten aus, wenn eines der folgenden Ausfallereignisse eintritt:

a) das T2S-Geldkonto und/oder PM-Konto der Stelle wird vorläufig oder endgültig geschlossen,

b) die betreffende Stelle erfüllt eine der in Anhang III der Harmonisierten Bedingungen für die Eröffnung und Führung eines PM-Kontos und in den Harmonisierten Bedingungen für die Eröffnung und Führung eines T2S-Geldkontos jeweils festgelegten Anforderungen nicht mehr,

c) eine zuständige Justiz- oder sonstige Behörde hat die Entscheidung getroffen, ein Verfahren zur Abwicklung der Stelle durchzuführen, einen Insolvenzverwalter oder einen entsprechenden Verantwortlichen für die Stelle einzusetzen oder ein anderes entsprechendes Verfahren einzuleiten,

d) die Gelder der Stelle werden gesperrt und/oder ihr werden andere Maßnahmen von der Europäischen Union auferlegt, die ihre Fähigkeiten beschränken, über ihre Gelder zu verfügen,

e) die Zulassung der Stelle als Geschäftspartner für geldpolitische Geschäfte des Eurosystems wird vorläufig oder endgültig beendet.

Eine Zentralbank kann einen vorläufigen oder endgültigen Ausschluss vom Zugang zu Innertageskrediten und/oder Selbstbesicherungsfazilitäten vornehmen, wenn sie oder eine andere Zentralbank den T2S-Geldkontoinhaber von TARGET2 suspendiert oder dessen Teilnahme beendet oder ein oder mehrere Ausfallereignisse eintreten.

Beschließt das Eurosystem, den Zugang der Geschäftspartner zu geldpolitischen Instrumenten aufgrund von Risikoerwägungen oder aus sonstigen Gründen gemäß Anhang I, Kapitel 2.4 der Leitlinie EZB/2011/14 vorläufig oder endgültig auszuschließen oder zu beschränken, setzt die Zentralbank diesen Beschluss im Hinblick auf den Zugang zu Innertageskrediten und/oder Selbstbesicherungsfazilitäten gemäß den Bestimmungen der von ihr angewandten vertraglichen Regelungen oder Rechtsvorschriften um.

Die Zentralbank kann beschließen, den Zugang zu Innertageskrediten und/oder Selbstbesicherungsfazilitäten vorläufig oder endgültig auszuschließen oder zu begrenzen, wenn der PM-Kontoinhaber/T2S-Geldkontoinhaber unter Risikoerwägungen als Gefahr angesehen wird. In solchen Fällen setzt die Zentralbank die EZB und andere Zentralbanken hiervon unverzüglich schriftlich in Kenntnis. Ein solcher Beschluss wird erst mit Zustimmung der EZB wirksam. Sofern es angemessen

erscheint, kann der EZB-Rat eine einheitliche Umsetzung der in allen TARGET2-Komponentensystemen ergriffenen Maßnahmen beschließen.

In dringenden Fällen kann eine Zentralbank den Zugang zu Innertageskrediten und/oder Selbstbesicherungsfazilitäten jedoch mit sofortiger Wirkung vorläufig ausschließen. In solchen Fällen hat die Zentralbank dies der EZB umgehend schriftlich mitzuteilen. Die EZB ist befugt, die Maßnahme der Zentralbank aufzuheben. Wenn die EZB der Zentralbank nicht innerhalb von zehn Geschäftstagen ab dem Zeitpunkt des Zugangs der Mitteilung bei der EZB eine Benachrichtigung über die Aufhebung der Maßnahme übermittelt, gilt dies als Zustimmung der EZB zu der betreffenden Maßnahme.

Bei Begrenzung von Innertageskrediten ist die Innertageskreditlinie an die Höhe des festgelegten Limits anzupassen. **Bei Innertageskrediten** ist die Innertageskreditlinie auf null zu setzen.

Bei Begrenzung von Selbstbesicherungsfazilitäten ist das Limit für die Zentralbank-Selbstbesicherungsfazilitäten an die Höhe des festgelegten Limits anzupassen. **Bei vorläufiger oder endgültiger Kündigung der Selbstbesicherungsfazilitäten** ist das Limit für die Zentralbank-Selbstbesicherung auf null zu setzen.

3.10 Rechnungsstellung in TARGET2

Die monatliche Rechnung für die in Anspruch genommenen TARGET2-Dienstleistungen wird von der betreffenden Zentralbank zu Beginn des Folgemonats (bis spätestens zum neunten TARGET2-Geschäftstag) an die PM-Kontoinhaber und Nebensysteme geschickt und ist spätestens am 14. TARGET2-Geschäftstag dieses Monats fällig.

Ferner werden allen PM-Kontoinhabern, deren PM-Konto (PM-Hauptkonto) mit einem oder mehreren T2S-Geldkonten verknüpft ist oder die als T2S-Partei definiert wurden, gemäß den Preisvorgaben für T2S auch die Kosten für geldbezogene T2S-Dienstleistungen in Rechnung gestellt.

Nähere Informationen finden sich im Dokument TARGET2 Pricing Guide for Users.

3.11 Rechnungsstellung für TIPS

Von Januar 2022 (für den Zeitraum Dezember 2021) bis zur Außerbetriebnahme von TARGET2 im November 2022 gilt – auch infolge der Migration der TIPS-Fakturierung zur „T2/TS2 Consolidation Common Billing“-Komponente (BILL) – eine Übergangslösung für die Rechnungsstellung für TIPS. TIPS-Geldkontoinhaber und in TIPS aktive Nebensysteme erhalten die monatliche Rechnung für TIPS-Leistungen zu Beginn des nächsten Monats (bis spätestens zum vierten TARGET2-Geschäftstag). Die Rechnung muss bis spätestens zum elften TARGET2-Geschäftstags dieses Monats beglichen werden.

Teilnahme

Bei allen Inhabern von TIPS-Geldkonten und von TIPS ASTAs erfolgt die Rechnungsstellung gemäß dem TIPS-Gebührenmodell.

Weitere Informationen finden sich im TARGET Services pricing guide.

4 Der Geschäftstag im Normalbetrieb

TARGET2-Nutzer sind für die Überwachung ihrer täglichen Operationen auf der Gemeinschaftsplattform und/oder der TIPS-Plattform und/oder der T2S-Plattform verantwortlich. Parallel dazu kümmern sich die jeweiligen National Service Desks auch um die allgemeine Überwachung des Betriebs im Tagesablauf und um die entsprechenden Bedürfnisse im Bankensektor.

Geeignet für die Durchführung dieser Überwachungsaufgaben sind, was die Dienste auf der Gemeinschaftsplattform (einschließlich TARGET2-Zusatzleistungen) betrifft, das ICM (Informations- und Steuerungsmodul), was die TIPS-Plattform betrifft, die TIPS GUI, wenn es um die Dienste auf der T2S-Plattform geht, die T2S GUI, und in Bezug auf die Referenzdaten die CRDM GUI.

Im Folgenden werden die Abläufe eines normalen Geschäftstags nach Phasen untergliedert beschrieben. Dabei gilt es zu beachten, dass der Geschäftstag bereits am Abend des vorherigen Werktags beginnt.

4.1 Täglicher Betrieb in TARGET2

4.1.1 Beginn des Geschäftstags

In TARGET2 (SSP) beginnt der neue Geschäftstag nach erfolgreichem Abschluss der Tagesendarbeiten des vorangegangenen Tages sowie der Vorbereitungsarbeiten für den laufenden Tag (wobei die erste Tätigkeit darin besteht, die Änderungen der Nutzerstammdaten zu laden). Der Wechsel zum neuen Geschäftstag wird in der Regel zwischen 18.45 Uhr und 19.00 Uhr durch eine Nachricht an alle Nutzer bestätigt. Angezeigt werden die Phasen auch auf dem ICM-Bildschirm „SSP Operating Day“ unter „Services“ – „Administration“.

Die ICM-Nachricht lautet wie folgt: „*Die Tagesendarbeiten für TT-MM-JJ sind abgeschlossen. Der Geschäftstag TT-MM-JJ ist nun eröffnet.*“

Das Verfahren zum **T2S-Tagesbeginn** wird ebenfalls um 18.45 Uhr gestartet und dauert bis 20.00 Uhr. Die Bestätigung erfolgt durch eine Statusmeldung zum T2S-Abwicklungstag („Status of the T2S Settlement Day Notification“) auf dem GUI-Bildschirm „Daily Schedule“ und/oder über „T2S Diary Query“. Die Geschäftsanfangsphase beinhaltet die Änderung des Abwicklungsdatums, die Annahme der Datenfeeds von T2S-Geldkontoinhabern für die Client Auto-Collateralisation (die bis 19.00 Uhr empfangen werden und für das laufende Abwicklungsdatum gültig sind), die Bewertung der Sicherheiten für die Client Collateralisation on Stock und die Bewertung der besicherungsfähigen Abwicklungsinstruktionen.

In dieser Phase erfolgt keine Geldverrechnung; sie sollte von den Teilnehmern dazu genutzt werden, die

Nachtverarbeitung vorzubereiten.

Kasten 2: Datenfeeds für die Client Auto-Collateralisation

Jeder T2S-Geldkontoinhaber, der Client Auto-Collateralisation in T2S anbietet, ist für die Einrichtung und Pflege dieser Selbstbesicherungsfunktion in T2S einschließlich der Konfiguration der erforderlichen Stammdaten verantwortlich. So sollten die folgenden Informationen (Datenfeeds) an T2S übermittelt werden:

- Liste der besicherungsfähigen Wertpapiere für die Selbstbesicherung (nach dem ersten Hochladen sollte sie, wann immer Änderungen vorliegen, aktualisiert werden)

- die täglichen Bewertungen der besicherungsfähigen Wertpapiere

Datenfeeds im Zusammenhang mit der Besicherung (besicherungsfähige Wertpapiere bzw. entsprechende Bewertungen), die für den um 18.45 Uhr beginnenden Abwicklungstag zu verwenden sind, sollten über den ganzen Tag hinweg und idealerweise bis spätestens 17.45 Uhr geliefert werden (wenngleich bis 19.00 Uhr eingehende Informationen noch angenommen werden). Die Bewertungen sollten in Form einer „Flat File“ übermittelt werden, während die Liste der notenbankfähigen Wertpapiere gemäß T2S-UDFS[65] per Nachricht bzw. Datei im Format ISO 20022 zu liefern ist.

Kommt es bei der Übermittlung der Bewertungen der besicherungsfähigen Wertpapiere zu Verzögerungen (z. B. wenn die Informationen nicht bis 19.00 Uhr vorliegen), werden die bisher verfügbaren Bewertungen genutzt. Liegen zu den am Vortag geltenden Bewertungen eines bestimmten besicherungsfähigen Wertpapiers keine Informationen vor, wird ein Wert von null angesetzt.

Es sei darauf hingewiesen, dass derzeit die T2S-Funktion „Close Links“ vom Eurosystem nicht genutzt wird und es daher nicht nötig ist, Informationen zur Liste der „Close Links“ zu liefern.

4.1.2 Liquiditätsbereitstellung

Von 19.00 Uhr bis 19.30 Uhr wird im Bedarfsfall Liquidität für den Zahlungsausgleich während des Tages bzw. der Nacht bereitgestellt. Dabei kann es zu folgenden Liquiditätsbewegungen kommen:

- vom SF auf das PM oder HAM
- vom HAM oder dem PHA auf das PM.

65 Die Bereitstellung dieser Information erfordert eine direkte Verbindung zu T2S im A2A-Modus.

Diese 30 Minuten können auch für die Aktualisierung von Kreditlinien oder für die Abwicklung von Repogeschäften vor der Eröffnung genutzt werden.

4.1.3 Nachtverarbeitung auf der Gemeinschaftsplattform

Liquidität für die Nachtverarbeitung (Dedizierung auf Unter-/Spiegelkonten)

Um 19.30 Uhr erfolgen die Gutschriften auf die Unter- und Spiegelkonten, damit die Nachtverarbeitung der Nebensysteme beginnen kann.

Das Nachtfenster steht von 19.30 Uhr bis 7.00 Uhr zur Verfügung,[66] wobei die Zeit zwischen 22.00 Uhr und 1.00 Uhr als technisches Wartungsfenster für die Gemeinschaftsplattform vorgesehen ist. Auf diese Weise wird die Nachtverarbeitung der unterschiedlichen Nebensysteme in Zentralbankgeld erleichtert. Die in TARGET2 verfügbaren technischen und operationellen Tools ermöglichen eine reibungslose Durchführung der Nachtverarbeitung.

Der Support für an der Nachtverarbeitung teilnehmende Kreditinstitute oder Nebensysteme muss mit der jeweiligen Zentralbank vereinbart werden.

Während des Nachtverarbeitungsfensters können grundsätzlich Liquiditätsübertragungen mittels ICM zum und vom PM-Konto durchgeführt werden.

Liquiditätsbereitstellung für die Nachtverarbeitung („nicht konkordante Aufträge“)

In der folgenden Abbildung sind die Abläufe des Abwicklungsverfahrens 6[67] dargestellt.

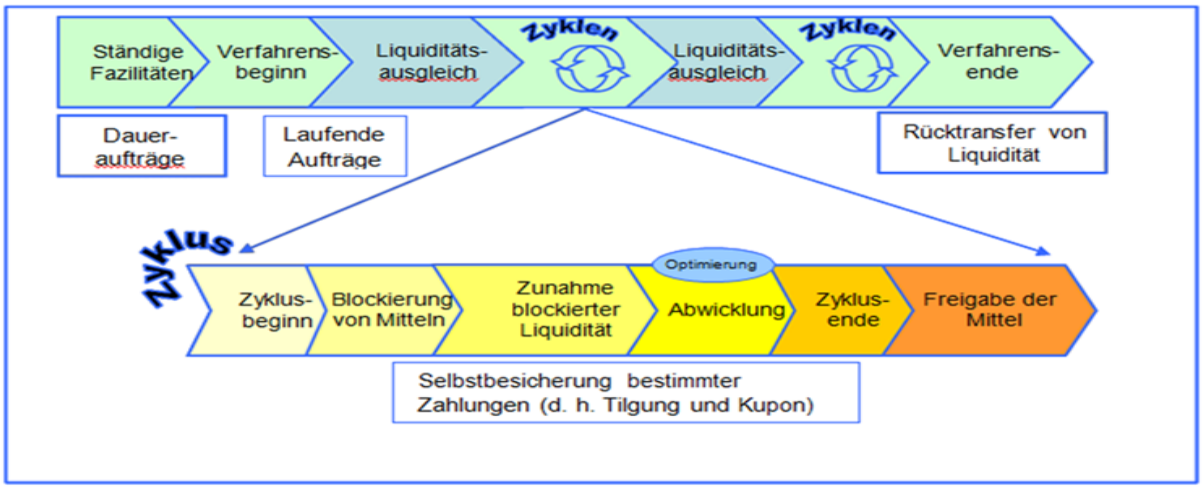


Abbildung 15: Abwicklungsverfahren 6

66 In der Zeit von 6.45 Uhr bis 7.00 Uhr (Beginn der Tagverarbeitung) wird die Öffnung des Tagesbetriebs vorbereitet.

67 Während der Nachtverarbeitung kann nur das Abwicklungsverfahren 6 verwendet werden. Das Abwicklungsverfahren 6 kann jedoch neben der Nacht- auch für die Tagverarbeitung genutzt werden.

In diesem Zusammenhang ist zwischen Daueraufträgen und laufenden Aufträgen des PM-Kontoinhabers/der Verrechnungsbank und des Nebensystems zu unterscheiden:

a) Dauerauftrag (nur der Verrechnungsbank)

Der gespeicherte Betrag ist durchgängig bis zur nächsten Änderung maßgebend. Für die Tag- und Nachtverarbeitung können unterschiedliche Aufträge definiert werden. Daueraufträge müssen von der Verrechnungsbank über das ICM bis spätestens 18.00 Uhr eingegeben werden (wirksam ab der nächsten Nachtverarbeitung).

Sie werden unmittelbar nach dem Versand der Nachricht „Beginn des Verfahrens“ („Start of procedure“) ausgeführt. Bei unzureichender Liquidität könnte es zu einer Teilausführung kommen. Der verbleibende Teil wird in diesem Fall nicht ausgeführt.

b) Laufender Auftrag der Verrechnungsbank

Nach Versand der Nachricht „Beginn des Verfahrens“ („Start of procedure“) – jedoch vor Versand der Nachricht „Ende des Verfahrens“ („End of procedure“) – stellt die Verrechnungsbank per ICM einen laufenden Auftrag ein. Geht er vor dem ersten Zyklus oder zwischen zwei Zyklen (während der Liquiditätsanpassungsphase) ein, wird er sofort ausgeführt. Geht der laufende Auftrag während eines Zyklus ein, wird er zunächst zwischengespeichert. Bei unzureichender Liquidität werden laufende Aufträge zurückgewiesen.

c) Laufender Auftrag des Nebensystems

Laufende Aufträge von Nebensystemen unterliegen internen Regelungen. Es bedarf einer Vorabvereinbarung zwischen dem Nebensystem und der Verrechnungsbank. Der Versand laufender Aufträge kann erfolgen, sobald die Nachricht „Beginn des Verfahrens“ verschickt wurde. Geht der laufende Auftrag vor dem ersten Zyklus oder zwischen zwei Zyklen (während der Liquiditätsanpassungsphase) ein, erfolgt eine sofortige Ausführung. Geht er während eines Zyklus ein, wird er zunächst zwischengespeichert. Bei unzureichender Liquidität kommt es zu einer Teilausführung. Der verbleibende Teil wird in diesem Fall nicht ausgeführt.

Konkordanz von Aufträgen

Daueraufträge und laufende Aufträge werden nicht parallel ausgeführt, da Daueraufträge bereits abgewickelt werden, bevor laufende Aufträge versandt werden können.

Unabhängig davon, ob die laufenden Aufträge von einer Verrechnungsbank oder einem Nebensystem erteilt sind, werden sie unmittelbar nach Eingang ausgeführt. Laufende Aufträge, die zunächst zwischengespeichert wurden, weil sie während eines Zyklus eingegangen sind, werden nach dem FIFO-

Prinzip („First In, First Out“), d. h. in der Reihenfolge ihres Eingangs, ausgeführt.

Bei der Nachtverarbeitung wird für alle teilnehmenden Nebensysteme automatisch eine gemeinsame Nachricht „Beginn des Verfahrens“ verschickt. Dies bedeutet, dass alle Daueraufträge, die eine zu verschiedenen Nebensystemen gehörende Verrechnungsbank erteilt hat, zeitgleich ausgeführt werden. Ist für die Summe der Daueraufträge nicht genügend Liquidität verfügbar, werden alle Daueraufträge anteilig gekürzt. Dies geschieht folgendermaßen:

Ermittlung eines Kürzungsfaktors: bestehende Liquidität / Summe der Daueraufträge

Kürzung der Daueraufträge: Dauerauftrag x Kürzungsfaktor

4.1.4 Geldrelevante Aspekte der T2S-Nachtverarbeitung

Während der T2S-Nachtverarbeitung durchlaufen die Liquiditätsübertragungen – gemäß einer automatischen vordefinierten Reihenfolge namens Sequenz („sequence“) – zwei Abwicklungszyklen. Ein Abwicklungszyklus besteht aus mehr als einer Sequenz.

Liquiditätsübertragungen von PM-Konten auf T2S-Geldkonten und zwischen T2S-Geldkonten werden ab Sequenz 0 (im ersten Nachtverarbeitungszyklus) verarbeitet, d. h., der erste Liquiditätseingang wird gleich zu Beginn der Nachtverarbeitung abgewickelt. Es sei darauf hingewiesen, dass Daueraufträge für Liquiditätsübertragungen von PM-Konten zu T2S-Geldkonten auf der Gemeinschaftsplattform um 19.30 Uhr und auf der T2S-Plattform um 20.00 Uhr mit dem Start der Sequenz 0 verarbeitet werden.

Liquiditätsübertragungen von T2S-Geldkonten auf PM-Konten werden ab Sequenz 1 (im ersten Nachtverarbeitungszyklus) abgewickelt. Liquiditätsübertragungen, die bei einer laufenden Sequenz eingehen, werden in folgenden Sequenzen berücksichtigt.

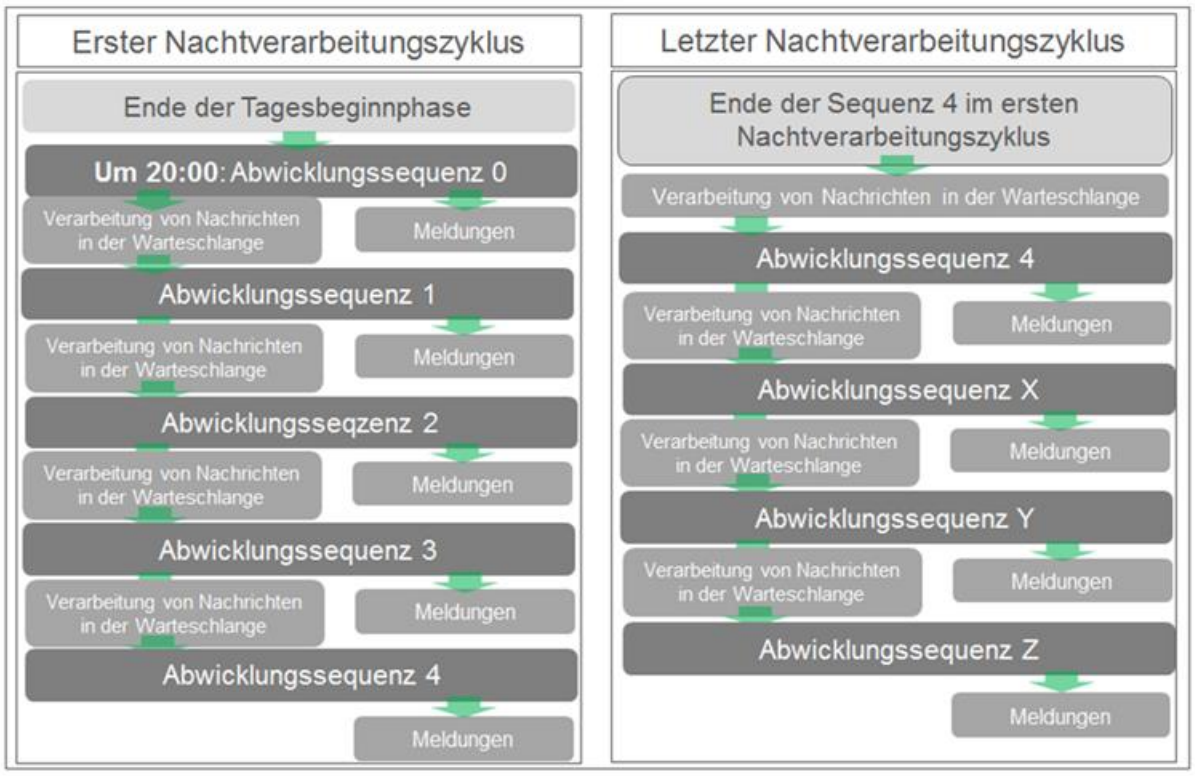


Abbildung 16: T2S-Nachtverarbeitungssequenzen

Am Ende jeder Sequenz generiert T2S vollständige oder Delta-Berichte gemäß Berichtskonfiguration der betreffenden direkt angeschlossenen T2S-Geldkontoinhaber. Indirekt angebundenen T2S-Geldkontoinhabern werden diese Berichte nicht angeboten.

Wird die Nachtverarbeitung vor 3.00 Uhr abgeschlossen, beginnt die Echtzeitabwicklung vor dem Start des Wartungsfensters (um 3.00 Uhr). Während das Wartungsfenster geöffnet ist, findet in T2S keine Abwicklung statt.

Funktion „Multiple Liquiditätsgeber“

In T2S ist es möglich, dass T2S-Geldkontoinhaber Liquidität von verschiedenen PM-Konten erhalten, d. h. von verschiedenen Liquiditätsgebern. Nutzt der T2S-Geldkontoinhaber die Funktion „Multiple Liquiditätsgeber“ („multiple liquidity provider“), können die Liquiditätsgeber die erforderlichen Liquiditätsübertragungen auf das T2S-Geldkonto veranlassen.

Am Ende der Nachtverarbeitung – in Sequenz Y des letzten Nachtverarbeitungszyklus – wird die restliche Liquidität auf dem T2S-Geldkonto automatisch auf die PM-Konten der Liquiditätsgeber – gemäß den Daueraufträgen für Liquiditätsübertragungen (zur Rückführung der verbleibenden Liquidität auf die PM-Konten) und dem vorab festgelegten Auftrag für die Ausführung dieser Daueraufträge

gemäß der Definition in den Stammdaten – zurückübertragen.

Die Funktion „Multiple Liquiditätsgeber“ ist optional und kann nur während der Nachtverarbeitung, in der Sequenz Y des letzten Nachtverarbeitungszyklus verwendet werden.

4.1.5 Betriebsfenster

Das Eurosystem nutzt dieses Fenster zur Vorbereitung des Tagesgeschäfts.

4.1.6 SSP-Tagverarbeitung

Um 7.00 Uhr wird TARGET2 für die Verarbeitung von Zahlungsaufträgen geöffnet, was auf dem jeweiligen ICM-Bildschirm angezeigt wird. Die Bestätigung über den störungsfreien Beginn des Tagesbetriebs erfolgt durch eine T2-IS-Nachricht.

Während des Tagesbetriebs sollten bestimmte Zahlungsströme aufgrund ihrer systemweiten Bedeutung besonders aufmerksam verfolgt werden. Es wird erwartet, dass die direkten Teilnehmer diese Zahlungen intern vorrangig behandeln.

- 7.00 Uhr – 12.00 Uhr: CLS-Zahlungen

Das CLS-System (Continuous Linked Settlement – CLS) ermöglicht die globale Abwicklung von Devisengeschäften in mehreren Währungen, wobei ein Zahlung-gegen-Zahlung-Mechanismus (Payment versus Payment – PvP) Anwendung findet. Zu diesem Zweck hat CLS in jeder zugelassenen Währung Zugang zu Zentralbankgeld. Für die Abwicklung in Euro unterhält CLS ein Konto bei der EZB und nutzt TARGET2, um Euro-Zahlungen zu empfangen und zu versenden. CLS erstellt täglich einen Einzahlungsplan, in dem die Beträge aufgeführt sind, die die Verrechnungsteilnehmer (Settlement Members) zu fünf Zeitpunkten in stündlichem Abstand (8.00 Uhr, 9.00 Uhr, 10.00 Uhr, 11.00 Uhr und 12.00 Uhr) an CLS transferieren müssen. Es steht den Verrechnungsteilnehmern frei, alle ihre Zahlungsverpflichtungen bereits vor diesen Zeitpunkten „in einem Mal“ zu erfüllen. Eine Verzögerung bei der Bereitstellung von Euro-Mitteln könnte zu Beeinträchtigungen der Mehrwährungsabwicklung von CLS und womöglich auch der Systeme anderer Währungsräume führen – insbesondere im asiatisch-pazifischen Raum, wenn dieser wegen des Zeitunterschieds kurz vor Geschäftsschluss steht.

- Zahlungen im Zusammenhang mit Margin Calls für zentrale Kontrahenten (Sicherheitenmargen und Nachschusszahlungen)

Den Beteiligten an Finanzkontrakten, die an einem oder mehreren Märkten gehandelt werden, ist ein zentraler Kontrahent (Central Counterparty – CCP) zwischengeschaltet, der für jeden Verkäufer als Käufer und für jeden Käufer als Verkäufer fungiert.

Ein zentraler Kontrahent kann das Risiko für die Marktteilnehmer insofern erheblich mindern, als er

allen Teilnehmern schärfere Risikokontrollmechanismen auferlegt und oftmals auch ein multilaterales Netting der Geschäfte gewährleistet. Ferner erhöht er meist die Liquidität an den von ihm bedienten Märkten, da er für gewöhnlich die Risiken für die Teilnehmer mindert und vielfach den anonymen Handel erleichtert.

Margin Calls für zentrale Kontrahenten erfolgen, indem das Clearinghaus von einem Mitglied zusätzliche Mittel oder Sicherheiten für den Ausgleich von Verlustpositionen auf einem Margenkonto einfordert. Sollten keine Sicherheitenmargen eingehen, verschiebt das Clearinghaus in der Regel den Handelsbeginn am betroffenen Markt. Bleibt die Leistung von Margenzahlungen aus, reichen die möglichen Konsequenzen von der Schließung der Positionen des säumigen Mitglieds bis hin zu dessen Ausschluss.

- 16.08 Uhr – 16.45 Uhr: EURO1-Zahlungsausgleich

EURO1 ist ein Großbetragszahlungssystem für grenzüberschreitende und inländische auf Euro lautende Transaktionen zwischen Banken, die in der EU operieren. Die Verrechnung erfolgt bei Tagesabschluss über die Nebensystemschnittstelle (ASI) mittels Abwicklungsverfahren 4. Gegen 16.08 Uhr wird die Datei zur Durchführung des Zahlungsausgleichs an die ASI gesendet. Der Verrechnungszeitraum endet um 16.45 Uhr. Falls eine Bank ihre Verpflichtungen im Rahmen des EURO1-Zahlungsausgleichs am Tagesende aufgrund von Liquiditätsproblemen nicht erfüllt, wird ein Garantiekonto-Verfahren eingeleitet.

- Abwicklung von Nebensystemen

Die gegenseitigen Abhängigkeiten zwischen TARGET2 und der Abwicklung von Nebensystemen, die nicht unter die vorgenannten Nebensysteme fallen, sowie deren Bedeutungsgrad sind von Land zu Land unterschiedlich und unterliegen der nationalen Zuständigkeit. Daher wird die Frage, in welchem Umfang die Abwicklung von Nebensystemen zu überwachen ist, von den nationalen Zentralbanken selbst geregelt.

- Probleme bei der Verarbeitung

Treten bei der Verarbeitung der oben genannten Geschäftskategorien Schwierigkeiten auf, sollten umgehend Problemlösungsverfahren aktiviert werden. Hier sollten die betroffenen TARGET2-Nutzer zusammen mit den National Service Desks proaktiv handeln.

- 17.00 Uhr: Annahmeschluss für Kundenzahlungen

Um 17.00 Uhr ist Annahmeschluss für Kundenzahlungen. Da Kontobelastungen und -gutschriften zeitgleich erfolgen, gilt Punkt 17.00 Uhr als Annahmeschluss; dies bedeutet, dass Zahlungsaufträge unmittelbar ab diesem Zeitpunkt zurückgewiesen werden. Die Zurückweisung erfolgt nach Ablauf von Algorithmus 3. Der Zeitstempel der Gemeinschaftsplattform ist verbindlich; konkret entscheidet die

Uhrzeit, zu der das Modul die Nachricht empfängt. Zentralbanken mit einem PHA-Konto sollten die Konformität mit diesem Annahmeschluss sicherstellen, indem sie beispielsweise frühere Annahmeschlusszeiten ansetzen.

- 18.00 Uhr: Annahmeschluss für Interbankzahlungen

Um 18.00 Uhr ist Annahmeschluss für Interbankzahlungen, aber auch das Ende der Frist für die Zahlungsverarbeitung. Da Kontobelastungen und -gutschriften zeitgleich erfolgen, gilt Punkt 18.00 Uhr als Annahmeschluss; dies bedeutet, dass eingehende Aufträge für Interbankzahlungen unmittelbar nach diesem Zeitpunkt zurückgewiesen werden. Die Zurückweisung erfolgt nach Ablauf von Algorithmus 3. Der Zeitstempel der Gemeinschaftsplattform ist verbindlich; konkret entscheidet die Uhrzeit, zu der das Modul die Nachricht empfängt. Zentralbanken mit PHA-Konten sollten die Erfüllung dieser Ausschlussfrist sicherstellen, indem sie beispielsweise frühere Annahmeschlusszeiten ansetzen.

4.1.7 Geldrelevante Aspekte der T2S-Echtzeitabwicklung

Der Start der T2S-Echtzeitabwicklung (RTS) könnte über eine „Status of the T2S Settlement Day Notification“, einen Eintrag im T2S-GUI-Bildschirm „Daily Schedule“ oder eine Nachricht zur Suchanfrage in Verbindung mit „T2S Diary Response“ überprüft werden.

Die RTS umfasst:

a) Die **Vorbereitung der Echtzeitverarbeitung**,

b) Fünf **Teilabwicklungsfenster** von je 15 Minuten, die um 8.00 Uhr, 10.00 Uhr, 12.00 Uhr, 14.00 Uhr und 15.45 Uhr (15 Minuten vor Beginn des DVP-Annahmeschlusses) geöffnet werden. Im Fenster für die Teilabwicklung verarbeitet T2S partiell neue Abwicklungsinstruktionen, die in T2S eingehen und für eine Teilabwicklung in Frage kommen, sowie bislang unverarbeitete oder nur zum Teil verarbeitete Abwicklungsinstruktionen, die für eine partielle Abwicklung infrage kommen.

c) Schließung der Echtzeitverarbeitung (Real-Time Settlement Closure). Die Schließung der Echtzeitverarbeitungsphase beginnt planmäßig um 16.00 Uhr und umfasst folgende, für die Geldverrechnung äußerst relevante Verfahren:

Zeit	Ereignisse/Verfahren während des T2S-Euro-Abwicklungstags
16.00 Uhr	DVP-Annahmeschluss (nach diesem Annahmeschluss können keine neuen Selbstbesicherungsinstruktionen veranlasst werden)
	Annahmeschluss für Geldverrechnungsrestriktionen („Cash settlement restriction“)
	Freigabe nicht genutzter „Cash settlement restriction“
16.30 Uhr	Automatische Erstattung der Zentralbank-Selbstbesicherung
(danach)	Optionaler automatisierter „Cash Sweep“ (falls über Daueraufträge zu Liquiditätsübertragungen konfiguriert)
17.40 Uhr	Annahmeschluss für Abwicklungsinstruktionen für bilaterale besicherte Geldhandelsgeschäfte (Bilaterally Agreed Treasury Management – BATM) und Zentralbankgeschäfte
17.45 Uhr	Annahmeschluss für Liquiditätsübertragungen von PM-Konten auf T2S-Geldkonten
(danach)	Automatisierter „Cash Sweep“ zur Übertragung der verbleibenden Liquidität von den T2S-Geldkonten auf das entsprechende PM-Hauptkonto **ANMERKUNG**: T2S-Geldkontoinhabern wird empfohlen, die Liquidität von den T2S-Geldkonten auf die PM-Konten frühzeitiger, z. B. vor dem automatisierten „Cash Sweep“, zu transferieren, um bei Problemen mit diesem Prozess die Liquiditätsrisiken zu begrenzen.
18.00 Uhr	Annahmeschluss für Wertpapierabwicklungsrestriktion sowie Free-of-Payment-Annahmeschluss

Tabelle 8: Abschluss der T2S-Echtzeitabwicklung

Direkt angebundene T2S-Geldkontoinhaber können die erwähnten Annahmeschlüsse über den T2S-GUI-Bildschirm „Daily Schedule“ und/oder über „T2S Diary Response“ Nachrichten zur Suchanfrage überprüfen.

Kasten 3: Automatisierte Rückführung der Zentralbank-Selbstbesicherung

Während der Nachtverarbeitung und auch im Tagbetrieb können T2S-Geldkontoinhaber von der Zentralbank-Selbstbesicherung profitieren. Allerdings sind Übernachtkredite auf der T2S-Plattform nicht zulässig, und die T2S-Geldkontoinhaber müssen die Zentralbank-Selbstbesicherung daher vor 16.30 Uhr zurückzahlen. Dies sollte über die Freigabe (als CSD-Teilnehmer oder als T2S-Geldkontoinhaber, sofern dieser die Objekt-Berechtigung für das/die entsprechende/n Wertpapierkonto/Wertpapierkonten hat) der betreffenden Rückführungsinstruktionen geschehen. Erfolgt dies nicht bis 16.30 Uhr, wird die automatische Rückführung durch die T2S-Plattform ausgelöst. Die T2S-Geldkontoinhaber sollten daher die Zentralbank-Selbstbesicherung entweder bis 16.30 Uhr selbst zurückführen oder genügend Liquidität auf dem T2S-Geldkonto bereitstellen, um die Rückführung der Selbstbesicherung über das automatische „Auto-Collateralisation Reimbursement“ (um 16.30 Uhr) zu ermöglichen.

Dieses Verfahren umfasst die folgenden Schritte, die von der T2S-Plattform automatisch ausgelöst werden:

a) Freigabe der Instruktionen zur Rückführung der Selbstbesicherung, die zunächst auf „on hold“ gesetzt worden waren

b) Versuch der Abwicklung der noch ausstehenden Rückführungstransaktionen – in Abhängigkeit von der auf dem T2S-Geldkonto vorhandenen Liquidität

c) Versuch, die (restlichen) noch ausstehenden Rückführungstransaktionen abzuwickeln – in Abhängigkeit von der auf anderen bei derselben Zentralbank geführten T2S-Geldkonten desselben (über BIC11 identifizierten) T2S-Geldkontoinhabers (z. B. Rebalancing) vorhandenen Liquidität

d) Umbuchung der Sicherheiten (Collateral relocation) – ein Schritt, über den eine neue Wertpapiertransaktion initiiert wird, um die vom T2S-Geldkontoinhaber als Sicherheiten hinterlegten Wertpapiere auf das reguläre Sicherheitenkonto bei der entsprechenden Zentralbank zu transferieren. Nach Erhalt der Information bezüglich dieses Sicherheitentransfers wird die Zentralbank die Zentralbank-Selbstbesicherung in einen Innertageskredit verwandeln, und zwar auf dem PM-Konto, das vom T2S-Geldkontoinhaber als Konto für die automatisierte Rückerstattung der Zentralbank-Selbstbesicherung angegeben wird. Dies erfolgt in der Regel über eine verknüpfte Zahlung (connected payment), über die die Zentralbank die Kreditlinie der Gegenpartei erhöht und gleichzeitig das entsprechende Konto belastet.

Eine Strafgebühr von 1 000 € wird fällig für jeden Geschäftstag, an dem ein oder mehrere Inanspruchnahmen im Zusammenhang mit der Umbuchung der Sicherheiten erfolgen. Im Einklang mit den von der jeweiligen Zentralbank festgelegten nationalen Verfahren wird diese Strafgebühr dem PM-Kontoinhaber für das Konto in Rechnung gestellt, das als Konto für die automatisierte Rückerstattung

der Zentralbank-Selbstbesicherung angegeben ist.

Anmerkung: Die in dem entsprechenden PM-Konto registrierte Kreditlinie besteht unabhängig von der Zentralbank-Selbstbesicherung, die im Laufe des Tages an das T2S-Geldkonto auf der T2S-Plattform gewährt wurde. Die Kreditlinie wird ihrer Höhe nach durch einen Pool von Sicherheiten unterlegt. Die während des Tages gewährte Zentralbank-Selbstbesicherung wird mit Wertpapieren unterlegt, die zuvor nicht zum Pool gehörten. Erst wenn es der Geschäftspartner versäumt, die Selbstbesicherung bis 16.30 Uhr zurückzuführen, wird die Sicherheit in den regulären Pool umgeschichtet, was zur Ausweitung der Kreditlinie im PM-Konto führt. Um sicherzustellen, dass die höhere Kreditlinie für die Rückerstattung der Zentralbank-Selbstbesicherung verwendet wird, wird die Liquidität aus der Erhöhung der Kreditlinie unmittelbar von dem PM-Konto des Teilnehmers auf das PM-Konto der Zentralbank transferiert. Dies wird in der Regel durch die Nutzung einer verknüpften Zahlung (connected payment) sichergestellt (in bestimmten Situationen können Zentralbanken von diesem Verfahren abweichen, wenn z. B. eine feste Kreditlinie verwendet wird).

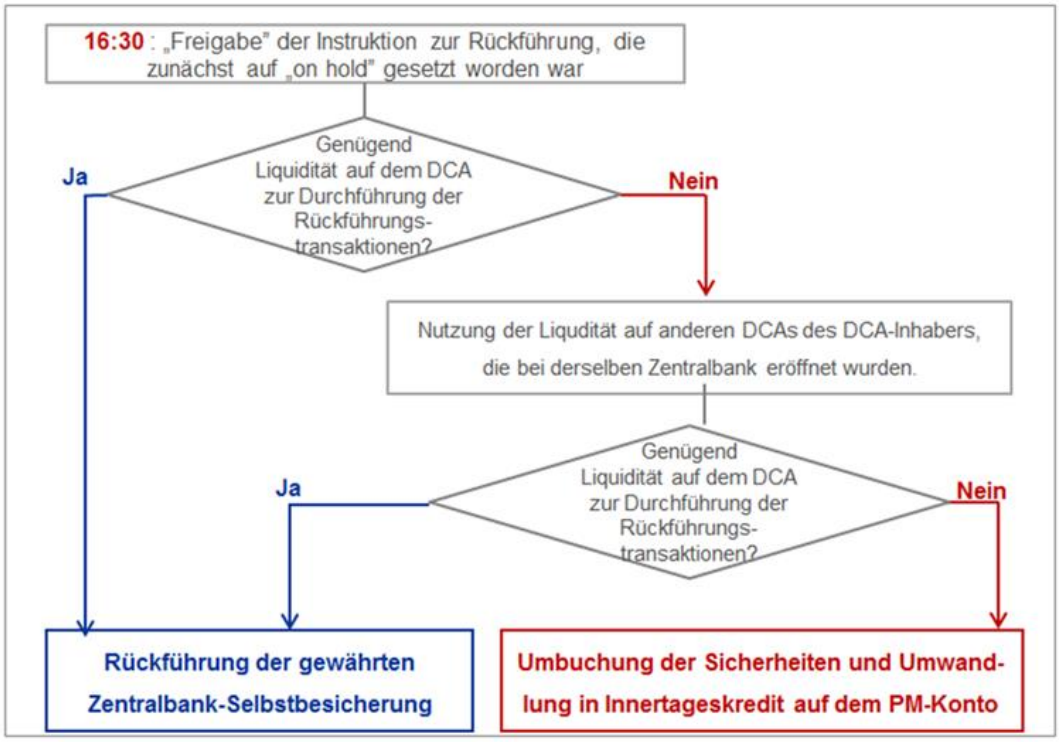


Abbildung 17: Automatische Rückführung der Zentralbank-Selbstbesicherung

Es gibt keine automatische Rückerstattung im Falle von Client Auto-Collateralisation.

4.1.8 Tagesendeverarbeitung

TARGET2 schließt um 18.00 Uhr. Die Schließung der Gemeinschaftsplattform wird durch eine Nachricht im ICM und im T2 IS bestätigt. Die Uhrzeit für den Annahmeschluss wird auch im ICM unter „Services" – „Administration" – „SSP Operating Day" angezeigt. In der Zeit von 18.00 Uhr bis 18.15 Uhr finden folgende Aktivitäten statt:

- Rückübertragung von Liquidität von den Unterkonten auf die Hauptkonten (Contingency-Verfahren)
- Zurückweisung von Zahlungen in der Warteschlange um 18.00 Uhr (unmittelbar nach Ablauf von Algorithmus 3)
- automatisches Verfahren, wenn der Leiter einer Kontengruppe die Konten nicht rechtzeitig ausgleichen konnte und ein Konto der Kontengruppe ohne vorhandene Besicherung in entsprechender Höhe überzogen ist
- automatische Liquiditätsübertragung an das PHA (optional)
- Nutzung der ständigen Fazilitäten bis 18.15 Uhr (bzw. 18.30 Uhr am letzten Tag der Mindestreserve-Erfüllungsperiode)
- automatische Liquiditätsübertragung auf das HAM-Konto (optional)
- Ausgleich der Kontengruppe (Contingency-Verfahren)
- Versand der Saldeninformationen an das RM-Modul
- Senden der Kontonachrichten (MT 940/MT 950) an die PM-Kontoinhaber (optional).

Nach 18.30 Uhr wird die interne Zentralbankverbuchung vorgenommen.

Was die T2S-Plattform betrifft, so könnte die Ausführung des Tagesendprozesses durch direkt angeschlossene T2S-Geldkontoinhaber per „Status of the T2S Settlement Day Notification", über einen Eintrag im GUI-Bildschirm „Daily Schedule" und/oder via „T2S Diary Query" bestätigt werden. Inzwischen generiert T2S alle Tagesschlussberichte und Kontoauszüge auf den T2S-Geldkonten – im Einklang mit der Berichtskonfiguration – und sendet sie an die direkt angeschlossenen T2S-Geldkontoinhaber. Indirekt angebundene T2S-Geldkontoinhaber erhalten keine Tagesschlussberichte aus T2S (und insbesondere keine Kontoauszüge).

4.2 Täglicher Betrieb in TIPS

4.2.1 Geschäftstag – für Euro-Zahlungen

TIPS verarbeitet Anweisungen kontinuierlich an 365 Tagen im Jahr, rund um die Uhr. Es gibt keine planmäßigen Schließungszeiten.

Der Geschäftstag von TIPS beginnt kurz nach dem Ende der Tagverarbeitung von TARGET2 (d. h. im Normalbetrieb kurz nach 18.00 Uhr). Die Abwicklung von Instant-Zahlungen und die Verarbeitung von Rückrufen erfolgt während des Geschäftstags ohne Unterbrechung. Der TIPS-Geschäftstag endet kurz nach dem Annahmeschluss für Interbankzahlungen in TARGET2 (im Normalbetrieb um 18.00 Uhr).

Der Wechsel auf einen neuen TIPS-Geschäftstag wird durch eine Reihe von Aktivitäten bei der Interaktion mit TARGET2 ausgelöst (siehe Abschnitt 4.2.3).

In bestimmten Zeitfenstern und zu bestimmten Zeitpunkten während eines Geschäftstags verarbeitet TIPS auch andere Arten von Instruktionen/Informationen, z. B. Liquiditätsübertragungen, Updates lokaler Referenzdaten und Abfragen/Meldeanfragen.

Folgende Instruktionen verarbeitet TIPS an 365 Tagen im Jahr, rund um die Uhr:

a) Instant-Zahlungen

b) serviceinterne Liquiditätsübertragungen

c) Rückruf-Anfragen und Rückruf-Antworten

d) Abfragen und Berichte

e) Updates lokaler Referenzdaten **mit sofortiger Wirkung**. Hierzu zählen lediglich:

- Sperrung/Entsperrung eines TIPS-Teilnehmers (nur für Zentralbanken verfügbar)
- Sperrung/Entsperrung eines Kontos (nur für Zentralbanken verfügbar)
- Sperrung/Entsperrung eines Credit Memorandum Balance (CMB)
- Aktualisierung eines CMB-Limits.

Zusätzlich werden während des Tages folgende Aktionen durchgeführt:[68]

a) 17.00 Uhr: Beginn der täglichen Übertragung der Daten aus dem CRDM

An jedem CRDM-Öffnungstag löst ein Ad-hoc-Ereignis die Übertragung aller TIPS- und MPL-

68 Alle genannten Uhrzeiten beziehen sich auf die MEZ.

Referenzdaten aus dem CRDM an TIPS bzw. MPL aus. Der Vorgang findet um 17.00 Uhr statt, um sicherzustellen, dass eine reibungslose und vollständige Übertragung der Referenzdaten erfolgt, bevor TIPS die Benachrichtigung über den Beginn eines neuen Geschäftstags erhält. Der Referenzdatensatz, der bei TIPS und MPL jeden Geschäftstag eingeht, umfasst alle aktiven Daten zum genannten Geschäftsdatum.

In einer Contingency-Situation in TIPS kann der Betreiber von TIPS eine tägliche Ad-hoc-Übertragung (Contingency-Übertragung) aus dem CRDM an TIPS auslösen. Die Contingency-Übertragung ist eine tägliche Übertragung, die innertägig ausgelöst wird, wenn eine sofortige Änderung eines Datensatzes durchgeführt werden muss, die nicht direkt in TIPS erfolgen kann.

b) 18.00 Uhr: Sperrung der Liquiditätsübertragungen (diese Uhrzeit ist unverbindlich und richtet sich nach dem Annahmeschluss für Interbankzahlungen in TARGET2, d. h. eine Verzögerung in TARGET2 führt zu einer verzögerten Sperrung der Liquiditätsübertragungen zwischen TARGET2 und TIPS).

c) Kurz nach 18.00 Uhr (im Normalbetrieb) und nach der Änderung des Geschäftstags in TIPS erstellt TIPS eine Hauptbuchdatei und sendet sie an TARGET2. Diese Datei enthält die Tagesendsalden der TIPS-Geldkonten für den abgelaufenen Geschäftstag.

d) 19.30 Uhr: Entsperrung der Liquiditätsübertragungen (diese Uhrzeit ist unverbindlich und richtet sich nach dem Beginn der Nachtverarbeitung in TARGET2, d. h. eine Verzögerung des Beginns der Nachtverarbeitung in TARGET2 führt zu einer verzögerten Entsperrung der Liquiditätsübertragungen zwischen TARGET2 und TIPS).

e) 22.00 Uhr – 1.00 Uhr: Sperrung der Liquiditätsübertragungen während des TARGET2-Wartungsfensters (diese Uhrzeiten sind unverbindlich und richten sich nach dem TARGET2-Wartungsfenster). Die Entsperrung erfolgt im Normalbetrieb um 1.00 Uhr.

Tritt im MPL eine Contingency-Situation auf, so kann der MPL-Betreiber eine tägliche Ad-hoc-Übertragung vom CRDM an den MPL-Service auslösen. Die Contingency-Übertragung ist eine tägliche Übertragung, die innertägig ausgelöst wird, wenn eine sofortige Änderung eines Datensatzes durchgeführt werden muss, die nicht direkt im MPL erfolgen kann. In diesem Fall werden folgende Schritte unternommen:

a) Alle für die tägliche Übertragung infrage kommenden und zum Zeitpunkt der Contingency-Übertragung gültigen Daten werden übertragen.

b) Die tägliche Übertragung wird wie geplant durchgeführt und umfasst alle am betreffenden Geschäftstag aktiven Daten.

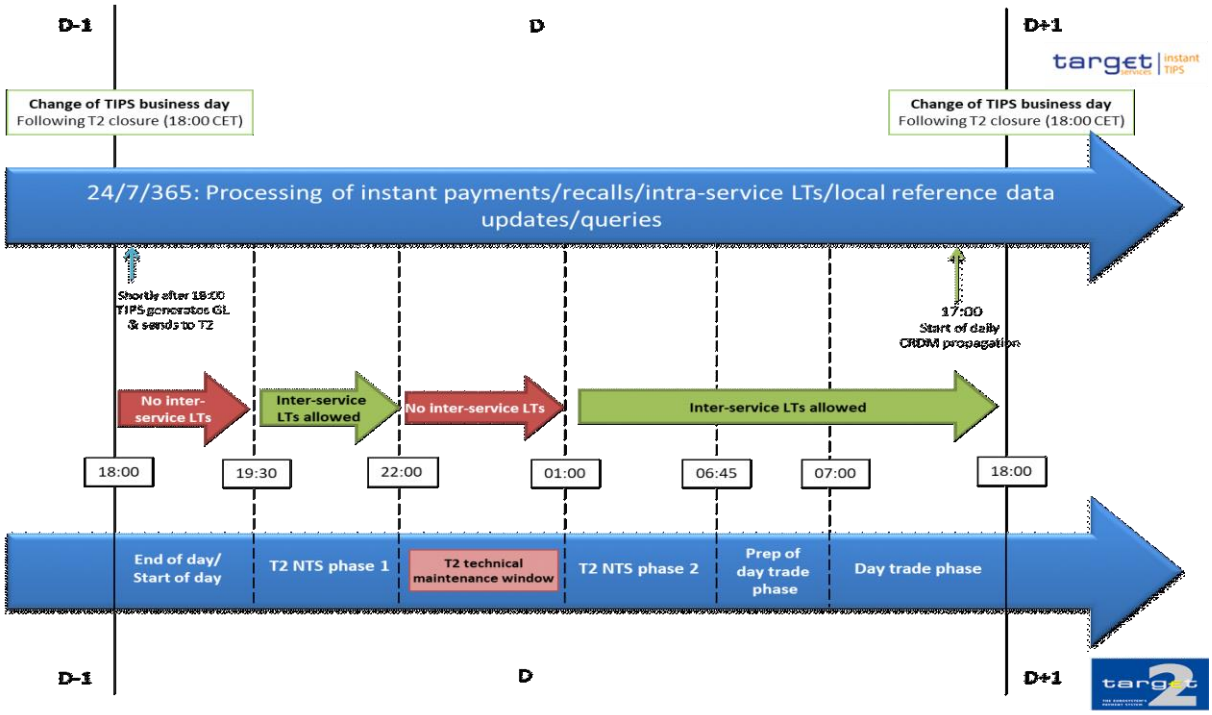


Abbildung 18: Überblick über den TIPS-Geschäftstag

4.2.2 Liquiditätsübertragungen – in Euro

In TIPS sind drei Arten der Liquiditätsübertragung vorgesehen: in Euro eingehende Liquiditätsübertragungen (von TARGET2 an TIPS), in Euro ausgehende Liquiditätsübertragungen (von TIPS an TARGET2) und serviceinterne Liquiditätsübertragungen in Euro.

Eingehende Aufträge zur Liquiditätsübertragung können nur in TARGET2 ausgelöst und von TIPS empfangen werden.

Ausgehende Aufträge zur Liquiditätsübertragung dienen der Liquiditätsrückverlagerung von einem TIPS-Geldkonto auf das jeweilige PM-Konto. Ausgehende Aufträge zur Liquiditätsübertragung können sowohl in TIPS als auch in TARGET2 (über die „Pull"-Funktionalität) ausgelöst werden.

Alle Liquiditätsübertragungen zwischen TIPS und TARGET2, gleich welcher Art, werden durch Bewegung der Liquidität über ein RTGS-Zwischenkonto abgewickelt.

Im Normalbetrieb können Liquiditätsübertragungen zwischen TIPS und TARGET2 in beiden Systemen zu folgenden Zeiten vorgenommen werden:

- 7.00 Uhr – 18.00 Uhr
- 19.30 Uhr – 22.00 Uhr
- 1.00 Uhr – 7.00 Uhr

Außergewöhnliche Ereignisse, die Veränderungen am Geschäftstag von TARGET2 nach sich ziehen, wirken sich entsprechend auch auf die Zeiten der Liquiditätsbereitstellung in beiden Systemen aus.

Durch serviceinterne Liquiditätsübertragungen kann Liquidität in TIPS zwischen TIPS-Geldkonten und TIPS ASTAs übertragen werden. Serviceinterne Liquiditätsübertragungen sind an 365 Tagen im Jahr rund um die Uhr möglich.

Liquiditätsübertragungen erfolgen, anders als Instant-Zahlungen, nicht über die Reservierung von Liquidität, sondern werden sofort abgewickelt.

4.2.3 Tagesendarbeiten – für Euro-Zahlungen

Der Wechsel des Geschäftstags erfolgt in TIPS ohne Leistungsunterbrechung kurz nach dem Ende der Tagverarbeitung in TARGET2 (d. h. im Normalbetrieb kurz nach 18.00 Uhr). Der Wechsel hängt von der Interaktion zwischen TIPS und TARGET2 ab und läuft wie folgt ab:

a) TARGET2 sendet eine Statusnachricht, die TIPS darüber informiert, dass der Annahmeschluss für Liquiditätsübertragungen erreicht wurde.

b) Alle weiteren Nachrichten über ausgehende Liquiditätsübertragungen, die TIPS nach dieser Nachricht erreichen, werden zurückgewiesen.

c) In der Zwischenzeit wird die Abwicklung von Liquiditätsübertragungen, die vor dem Annahmeschluss eingegangenen sind, sowohl in TIPS als auch in TARGET2 fortgesetzt. TARGET2 sendet weiterhin die damit zusammenhängenden Benachrichtigungen an TIPS, um alle ausstehenden Transaktionen in Einklang zu bringen. TIPS nimmt die eingehenden Liquiditätsübertragungen weiter an und verarbeitet diese.

d) Erhält TIPS die Bestätigung über den Abschluss der Abwicklung aller *schwebenden* Liquiditätsübertragungen, informiert es TARGET2, dass fortgefahren werden kann.

e) Wenn TARGET2 die Abwicklung der ausstehenden Liquiditätsübertragungen auf seiner Seite abgeschlossen hat und von TIPS die Bestätigung erhalten hat, dass fortgefahren werden kann, sendet TARGET2 eine weitere Statusnachricht, in der es TIPS mitteilt, dass das Datum des Geschäftstags umgestellt werden kann. Diese Statusnachricht enthält das neue Geschäftsdatum,

auf das TARGET2 wechselt. TIPS aktualisiert den Status und das Geschäftsdatum und beginnt, die Tagesendsalden für den gerade abgelaufenen Geschäftstag zu sammeln.

f) TIPS speichert den Stand der Salden im Moment des Eintreffens der Statusnachricht und sendet die Hauptbuchdatei an TARGET2. Die Salden der TIPS-Geldkonten am Tagesschluss werden für den Saldo des TARGET2-Teilnehmers berücksichtigt, entsprechend den in den RM-/SF-Links enthaltenen Informationen für die Mindestreservepflicht und die automatisierte Inanspruchnahme der Spitzenrefinanzierungsfazilität (Übernachtkredit).

g) TARGET2 sendet eine weitere Statusnachricht, in der TIPS informiert wird, dass wieder Liquiditätsübertragungen angenommen und verarbeitet werden können.

Der oben beschriebene Prozess gilt für den Normalbetrieb und wird in der nachstehenden Abbildung veranschaulicht:

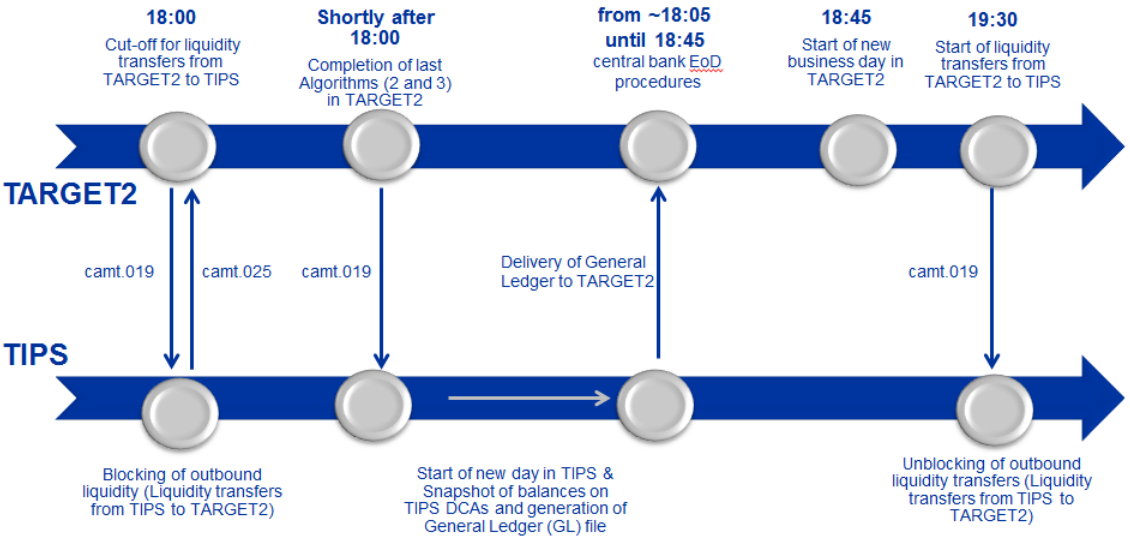


Abbildung 19: Tagesendarbeiten in TARGET2 und TIPS

4.2.4 Geplante TIPS-Ausfallzeiten

In Ausnahmefällen sind geplante Ausfallzeiten des TIPS-Service möglich. Dies kann vorkommen, wenn außergewöhnliche Änderungen erforderlich sind, die nicht ohne eine Unterbrechung des TIPS-Services vorgenommen werden können. In solchen Fällen werden die TIPS-Akteure a) im Voraus durch ihre Zentralbank über die bevorstehende Ausfallzeit informiert und b) am Tag der Ausfallzeit und/oder Wiederinbetriebnahme von TIPS über die Website der EZB auf dem Laufenden gehalten.

5 Grundsätzliche Aspekte der Verfahren für Ausnahmesituationen

5.1 Definition einer Störung

Störungen sind Situationen, die den normalen Betrieb von TARGET2 und/oder TIPS behindern. Solche Situationen können auf Probleme in der Gemeinschaftsplattform, der TIPS-Plattform, der T2S-Plattform, den PHAs, nationalen Anwendungen, Nebensystemen, bei direkten Teilnehmern und den SWIFT-Diensten oder Diensten von TIPS-Netzwerkdienstleistern zurückzuführen sein.

Eine Störung lässt sich als ein Ereignis definieren, das nicht zum Standardbetrieb gehört und zu einer Unterbrechung oder Einschränkung der von TARGET2 angebotenen Dienstleistungen führt bzw. führen kann. Die Folge könnte unmittelbar oder aber erst in einem späteren Stadium zu sehen und technischer, operationeller oder finanzieller Art sein. Jede Störung muss dokumentiert werden, und es ist so bald wie möglich eine Lösung zu finden und umzusetzen.

Störungen können sich aus einem oder mehreren der folgenden Ereignisse ergeben:

a) dem Ausfall einer wichtigen Komponente bzw. Software in der technischen Plattform des Systems

b) einem verfahrens- oder betriebstechnischen Fehler

c) Streiks oder schwerwiegenden externen Ereignissen (z. B. Naturkatastrophen, großflächige Stromausfälle, Terroranschläge, Koinzidenz von Ereignissen).

Die nachstehende Abbildung zeigt, welche Komponenten/Teilnehmer/Anbieter im Rahmen von TARGET2-/TIPS-Ausnahmesituationen betroffen sein können.

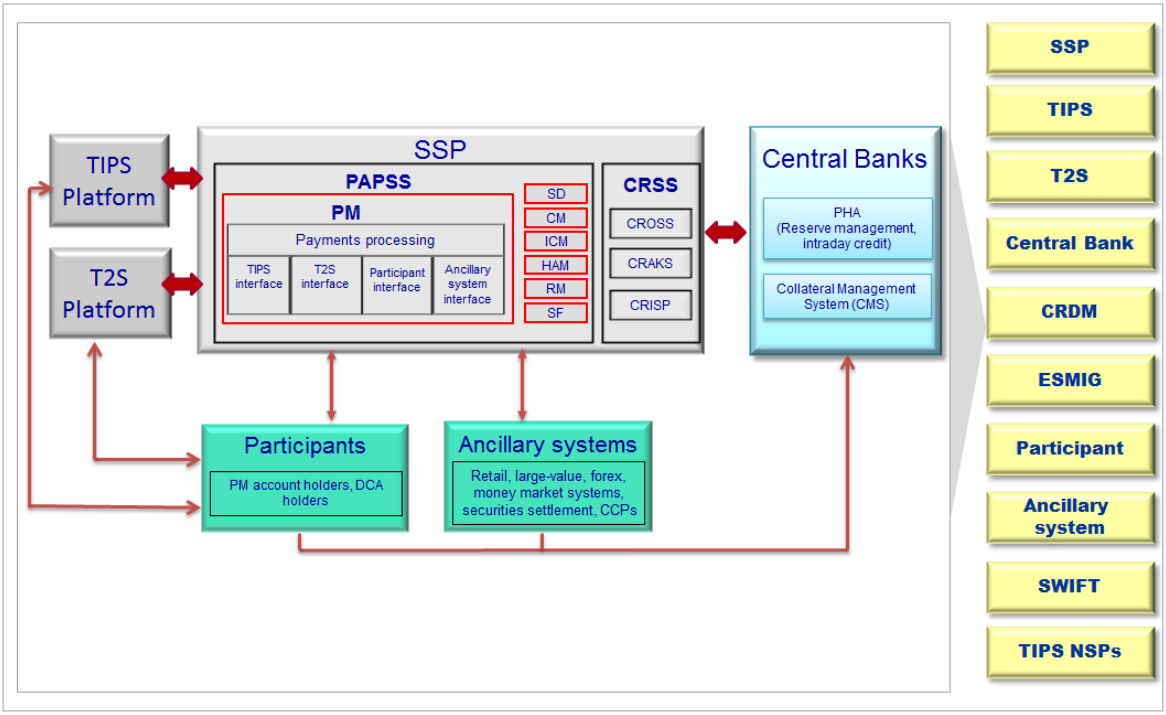


Abbildung 20: Ermittlung von potenziell von einer Störung betroffenen Komponenten/Teilnehmern/Anbietern

5.2 Verfahren zur Störungsbehebung

Die Behebung einer Störung beginnt mit der Problemidentifizierung. Die Identifikation von Problemen ist der Hauptzweck des Monitorings der verschiedenen Beteiligten. Sobald eine Abweichung vom Normalbetrieb erkannt und als Problem bestätigt worden ist, werden die Verfahren zur Kommunikation bei Störungen und zur Störungsbehebung eingeleitet. Bei TARGET2 und TIPS können Probleme entweder von TARGET2-Nutzern[69] oder von den Zentralbanken festgestellt werden.

Allgemein befassen sich die TARGET2-Maßnahmen zur Störungsbehebung mit folgenden Aspekten:

- Lösung/provisorische Lösung des Problems
- Business Continuity, d. h. Aufrechterhaltung der vollen Verarbeitungskapazität durch Umschalten auf ein zweites System/einen zweiten Standort/eine zweite Region
- Contingency-Verfahren, die die fortgesetzte Verarbeitung einer begrenzten Anzahl von Zahlungen ermöglichen
- Verlängerung des Annahmeschlusses, d. h. Verlängerung der Tagverarbeitung.

69 TARGET2-Nutzer bezieht sich auf TARGET2-Teilnehmer und Nebensysteme.

Da FIN-Nachrichten sowie InterAct- und FileAct-Dateien durch unterschiedliche SWIFT-Kanäle geleitet werden, könnte die InterAct- und FileAct-Verarbeitung bei einem Ausfall, der lediglich den FIN-Nachrichtenverkehr betrifft, fortgesetzt werden, wodurch die Abwicklung (sehr) kritischer Zahlungen möglich wäre.

Im Hinblick auf TIPS bietet das Eurosystem keine Contingency-Lösungen für Liquiditätsübertragungen im Zusammenhang mit TIPS an – weder für ausgehende noch für eingehende Liquiditätsübertragungen bei einem Ausfall der TIPS-Schnittstelle.

5.3 Kommunikation bei Störungen

In Ausnahmesituationen ist der Informationsfluss von entscheidender Bedeutung. Bei Störungen halten die TARGET2-Nutzer über nationale Kommunikationswege mit ihren üblichen für das Betriebsmanagement zuständigen Ansprechpartnern in der jeweiligen Zentralbank Kontakt.

Störungen mit möglichen systemischen Auswirkungen unterliegen einem koordinierten Management durch die Zentralbanken. Darüber hinaus gibt es bei den Zentralbanken eine interne Struktur für den Umgang mit TARGET2-Störungen, die zusätzlich zur normalen Organisationsstruktur eingesetzt wird.

Informationsbereitstellung bei Ausfällen

Bemerken die Zentralbanken einen Ausfall der Gemeinschaftsplattform oder andere Ausfälle, die sich auf die Abwicklung von TARGET2-Transaktionen auswirken könnten, aktivieren sie ihre internen, über die fest etablierten Telekonferenzsysteme laufenden Kommunikationswege für den Störungsfall. Nach der Festlegung des weiteren Vorgehens werden Informationen über die in Abschnitt 2.5.1 erläuterten Kommunikationsmittel gleichzeitig an alle TARGET2-Nutzer geleitet.

Um eine zeitnahe Kommunikation zu gewährleisten, bestehen die Mitteilungen aus im Voraus vereinbarten, standardisierten Begriffen und enthalten soweit verfügbar folgende Informationen:

a) Beschreibung des Fehlers

b) Erwartete Abwicklungsverzögerung (soweit möglich)

c) Information über die ergriffenen Maßnahmen und

d) Hinweise an die Nutzer.

Sind bei Feststellung einer Störung einige der oben genannten Angaben nicht verfügbar, wird zunächst eine relativ allgemein gehaltene Ankündigung des Vorfalls gemacht. Im weiteren Verlauf, in der Regel innerhalb von 30 Minuten nach der ersten Ankündigung, werden präzisere Angaben nachgereicht.

Sofern im Verlauf einer Störung weitere für die Nutzer relevante Informationen vorliegen, werden diese

über die obigen Kommunikationswege bekannt gegeben. Auf diese Weise werden die Nutzer auch von der Störungsbehebung in Kenntnis gesetzt.

6 Verfahren zur Handhabung von Störungen der Gemeinschaftsplattform

6.1 Verfahren bei Störungen zu Tagesbeginn (18.45 Uhr – 19.00 Uhr)

Der Abschluss des Tagesbeginns wird mit einer ICM-Nachricht an alle Nutzer bestätigt. Verzögert sich der Tagesbeginn, wird dies vom betreffenden National Service Desk über nationale Kommunikationswege, das T2 IS und gegebenenfalls das ICM mitgeteilt. Eine Verzögerung beim Tagesbeginn kann zu einem verzögerten Start der nachfolgenden Phasen führen und somit die Bereitstellung von Liquidität an die Nebensysteme, die TIPS-Geldkonten und/oder die T2S-Geldkonten beeinträchtigen.

6.2 Verfahren bei Störungen der Nachtverarbeitung[70] (19.00 Uhr – 22.00 Uhr und 1.00 Uhr – 7.00 Uhr)

Tritt eine Störung der Gemeinschaftsplattform während der Nachtverarbeitung auf, könnte sie sich negativ auf die Liquiditätsbereitstellung, die Nachtverarbeitung, auf die Liquiditätsübertragungen zwischen TIPS-/T2S-Geldkonten und PM-Konten und möglicherweise auch auf die Tagverarbeitung auswirken. Ansprechpartner für Nutzer der Nachtverarbeitung wäre auch hier der jeweilige National Service Desk.

Werden Daueraufträge zur Liquiditätsübertragung von PM-Konten auf TIPS-Geldkonten nicht rechtzeitig und/oder nicht erfolgreich durchgeführt, kann der normale Geschäftsbetrieb in TIPS dennoch fortgesetzt werden. Die Abwicklung von Instant-Zahlungen könnte jedoch durch eine Liquiditätsknappheit auf einigen TIPS-Geldkonten beeinträchtigt werden.

Werden Daueraufträge zur Liquiditätsübertragung von PM-Konten auf T2S-Geldkonten nicht rechtzeitig und/oder nicht erfolgreich ausgeführt, kann die T2S-Verarbeitung unter ausschließlicher Nutzung der Selbstbesicherung beginnen. Was die Liquiditätsübertragungen von den T2S-Geldkonten auf die PM-Konten betrifft, so sollten diese bis zur Wiederherstellung der Gemeinschaftsplattform in die Warteschlange gestellt werden. Je nach Art des SSP-Ausfalls besteht die Möglichkeit, das Problem entweder zu beheben oder gegebenenfalls eine Ausfallsicherung in die Wege zu leiten (siehe unten). Von großer Wichtigkeit ist es, zu allen nächtlichen Ereignissen und Maßnahmen, die Implikationen für den Beginn der Tagverarbeitung um 7.00 Uhr haben könnten, umfassende Informationen bereitzustellen. Der National Service Desk wird seine TARGET2-Nutzer daher vor dem regulären Start der Tagverarbeitung um 7.00 Uhr über die nationalen Kommunikationswege und über das T2 IS sowie

70 Keine Verfahren während des Wartungszeitraums (22.00 Uhr – 1.00 Uhr).

gegebenenfalls per ICM entsprechend informieren.

6.3 Betriebsfenster (6.45 Uhr – 7.00 Uhr)

Das Eurosystem nutzt das Betriebsfenster zur Vorbereitung der Tagverarbeitung. Bei Störungen gelten die Verfahren zur Störungsbehebung während der Tagverarbeitung.

6.4 Verfahren bei Störungen der Tagverarbeitung (7.00 Uhr – 18.00 Uhr)

6.4.1 Aufrechterhaltung des Geschäftsbetriebs (Business Continuity) auf der Gemeinschaftsplattform

Kann ein SSP-Problem nicht behoben werden, besteht das Hauptziel in der Wiederherstellung der vollen Verarbeitungskapazität. Die Entscheidung, eine Ausfallsicherung durchzuführen, hängt von der Art des Ausfalls, dessen voraussichtlicher Dauer, dem Zeitpunkt usw. ab. Dabei besteht keine definierte Hierarchie mit Blick auf intraregional (innerhalb einer Region) oder interregional (von einer Region zur anderen) zu ergreifende Ausfallsicherungen. Bei Problemen auf der Ebene der Gemeinschaftsplattform ist zu entscheiden, ob die Ausfallsicherung intraregional oder interregional erfolgen muss. Die Aktivierung letzterer Möglichkeit wird nur äußerst selten durchgeführt.

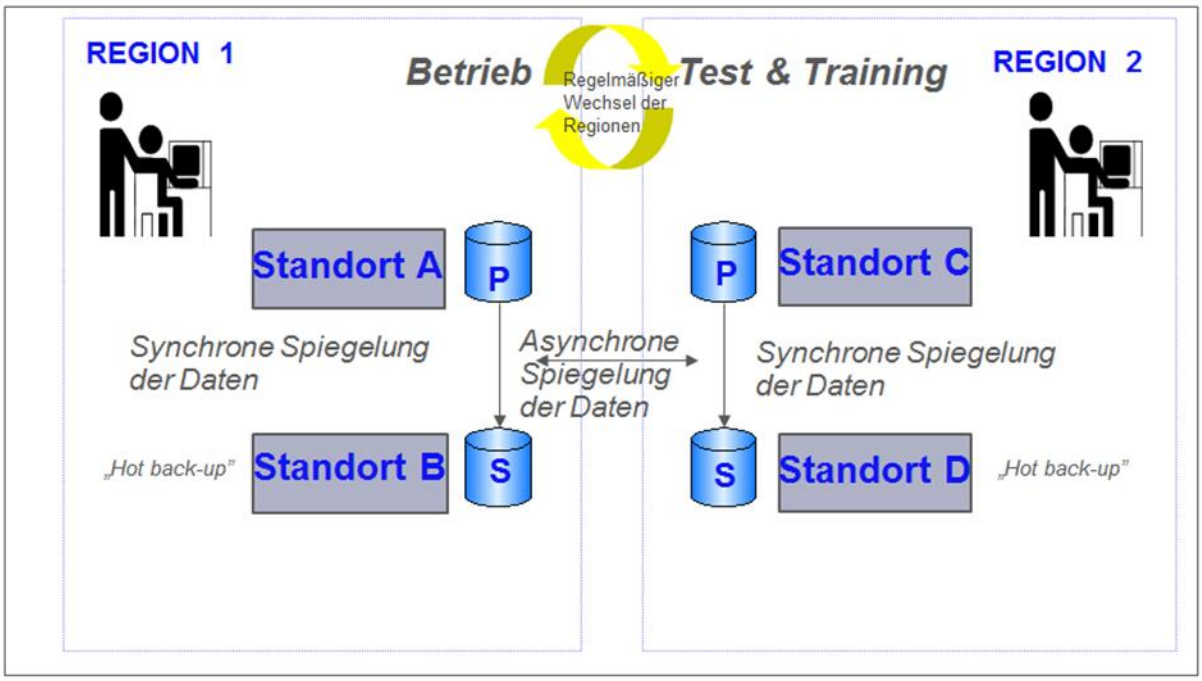


Abbildung 21: Zwei Regionen, vier Standorte

6.4.1.1 Intraregionale Ausfallsicherung

- Während kleinere Ausfälle durch die Sicherung der wichtigsten kritischen Elemente vor Ort aufgefangen werden können, erfordern größere Ausfälle oder Katastrophenfälle (z. B. Störungen wichtiger Hardware durch Brand, Überschwemmung, Terroranschläge oder Fehler in den Telekommunikationsanlagen) die Aktivierung des zweiten Standorts in derselben Region (intraregionale Ausfallsicherung).
- Eine intraregionale Ausfallsicherung bedeutet das Überwechseln von Standort A zu Standort B in ein- und derselben Region. Da im Synchronbetrieb gearbeitet wird, sind die Datenbanken an beiden Standorten auf exakt demselben Stand, weshalb keine Abstimmung nach der Ausfallsicherung erforderlich ist.
- Eine intraregionale Ausfallsicherung gewährleistet die Fortsetzung des normalen Geschäftsbetriebs binnen maximal einer Stunde nach erfolgter Entscheidungsfindung der Zentralbanken.
- Die Zahlungsabwicklung ist während der Ausfallsicherung unterbrochen, doch können die TARGET2-Nutzer weiterhin FIN-Zahlungsaufträge (die auf der SWIFT-Ebene in eine Warteschlange gestellt werden) und FileAct-Nachrichten (im Store-and-forward-Modus) an die Gemeinschaftsplattform senden.

6.4.1.2 Interregionale Ausfallsicherung

- Weitreichende regionale Störungen (z. B. schwerwiegende Verkehrs-, Telekommunikations- oder Stromversorgungsstörungen oder sonstige Beeinträchtigungen kritischer Infrastrukturen, die ein ganzes Ballungsgebiet oder einen geografischen Großraum erfassen) erfordern den Umstieg auf die zweite Region (interregionale Ausfallsicherung).
- Eine interregionale Ausfallsicherung bedeutet das Überwechseln von Region 1 zu Region 2, die in der Regel ein normales Herunterfahren des Standorts in Region 1 ermöglicht. Infolgedessen kann der Betrieb in Region 2 binnen zwei Stunden nach der Entscheidungsfindung ohne Datenverlust wiederaufgenommen werden. Die Nutzer werden informiert, sobald TARGET2 wieder voll zur Verfügung steht.
- Zu einem Datenverlust kann es dank des asynchronen Betriebs nach einer interregionalen Ausfallsicherung lediglich in dem extrem seltenen Fall kommen, dass die beiden Standorte in Region 1 unversehens gleichzeitig ausfallen. In einer solchen Situation bleibt nur die Möglichkeit der Ausfallsicherung auf die Region 2 und der Abstimmung der fehlenden Daten sowie der Wiederherstellung der Datenbasis. Gleichwohl sollte die Wiederaufnahme des Geschäftsbetriebs in Region 2 einschließlich der Rekonstruierung und Abstimmung der

SWIFTNet FIN-Nachrichten[71] binnen zwei Stunden nach der Entscheidungsfindung möglich sein. Der Wiederherstellungsprozess erfordert die aktive Beteiligung der Nutzer. Dieses Verfahren für interregionale Ausfallsicherungen mit Datenverlust, einschließlich des Wiederherstellungsprozesses, wird in Anhang I beschrieben.

- Die Zahlungsabwicklung wird während einer interregionalen Ausfallsicherung unterbrochen. Wenn die Nutzer weiterhin FIN-Zahlungsaufträge senden, so werden diese auf SWIFT-Ebene in eine Warteschlange gestellt und nach Wiederaufnahme des Betriebs der SSP abgewickelt. Dasselbe gilt für Liquiditätsübertragungen an/von TIPS-Geldkonten und/oder T2S-Geldkonten, die direkt über TIPS oder T2S oder über die TARGET2-Kern- oder -Zusatzleistungen initiiert wurden und auf Ebene der TIPS- oder T2S-Schnittstelle oder der SWIFT-Ebene in die Warteschlange eingestellt werden.

Behandlung von vorab eingereichten Zahlungsaufträgen

➢ Interregionale Ausfallsicherung **(ohne Datenverlust)**

Ist eine interregionale Ausfallsicherung ohne Datenverlust erfolgt und der hinter dem Codewort angegebene Zeitpunkt verstrichen, so funktioniert die Gemeinschaftsplattform nach den „normalen“ Verfahren. Dies bedeutet:

/FROTIME/	Zahlungen werden in die Verrechnung einbezogen
/TILTIME/	eine Warnmeldung wird im ICM angezeigt
/REJTIME/	Zahlungen werden zurückgewiesen

➢ Interregionale Ausfallsicherung **mit Datenverlust**

Ist eine interregionale Ausfallsicherung mit Datenverlust verbunden und der hinter dem Codewort angegebene Zeitpunkt verstrichen, arbeitet die Gemeinschaftsplattform nach einem besonderen Verfahren: Zahlungen mit dem Codewort /REJTIME/ werden nicht sofort zurückgewiesen, da die Zeitangabe in einen in der Zukunft liegenden Zeitpunkt umgewandelt wird.

71 Die Wiederherstellung ist eine von SWIFT angebotene Dienstleistung, die gegenüber den TARGET2-Nutzern nach dem üblichen SWIFT-Gebührenmodell abgerechnet wird.

Behandlung von Nebensystem-Transaktionen, für die optionale Dienste genutzt werden

Abwicklungsverfahren	Optionaler Dienst	Auswirkung bei Verstreichen des Zeitpunkts
1, 2	festgelegter Abwicklungszeitpunkt („von“)	Abwicklung
	Abwicklungszeitraum („bis“)	Zurückweisung
3	Informationsfrist	Abwicklungsversuch
	Abwicklungszeitraum („bis“)	Zurückweisung
4, 5	Informationsfrist	Abwicklungsversuch
	Abwicklungszeitraum („bis“) - ohne Garantieperiode - mit Garantieperiode	 Zurückweisung Aktivierung des Garantiekonto-Verfahrens

Tabelle 9: Behandlung von Nebensystem-Transaktionen

Bei einer interregionalen Ausfallsicherung mit Datenverlust verschieben die drei Anbieter-Zentralbanken die Informationsfrist auf 15 Minuten vor dem Annahmeschluss für Kundenzahlungen und verlegen das Ende der Abwicklungszeit auf den Annahmeschluss für Kundenzahlungen, um eine Zurückweisung von Zahlungen nach der Wiedereröffnung der Gemeinschaftsplattform zu vermeiden.

6.4.2 Contingency-Abwicklung mithilfe der Enhanced Contingency Solution (ECONS I)[72]

Die Contingency-Abwicklung umfasst die manuelle Abwicklung von Zahlungen während eines Ausfalls der Gemeinschaftsplattform. Im Falle des Ausfalls der Gemeinschaftsplattform sind die Zahlungsmöglichkeiten der Teilnehmer und der Nebensysteme in der Gemeinschaftsplattform blockiert.

Die Contingency-Abwicklung mit ECONS I ist eine vorübergehende Maßnahme, bei der eine begrenzte Anzahl an Transaktionen abgewickelt wird. Vorrangiges Ziel ist es, die Entstehung eines systemischen Risikos zu vermeiden.[73] Nach der Entscheidung, eine Contingency-Abwicklung über ECONS I einzuleiten, soll der normale TARGET2-Betrieb so schnell wie möglich wieder aufgenommen werden. Es ist jedoch nicht vollkommen auszuschließen, dass der normale TARGET2-Betrieb unter sehr außergewöhnlichen und extremen Umständen für längere Zeit nicht verwendet werden kann. Die Contingency-Abwicklung über ECONS I bietet zwar keine vollumfänglichen RTGS-Services, sie kann jedoch über mehrere Tage hinweg genutzt werden und ermöglicht, dass ein Geschäftstag ordnungsgemäß abgeschlossen und das Wertstellungsdatum geändert werden kann.

Das Konzept der (sehr) kritischen TARGET2-Zahlungen legt fest, welche Zahlungen als systemisch relevant und somit als für die Contingency-Abwicklung zugelassen eingestuft werden. In Kasten 4 wird erläutert, welche Zahlungen abgewickelt werden sollten (sehr kritische Zahlungen) und welche fakultativ abgewickelt werden können (kritische Zahlungen).

TARGET2-Nutzer können sich an ECONS I anbinden und Geschäfte, die sie für ihre Geschäftstätigkeit als kritisch erachten über eine grafische Benutzeroberfläche (GUI) im U2A-Modus einreichen. Die eingereichten Zahlungen werden nur nach Genehmigung durch den zuständigen National Service Desk abgewickelt. Kasten 5 am Ende des Kapitels bietet den National Service Desks eine Entscheidungshilfe für die Freigabe kritischer Zahlungen.

Eine Anbindung an ECONS I ist für die Zentralbanken des Eurosystems, kritische Teilnehmer und kritische Nebensysteme[74] sowie für Nutzer obligatorisch, die sehr kritische Zahlungen in TARGET2 abwickeln (d. h. Teilnehmer, die CLS- und/oder EURO1-Zahlungen oder Margenausgleiche für CCPs abwickeln). ECONS I ist über die standardmäßige SWIFT-Schnittstelle zugänglich und wird stets in der nicht aktiven Region der Gemeinschaftsplattform betrieben.

Aufgrund der nachstehenden Einschränkungen ist der Durchsatz im Contingency-Fall begrenzt:

---

72 Die Contingency-Abwicklung mithilfe des Contingency-Netzwerks wird in Kapitel 7.4 dargestellt.

73 Der Einsatz von ECONS I hindert die Nebensysteme nicht an der Nutzung ihrer eigenen alternativen Contingency-Mechanismen (z. B. die Hereinnahme zusätzlicher Sicherheiten oder anderer Währungen).

74 Nebensysteme, die nur ASI-Dateien abwickeln, können lediglich den Abwicklungsstatus überwachen, aber keine Zahlungen einreichen.

- Es muss frische Liquidität bereitgestellt werden.
- Es ist ein Mechanismus zur Nichtabstreitbarkeit der Herkunft (Non Repudiation of Origin) anzuwenden.
- Die Kapazität von ECONS I ist auf rund 40 000 Transaktionen pro Tag beschränkt.
- Nebensystem-Dateien können mithilfe des Abwicklungsverfahrens 4 abgewickelt werden, wenn sie von einer Zentralbank im Auftrag eines Nebensystems in A2A gesendet werden.

6.4.2.1 Aktivierungsverfahren für ECONS I

Der Beschluss, ECONS I zu aktivieren und zu nutzen, wird von den Settlement-Managern, die die National Service Desks vertreten, in einer Telekonferenz gefasst. Bei Initiierung des Contingency-Verfahrens werden die Teilnehmer über die Kommunikationskanäle informiert, die im vorliegenden Dokument in Abschnitt 2.5.1 und Abschnitt 5.3 erläutert sind.

Zentralbanken und Nutzer können über die Standardschnittstelle auf ECONS I zugreifen (mittels einer spezifischen URL).[75] ECONS I beginnt mit einem Saldo von null, d. h. die Zahlungskapazität der Gemeinschaftsplattform steht für eine Contingency-Abwicklung über ECONS I nicht zur Verfügung. Folglich erfordert die Abwicklung von Contingency-Zahlungen in ECONS I die Bereitstellung von frischer Liquidität durch die TARGET2-Nutzer.

6.4.2.2 Zahlungsabwicklung in ECONS I

1. TARGET2-Nutzer, die Contingency-Zahlungen vornehmen wollen, müssen dazu neue Liquidität bereitstellen. Neue Liquidität kann – entsprechend den jeweiligen nationalen Bestimmungen – aus den folgenden Quellen stammen:
    - Bereitstellung neuer Sicherheiten
    - Nutzung bereits vorhandener Sicherheiten, die nicht für andere Zwecke verwendet werden (abhängig von den nationalen Vorgaben für das Sicherheitenmanagement)
    - Nutzung von speziell für Contingency-Fälle vorgesehenen Sicherheiten (abhängig von den nationalen Vorgaben für das Sicherheitenmanagement)
    - Liquiditätsübertragungen von T2S nach ECONS I – Eine Übertragung von Liquidität (auch von ECONS I nach T2S) ist auf indirektem Wege möglich,

75 Zahlungen können von Zentralbanken und Teilnehmern eingestellt werden. Nebensysteme hingegen haben nur die Möglichkeit, sich die aktuelle Liquidität anzeigen zu lassen.

indem parallel Übertragungen zwischen den Konten der Teilnehmer und der Zentralbank in T2S und in ECONS 1 durchgeführt werden (wobei die Details der Abwicklung von den nationalen Vorgaben abhängig sind).

- Eingehende Zahlungen innerhalb von ECONS I
- Sonstige (abhängig von den nationalen Vorgaben für das Sicherheitenmanagement)

Die Verfahren zur Bereitstellung zusätzlicher Sicherheiten hängen von den jeweiligen nationalen Regelungen ab, die möglicherweise auf T2S zurückgreifen. Sollte es also zeitgleich zu einer T2S-Störung kommen, kann es für TARGET2-Nutzer unter Umständen schwierig werden, zusätzliche Sicherheiten bereitzustellen. Es können jedoch zusätzliche nationale Möglichkeiten zur Liquiditätsbereitstellung genutzt werden.

Zwischen ECONS I und TIPS sind unabhängig von der Richtung keine Contingency-Zahlungen möglich.

2. TARGET2-Nutzer können ihre aktuellen Salden in ECONS I einsehen. Sobald die Liquidität (von einer Zentralbank oder über eingehende Zahlungen) auf den Konten in ECONS I für einen TARGET2-Nutzer bereitgestellt wurde, kann der Nutzer mit der Abwicklung von Contingency-Zahlungen beginnen. Der Sender erfasst Zahlungen direkt in ECONS I. Kann ein Teilnehmer einen Zahlungsauftrag nicht erfassen (weil er beispielsweise keine Verbindung zu ECONS I herstellen kann), kann er seine Zentralbank über die entsprechenden nationalen Kommunikationswege ersuchen, eine Contingency-Zahlung zu instruieren.

3. Die Zentralbank des Senders kann der Abwicklung zustimmen oder sie ablehnen; dabei hat sie insbesondere sicherzustellen, dass sehr kritische Zahlungen und Zahlungen mit SIPS-Bezug (gemäß Definition des Eurosystems) abgewickelt werden. Die Zustimmung zu oder Ablehnung von kritischen Zahlungen erfolgt nach bestem Wissen und Gewissen.

4. Die zuständige Zentralbank und der Zahlungsempfänger (sofern er an ECONS I angebunden ist) sehen alle eingehenden Zahlungen in ECONS I, und zwar sortiert nach Zeitpunkt des Eingangs und Betrag. Wird eine Zahlung an das Konto eines Nutzers gesendet, der nicht an ECONS I angebunden ist, informiert die zuständige Zentralbank diesen Nutzer nach besten Möglichkeiten im Rahmen der zur Verfügung stehenden Ressourcen über den Zahlungseingang.

5. ECONS I ermöglicht es Zentralbanken oder dem in deren Auftrag handelnden SSP Service Desk, auf Anfrage von Nebensystemen Transaktionsdateien im A2A-Modus für die Nebensystemverrechnung zu versenden (nur ASI-Verfahren 4). Zur Einreichung der Dateien an die zuständige Zentralbank sind die bilateral vereinbarten Übertragungskanäle zu verwenden.

ECONS I unterstützt das ASI-Verfahren 4 unter Nutzung eines technischen Kontos. ANMERKUNG: Das genannte Verfahren der Zustimmung/Ablehnung gilt nicht für Zahlungen, die NZBen im Auftrag von Nebensystemen als Dateien hochladen. Beantragt ein Nebensystem, das normalerweise ein anderes AS-Abwicklungsverfahren für Nebensystemzahlungen verwendet, die Abwicklung von Nebensystem-Dateien, muss die zuständige Zentralbank kontaktiert werden und es können – soweit möglich – andere Lösungen in Erwägung gezogen werden.

6.4.2.3 Nutzung von ECONS I für mehr als einen Tag

ECONS I kann für die Abwicklung von Contingency-Zahlungen an mehreren aufeinanderfolgenden Tagen (bis zu 5 Geschäftstage) verwendet werden und ermöglicht den Abschluss von Geschäftstagen/die Änderung des Wertstellungsdatums. Bei mehrtätiger Nutzung dauert der ECONS I-Geschäftstag von 7.00 Uhr bis 18.00 Uhr, soweit die Krisenmanager nichts anderes beschließen.

Wird eine Fortsetzung der Contingency-Abwicklung auch am folgenden Geschäftstag beschlossen, dann werden die Nutzer über die entsprechenden nationalen Kommunikationswege und das T2IS kurz nach Ende des aktuellen ECONS I-Geschäftstags darüber informiert.

Bei Öffnung von ECONS I an mehreren aufeinanderfolgenden Tagen erfolgt die Zahlungsabwicklung weiterhin auf Basis der ursprünglich bereitgestellten Liquidität und/oder den eingehenden Zahlungen. Werden die von einem Teilnehmer zur Verfügung gestellten Sicherheiten im Hinblick auf den gewährten Kredit als nicht ausreichend erachtet (z. B. am Ende eines ECONS I-Geschäftstags), kann eine Zentralbank eine Anpassung des gewährten Kredits zu Beginn des neuen ECONS I-Geschäftstags einfordern (Margin Call). Zusätzlich besteht die Möglichkeit, dass die Zahlungsabwicklung so lange aufgeschoben wird, bis der Teilnehmer zusätzliche Sicherheiten bereitgestellt hat.

6.4.2.4 Abschluss der Abwicklung über ECONS I

Wenn die Gemeinschaftsplattform vollständig wiederhergestellt ist, werden die Nutzer über lokal eingerichtete Kommunikationswege darüber informiert, dass ein Wechsel der Zahlungsabwicklung von ECONS I zurück zur Gemeinschaftsplattform erfolgt.

Danach wird ECONS I geschlossen. Die verarbeiteten Daten stehen den Nutzern noch bis zum Ende des Geschäftstags zur Verfügung. Mit Schließung von ECONS I werden die Schlusssalden der ECONS-I-Konten auf das Zahlungsmodul übertragen und dort verbucht (keine Übertragung der einzelnen zugrunde liegenden Zahlungen). Die Tage, in denen eine Contingency-Abwicklung stattfand, werden als geschäftsfreie Tage im TARGET2-Kalender des Stammdatenmoduls erfasst.[76]

[76] Bei einer mehrtägigen Contingency-Abwicklung stellt ECONS I Kontoauszüge für jeden Geschäftstag direkt über eine

ECONS I kann erneut gestartet werden, wenn am gleichen Tag eine weitere Störung der Gemeinschaftsplattform auftritt oder es Unstimmigkeiten bei den Salden gibt (fehlender Teilnehmer-BIC).

6.4.2.5 Zusätzliche Informationen zur Nutzung von ECONS I

- Die Informationen über die ECONS I-Salden sowie Belastungen und Gutschriften stehen den jeweiligen Nutzern und deren Zentralbanken zur Verfügung.
- Alle Contingency-Zahlungen müssen vom Sender und nicht vom Begünstigten veranlasst werden.
- Alle ECONS I-Konten müssen den korrespondierenden PM-Konten entsprechen. Wenn ECONS I aktiviert wird, werden für PM-Teilnehmer automatisch Konten eröffnet, die die existierenden PM-Konten spiegeln.
- Eine Anbindung an ECONS I ist nur für direkte PM-Teilnehmer mit SWIFT-basiertem Zugang relevant.
- Um die Anzahl der Contingency-Zahlungen zu verringern, sollten die TARGET2-Nutzer Sammelüberweisungen verwenden.
- Hat ein TARGET2-Nutzer eine Zahlung an die Gemeinschaftsplattform übermittelt, die zunächst in die Warteschlange eingestellt wurde, und wickelt diese erneut über ECONS I ab, lässt sich eine „doppelte Ausführung“ der Zahlung nicht vermeiden (zunächst in ECONS I und dann nach Neustart der Gemeinschaftsplattform ein zweites Mal im Zahlungsmodul). Der Sender trägt die alleinige Verantwortung, geeignete Maßnahmen zur Vermeidung von Doppelausführungen zu ergreifen.

Kasten 4 Das Konzept (sehr) kritischer TARGET2-Zahlungen

Wichtigste Grundsätze:

- Die TARGET2-Contingency-Abwicklung ist im Wesentlichen für Zahlungen gedacht, die verarbeitet werden müssen, um ein systemisches Risiko während des Tages zu vermeiden.
- Aufgrund der technisch und operativ bedingten Volumenbeschränkungen in TARGET2-

eigens dafür vorgesehene Bildschirmmaske bereit, während die MT 940/MT 950-Nachrichten am Ende der Contingency-Abwicklung versendet werden, jedoch nur die Informationen zum letzten Geschäftstag enthalten (siehe UDFS Annex ECONS I (version 13.0)).

Contingency-Situationen sollte die Gesamtzahl der Contingency-Zahlungen möglichst gering gehalten werden.

- In erster Linie sollten ausgehende TARGET2-Zahlungen berücksichtigt werden. Ausgehende Zahlungen sind Zahlungen, die von anderen Systemen benötigt werden.
- Eingehende Zahlungen (z. B. Auszahlungen von Nebensystemen, Liquiditätsübertragungen zwischen Finanzinstituten, geldpolitische Geschäfte) könnten unter bestimmten Umständen als kritische Zahlungen betrachtet werden, wenn sich belegen lässt, dass sie zur Deckung (sehr) kritischer ausgehender Zahlungen benötigt werden. In diesem Fall können die Krisenmanager der Verarbeitung zustimmen. In jedem Fall sollte die Anzahl dieser Zahlungen strikt beschränkt bleiben.

Die folgenden Zahlungsarten unterliegen der Contingency-Abwicklung:

- Sehr kritische Zahlungen müssen in Contingency-Situationen verarbeitet werden (Reihenfolge: CLS, FIFO):
  - Zahlungen von TARGET2 an CLS („pay-ins“) im Zusammenhang mit der Abwicklung von CLS-Kernabwicklungsdienstleistungen
  - Zahlungen im Zusammenhang mit Ausgleichszahlungen am Tagesabschluss an EURO1 („pay-ins“; nur, wenn die EZB die Zentralbanken darüber informiert hat, dass diese Zahlungen über ECONS I abgewickelt werden sollen), und
  - Zahlungen im Zusammenhang mit Margin Calls an zentrale Kontrahenten („pay-ins“)
- Sonstige SIPS-Zahlungen[77] (z. B. STEP2)
- Kritische Zahlungen, d. h. Zahlungen, die erforderlich sind, um die Entstehung eines systemischen Risikos zu vermeiden. Beispiele hierfür sind:
  - Verrechnungszahlungen an Wertpapierabwicklungssysteme zur Echtzeitabwicklung,
  - eingehende Zahlungen und Zahlungen, durch die Liquidität im Euroraum (um)verteilt wird, wenn sich belegen lässt, dass sie zur Deckung (sehr) kritischer ausgehender Zahlungen erforderlich sind.

77 Gemäß Artikel 10 der EZB-Verordnung zu den Anforderungen an die Überwachung systemrelevanter Zahlungsverkehrssysteme (SIPS-Verordnung).

Kasten 5 Aspekte, die bei der Entscheidung über die Auswahl kritischer Zahlungen zu berücksichtigen sind

Zusätzlich zu den drei wichtigsten Grundsätzen (Vermeidung eines systemischen Risikos, Beschränkung des Verarbeitungsvolumens und Konzentration auf ausgehende Zahlungen) können folgende Aspekte berücksichtigt werden:

- Die Umstände des Ausfalls, insbesondere sein Zeitpunkt: Neben Tagesbeginn und Tagesende sind auch die Abwicklungszeiten der Nebensysteme kritisch. Mögliche systemübergreifende Konsequenzen, die Ursache des Ausfalls und seine Dauer sowie die voraussichtlich für die Wiederherstellung benötigte Zeit sind ebenfalls wichtige Aspekte. Der Geschäftstag: Es könnte von Bedeutung sein, ob eine Störung am Ende der Mindestreserve-Erfüllungsperiode, an einem Feiertag oder an einem Tag auftritt, an dem mit einem besonders hohen Zahlungsvolumen gerechnet wird.
- Der von Banken, Nebensystemen oder anderen Geschäftsbereichen der Zentralbank geäußerte Bedarf (z. B. im Zusammenhang mit geldpolitischen Geschäften).
- Die Liquiditätsbeschränkungen: Eine Contingency-Verarbeitung würde zusätzliche Sicherheiten erfordern. Je mehr Zahlungen in einer Contingency-Situation abgewickelt würden, umso mehr zusätzliche Sicherheiten müsste eine Bank also stellen. Je nach dem Zeitpunkt, an dem der Contingency-Fall eintritt, könnte sich die Bereitstellung solcher Sicherheiten als schwierig erweisen.
- Das Prinzip der Priorisierung: Sehr kritische Zahlungen sollten im Allgemeinen vor kritischen Zahlungen verarbeitet werden (solange die kritischen Zahlungen nicht zur Auflösung einer Anstauung sehr kritischer Zahlungen benötigt werden).
- Die Maßnahmen zur Störungsbehebung könnten den Bedarf an Contingency-Zahlungen verringern. Beispielsweise könnten große Nebensysteme ihre Abwicklung um den gleichen Zeitraum verlängern, um den sich der Annahmeschluss von TARGET2 verzögert. Zahlungen in der Warteschlange würden verarbeitet, sobald die Gemeinschaftsplattform wieder verfügbar ist. Als weiteres Beispiel könnten Nebensysteme eine Verrechnung versuchen, selbst wenn der Annahmeschluss in TARGET2 verschoben wird.
- Die Contingency-Mechanismen des Marktes: Mögliche alternative Contingency-Mechanismen von einzelnen Nebensystemen und Banken (z. B. Einzahlungen in einer anderen Währung) könnten die Notwendigkeit verringern, im Contingency-Fall kritische Zahlungen abzuwickeln.

6.4.3 Verlängerung des Annahmeschlusses

Die Entscheidung, bei einem Ausfall der Gemeinschaftsplattform die Schließung hinauszuschieben, d. h. die Tagverarbeitungsphase zu verlängern, wird stets von den Krisenmanagern getroffen. Die angekündigte neue Schlusszeit ist der neue Annahmeschluss für Interbankzahlungen. Dabei informiert das Eurosystem die Nutzer so frühzeitig wie möglich über die mögliche Dauer der Verlängerung. Solange dies nicht absehbar ist, insbesondere, wenn ein längerer Ausfall der Gemeinschaftsplattform vorliegt, werden in regelmäßigen Abständen aktualisierte Lageinformationen bereitgestellt. Durch eine Verlängerung der Tagverarbeitungsphase verschiebt sich auch der Annahmeschluss für Kundenzahlungen um den gleichen Zeitraum, wobei davon ausgegangen wird, dass die Verlängerung des Annahmeschlusses mindestens 15 Minuten vor dem eigentlichen Annahmeschluss für Kundenzahlungen (d. h. spätestens um 16.45 Uhr) bewilligt wird. Es ist nicht möglich, nur den Annahmeschluss für Kundenzahlungen zu verschieben.

Abgesehen von den geschilderten Situationen im Zusammenhang mit einem Ausfall der Gemeinschaftsplattform, die zu einer Verlängerung des Annahmeschlusses führen könnten, kommt es möglicherweise zu Situationen, in denen die Schlusszeit verschoben wird, um eine Bankenkrise in den Griff zu bekommen.

Grundsätzlich sollten TARGET2 und T2S für die Euro-Abwicklung immer am gleichen Valutatag in Betrieb sein, d. h., insofern TARGET2 am Tag D noch für die Geldverrechnung in Euro geöffnet ist, sollte T2S keine Wertpapierverrechnung in Euro am Tag D+1 zulassen. Somit sollte im Falle einer verzögerten TARGET2-Schließung eine verzögerte T2S-Schließung, ein verzögerter T2S-Beginn des nächsten Abwicklungstags oder ein T2S-Start ohne die Möglichkeit der Verrechnung in Euro ins Auge gefasst werden. Ein Vorteil einer verzögerten T2S-Schließung könnte darin liegen, dass Sicherheiten über T2S aktiviert werden könnten, um Liquidität für eine Abwicklung in ECONS I bereitzustellen.

Bei einer Verzögerung in TARGET2 informiert der TARGET-Services-Koordinator umgehend den T2S-Koordinator, damit der T2S-Prozess zur Störungsbehebung in Gang gesetzt werden kann. Doch wenn die T2S-Geldkonten über einen Nullsaldo verfügen, die Selbstbesicherungspositionen geschlossen sind und keine Wiederherstellungsaktivitäten nach dem Neustart im Anschluss an einen Katastrophenfall erforderlich sind, entfällt womöglich eine T2S-Verzögerung.

Bei einer Verlängerung des Annahmeschlusses für TARGET2 kommt es in TIPS bei der Änderung des Geschäftstags zu einer Verzögerung. Die Abwicklung von Instant-Zahlungen ist davon nicht betroffen.

6.4.3.1 Verlängerung des Annahmeschlusses aufgrund eines zuvor aufgetretenen SSP-Ausfalls

Um dem Markt zusätzliche Betriebszeit zur Verfügung zu stellen, kann die Tagverarbeitungsphase verlängert werden, wenn ein Ausfall der Gemeinschaftsplattform im Laufe des Tages auftritt, aber vor

18.00 Uhr behoben wird. Eine solche Verlängerung sollte zwei Stunden nicht überschreiten und frühzeitig angekündigt werden, um den TARGET2-Nutzern Klarheit und Sicherheit zu verschaffen. Wird eine solche Verlängerung vor 16.45 Uhr gewährt, sollte zwischen den Annahmeschlusszeiten für Kunden- und für Interbankzahlungen weiterhin mindestens eine Stunde liegen. Eine Verlängerung der Annahmefrist könnte auch bewilligt werden, um die Bewältigung einer Bankenkrise zu erleichtern.

Sobald eine Verlängerung gewährt ist, darf sie nicht mehr zurückgenommen werden, selbst wenn dies technisch möglich wäre.

6.4.3.2 Verlängerung des Annahmeschlusses aufgrund einer anhaltenden SSP-Störung

Ein späterer Annahmeschluss wird bewilligt, wenn ein Ausfall der Gemeinschaftsplattform vor 18.00 Uhr auftritt und bis zu diesem Zeitpunkt nicht behoben ist. In solchen Situationen gibt es keine andere Möglichkeit, als die Wiederherstellung der Plattform abzuwarten.

Unmittelbar nachdem die Krisenmanager in ihrer Telekonferenz einen Aufschub des Annahmeschlusses genehmigt haben, werden die TARGET2-Nutzer über die einschlägigen nationalen Kommunikationswege, das ICM (falls verfügbar), das TIPS IS und das T2 IS darüber informiert. Die TARGET2-Nutzer werden aufgefordert, ihre internen Vorgaben an die verzögerte Annahmeschlusszeit entsprechend anzupassen.

Bei einer Verlängerung der Annahmeschlusszeit sollten die TARGET2-Nutzer auch weiterhin SWIFTNet FIN-Nachrichten an die Gemeinschaftsplattform senden. Diese werden in eine Warteschlange gestellt und verarbeitet, sobald die Gemeinschaftsplattform wiederhergestellt ist. Dem liegt das Prinzip zugrunde, dass TARGET2 alle in einer Warteschlange befindlichen Zahlungen mit gleichtägiger Wertstellung abwickelt, um die Plattform restlos und endgültig schließen zu können.

Schritte nach der Wiederherstellung der Gemeinschaftsplattform

Nachstehend wird von einem Ausfall der Gemeinschaftsplattform in der Tagverarbeitung ausgegangen. Tritt der Ausfall zu einem späteren Zeitpunkt auf, beispielsweise zu Tagesbeginn, sind lediglich die übrigen Schritte relevant (als Kästen dargestellt).

Am Tag der Störung

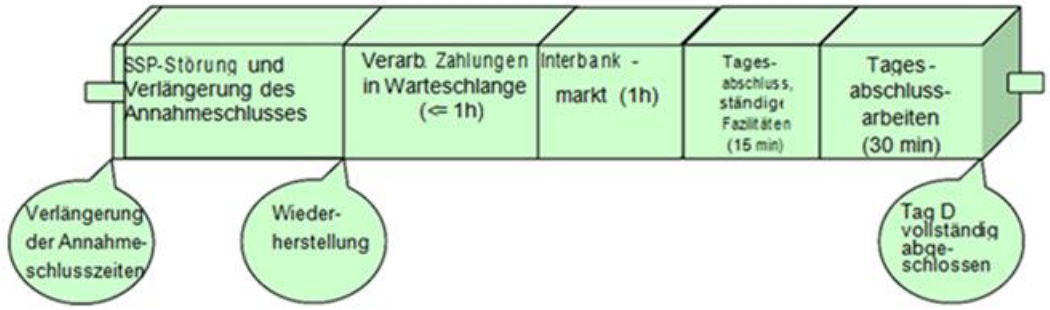


Abbildung 22: Ablauf am Tag der Störung

Die Wiederherstellung der Gemeinschaftsplattform bedeutet, dass wieder Nachrichten über sie verarbeitet werden können. Nach der Wiederherstellung werden – vorausgesetzt, der SSP-Ausfall trat während der Tagverarbeitungsphase auf – folgende Schritte eingeleitet:

- ☐ Abwicklung aller in der Warteschlange befindlichen Zahlungen (maximal eine Stunde); bei einem Plattform-Ausfall binnen 30 Minuten vor dem Annahmeschluss für Interbankzahlungen verkürzt sich dieser Zeitraum auf 30 Minuten. Die TARGET2-Nutzer können in dieser Phase auch neue Nachrichten senden.
- ☐ Ausgleich der Salden der Banken untereinander (eine Stunde); dieser Zeitraum verringert sich auf 30 Minuten, falls der Ausfall der Plattform innerhalb der 30 Minuten vor dem Annahmeschluss für Interbankzahlungen erfolgt.
- ☐ Nach dem Annahmeschluss für Interbankzahlungen findet die Tagesendeverarbeitung (45 Minuten bzw. am Ende der Erfüllungsperiode eine Stunde) statt, einschließlich der Inanspruchnahme der ständigen Fazilitäten.

Die Gesamtdauer dieser Schritte beträgt maximal 2 Stunden und 45 Minuten.

Schritte nach Verlängerung des Annahmeschlusses am Tag D

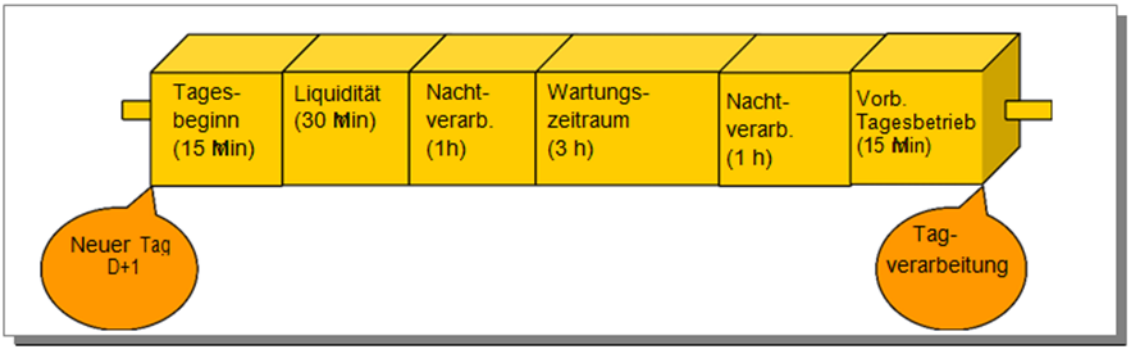


Abbildung 23: Ablauf am Tag nach der Störung

Außer den zuvor erwähnten obligatorischen Maßnahmen am Tag der Störung sind nach Abschluss des laufenden Geschäftstags mehrere obligatorische Schritte durchzuführen:

- Tagesbeginn (15 Minuten)
- Liquiditätsbereitstellung (30 Minuten)
- Nachtverarbeitung – NTS1 – einschließlich Liquiditätsbereitstellung an TIPS-Geldkonten und T2S-Geldkonten (mindestens 1 Stunde)
- Wartungsfenster (maximal 3 Stunden)
- Nachtverarbeitung – NTS2 (mindestens 1 Stunde)
- Vorbereitung der Tagverarbeitung (15 Minuten).

Diese Schritte summieren sich auf 6 Stunden und lassen sich weiter verkürzen durch die Reduzierung des Wartungsfensters und die Erleichterung der Nicht-Nachtverarbeitungsprozesse. Nachstehende Abbildung zeigt den Gesamtablauf:

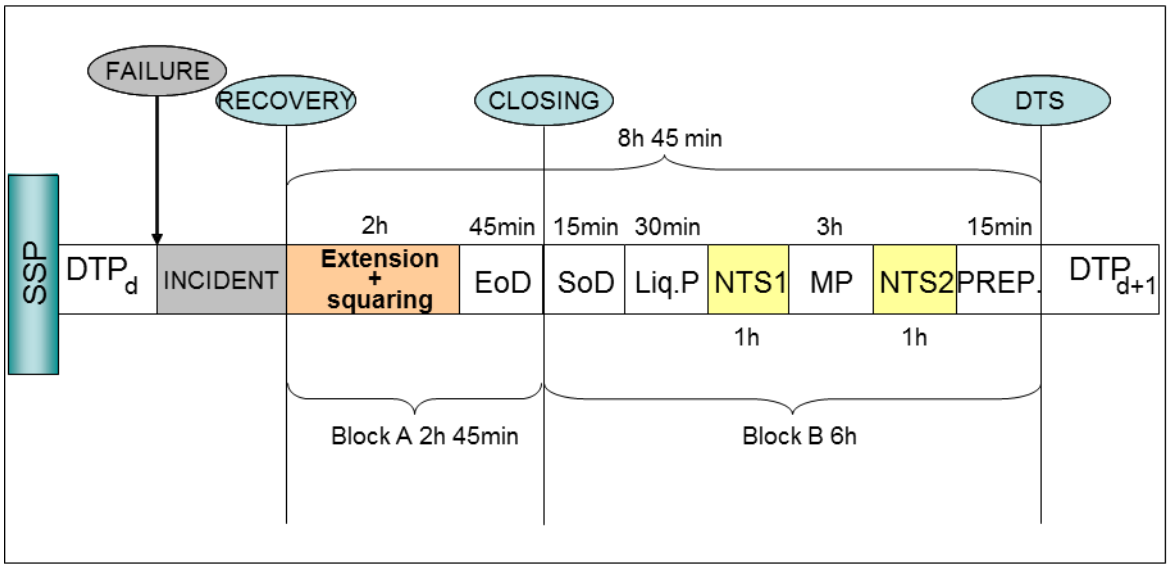


Abbildung 24: Überblick über den Ablauf im Fall einer Störung

Längerer Ausfall der Gemeinschaftsplattform

In Anbetracht der oben erwähnten Schritte wäre bei einem SSP-Ausfall während der Tagverarbeitungsphase und einer Wiederherstellung der Gemeinschaftsplattform bis 22.15 Uhr der Beginn der Tagverarbeitung um 7.00 Uhr noch möglich. Ein Ausfall, der nach 22.15 Uhr noch andauert (längerer Ausfall), könnte den Beginn der Tagverarbeitung um 7.00 Uhr verhindern, falls sich diese Phase (insbesondere das Wartungsfenster) nicht weiter verkürzen lässt.

Um Zeit einzusparen und die Tagverarbeitung möglichst bald nach 7.00 Uhr aufzunehmen, können die Schritte „Nachtverarbeitung 2“ und „Vorbereitung der Tagverarbeitung“ unmittelbar nach dem Wartungsfenster parallel erfolgen. Doch selbst durch dieses Vorgehen wäre ein Beginn der Tagverarbeitung um 7.00 Uhr womöglich noch nicht gesichert. Nebensysteme, die frühmorgens Liquidität in Euro benötigen, sollten für diesen Fall vorgesorgt haben.

6.5 Verfahren bei Störungen am Tagesende (18.00 Uhr – 18.45 Uhr)

Ein Ausfall der Gemeinschaftsplattform in dieser Phase würde die Tagesendeverarbeitung beeinträchtigen und somit möglicherweise auch die Inanspruchnahme der ständigen Fazilitäten, die Verfügbarkeit der endgültigen Kontosalden und den Beginn des neuen Geschäftstags. Die Ausführungen zur Verlängerung des Annahmeschlusses einschließlich der Auswirkungen auf den TIPS- und T2S-Zeitplan gelten hier in gleicher Weise wie oben beschrieben (siehe Abschnitt 6.4.3), wobei alle Annahmeschlusszeiten parallel zur ersten Verlängerung verschoben werden. Der nächste Schritt nach der Wiederherstellung der Gemeinschaftsplattform wäre die Fortsetzung der Tagesendeverarbeitung.

Geht die Hauptbuchdatei nicht innerhalb des normalen Zeitplans bei TARGET2 ein (d. h. 5 Minuten

nach TARGET2-Schließung), werden die Annahmeschlusszeiten am Tagesende aufgrund des zeitlich kritischen Charakters gemäß dem verkürzten Betriebszeitplan verschoben (siehe die nachfolgende Tabelle). Hält das Problem bis 18.40 Uhr an, kann die Tagesendeverarbeitung in TARGET2 ohne Berücksichtigung der TIPS-Kontosalden fortgesetzt werden; in diesem Fall müsste die entsprechende Zentralbank manuelle Anpassungen bei der möglichen automatisierten Inanspruchnahme der Spitzenrefinanzierungsfazilität und bei der Erfüllung der Mindestreserven vornehmen.

Normaler Betriebs-zeitplan (letzter Tag der Mindestreserve-Erfüllungsperiode)	Vefahren am Tages-ende/Tagesbeginn	Verkürzter Betriebs-zeitplan	**Verkürzter Betriebszeitplan** (letzter Tag der Mindestreserve-Erfüllungsperiode)
18.00 Uhr	Annahmeschluss für Interbankzahlungen	18.00 Uhr	18.00 Uhr
18.05 Uhr	Hauptbuchdatei von TIPS	**18.40 Uhr**	**18.40 Uhr**
18.15 Uhr/(18.30 Uhr)	Annahmeschluss für die Inanspruchnahme ständiger Faziliäten (Spitzenrefinanzierungs-fazilität und Einlage-fazilität)	18.50 Uhr	18.50 Uhr
18.40 Uhr/(18.55 Uhr)	Annahmeschluss für die Inanspruchnahme der Spitzenrefinanzierungs-fazilität (nur NZBen)	19.10 Uhr	19.10 Uhr
18.45 Uhr/(19.00 Uhr)	Tagesbeginn	19.15 Uhr	19.15 Uhr
19.00 Uhr/(19.15 Uhr)	Beginn der Liquiditäts-bereitstellung	19.30 Uhr	19.30 Uhr
19.30 Uhr/(19.45 Uhr)	Beginn der Nacht-verarbeitung (TARGET2)	19.50 Uhr	19.50 Uhr
20.00 Uhr	Beginn der Nacht-verarbeitung (T2S)	20.00 Uhr	20.00 Uhr

Tabelle 10: Verkürzter Betriebszeitplan bei Problemen mit der Hauptbuchdatei von TIPS

7 Störungen im Zusammenhang mit TIPS

Aufgrund der Anwendungsredundanz und der Fähigkeit zur Selbstregenerierung bietet TIPS eine hohe Ausfallsicherheit. Das Betriebsmodell von TIPS basiert auf dem Ansatz „eine Region, zwei Standorte".

Die TIPS-Infrastruktur besteht aus einem Cluster von Verarbeitungsknoten, die verschiedene Rollen übernehmen. Eine Untergruppe der Knotenpunkte ist für die Abwicklungsaktivitäten zuständig und kann als mehrere parallel laufende Instanzen des Abwicklungssystems betrachtet werden. Zu jedem Zeitpunkt übernimmt nur eine dieser Instanzen die Rolle des „Master-Knotens" und sendet ausgehende Nachrichten von TIPS. Die übrigen Instanzen sind „Slave-Knoten". Bei Bedarf kann jeder „Slave-Knoten" zu einem bestimmten Zeitpunkt die Aufgabe und Rolle des „Master-Knoten" übernehmen. Stehen einige lokale Knoten des Anwendungsclusters oder ein ganzer Standort nicht zur Verfügung, passt sich TIPS soweit möglich an, um den Betriebsablauf aufrechterhalten zu können **(Fähigkeit zur Selbstregenerierung)**.

Die Fähigkeit zur Selbstregenerierung bezieht sich auf die Betriebsdatenbank von TIPS. Der Ansatz für die Informationsdatenbank ist jedoch ein anderer. Hier werden durch zwei Kopien der vollständigen Informationsdatenbank die beiden Standorte zu jedem Zeitpunkt auf dem gleichen Stand gehalten. Eine aktive Kopie wird an einem Standort gespeichert. Von der gesamten TIPS-Anwendung kann hierauf schreibend zugegriffen werden. Außerdem wird diese Kopie fortlaufend mit Daten aus der Betriebsdatenbank aktualisiert. Die zweite Kopie wird an dem anderen Standort gespeichert. Hierauf kann nur schreibgeschützt zugegriffen werden.

Transaktionsintegrität und Datenpersistenz werden durch eine spezielle **Journaling-Komponente** sichergestellt, in der alle wesentlichen Informationen gespeichert sind. Der Status von TIPS lässt sich anhand der eingehenden Daten bestimmen (anders als in TARGET2, wo Optimierungsmechanismen und manuelle Änderungen an einer Warteschlange zu mehreren unterschiedlichen Ergebnissen auf Basis der gleichen eingegangenen Daten führen können). Daher kann die Journaling-Komponente jederzeit zur Wiederherstellung des aktuellen Status von TIPS verwendet werden.

Bei einer Standort-Ausfallsicherung bleibt die Betriebsdatenbank aufgrund der Fähigkeit zur Selbstregenerierung vollständig aktiv. Aus den Knoten des Standorts, auf den TIPS verlagert wird, wird der neue „Master-Knoten" ausgewählt. Steht bei der Informationsdatenbank die aktive Kopie nicht zur Verfügung, kann der Wechsel der zweiten Kopie von der passiven in die aktive Rolle manuell über den TIPS-Betreiber erfolgen. Daher kann die Standort-Ausfallsicherung der Informationsdatenbank nur während der üblichen Geschäftszeiten gewährleistet werden.

8 Störungen auf der T2S-Ebene

8.1 Auswirkungen auf TARGET2

Je nach Zeitpunkt des Auftretens kann eine T2S-Störung die Liquidität der Payment Bank, die Bereitstellung von Sicherheiten und/oder die Rückerstattung von Innertageskrediten (einschließlich der Selbstbesicherung) beeinträchtigen, wie nachfolgend aufgezeigt wird. So ist es möglich, dass ein technisches Versagen von T2S den Banken über den gesamten Abwicklungstag Schwierigkeiten bei der Bereitstellung neuer Sicherheiten zur Erhöhung ihrer Kreditlinien verursacht.

Phase des Geschäftstags	Auswirkung einer T2S-Störung
Tagesbeginn 18.45 Uhr – 20.00 Uhr	Bei für 20.00 Uhr geplanten T2S-Daueraufträgen zur Liquiditätsübertragung könnte eine erneute Versendung erforderlich werden.
Nachtverarbeitung 20.00 Uhr – 3.00 Uhr	Die Liquidität der T2S-Geldkonten würde auf der T2S-Plattform verbleiben. Da keine Contingency-Abwicklung vorgesehen ist, um die Liquidität nach TARGET2 zurückzutransferieren, könnten (sehr) kritische Zahlungen, die (früh) in der TARGET2-Tagverarbeitung abzuwickeln sind (CLS, EURO1 Bridge, zentrale Kontrahenten), beeinträchtigt werden.
Wartungsfenster 3.00 Uhr – 5.00 Uhr	Keine Auswirkungen auf TARGET2
Echtzeitverarbeitung 5.00 Uhr – 18.00 Uhr	Eine verzögerte automatisierte Rückerstattung der Selbstbesicherung (16.30 Uhr) könnte zu Verzögerungen in TARGET2 – bis der Innertageskredit in T2S zurückerstattet werden kann – führen. Womöglich wäre die Frist für die Rückerstattung von Innertageskrediten durch angeschlossene Nicht-Eurosystem-NZBen zu verlängern. Liquidität könnte möglicherweise nicht wie geplant auf TARGET2 transferiert bzw. die geldpolitischen Geschäfte nicht an TARGET2 weitergeleitet werden, was sich auf die Liquidität auswirken und eine Verzögerung in TARGET2[78] erfordern könnte.

78 Aufgrund einer technischen Störung in T2S könnten in Ausnahmefällen Mittel, die sich bei Tagesabschluss auf den T2S-Geldkonten befinden, über Nacht in T2S verbleiben, ohne dass es zu Verzögerungen in TARGET2 kommt. In solchen Fällen wird der verbliebene Saldo/werden die verbliebenen Salden auf dem T2S-Geldkonto/den T2S-Geldkonten bei der Berechnung der Mindestreserve berücksichtigt. Außerdem könnte ein Teilnehmer, der am Ende des Tages auf seinem PM-Konto einen Sollsaldo hätte, welcher durch den Saldo des T2S-Geldkontos gedeckt würde (wodurch der Teilnehmer gezwungen wäre, die Spitzenrefinanzierungsfazilität in Anspruch zu nehmen), gemäß der TARGET2-Ausgleichsregelung („Compensation Scheme“) Ausgleichsforderungen geltend machen.

	Auswirkungen auf bilaterale besicherte Geldhandelsgeschäfte (Bilaterally Agreed Treasury Management – BATM) mit Folgen für den Geldmarkt wären denkbar.
Tagesende 18.00 Uhr – 18.45 Uhr	Keine direkten Auswirkungen auf TARGET2

Tabelle 11: Auswirkungen einer T2S-Störung auf TARGET2

Angesichts der in vorstehender Tabelle dargestellten Abhängigkeiten bei einer Störung der T2S-Plattform ist der T2S-Koordinator verpflichtet, den TARGET2-Koordinator so früh wie möglich zu informieren.

Grundsätzlich sollten TARGET2 und T2S für die Wertpapierverrechnung in Euro immer am gleichen Valutatag in Betrieb sein, d. h., insofern TARGET2 am Tag D noch für die Geldverrechnung in Euro geöffnet ist, sollte T2S für die Wertpapierverrechnung in Euro am Tag D+1 nicht öffnen und umgekehrt. Somit könnte im Falle einer verzögerten T2S-Schließung eine verzögerte TARGET2-Schließung oder ein verzögerter Beginn am nächsten Abwicklungstag ins Auge gefasst werden. Wenn allerdings die T2S-Geldkonten einen Nullsaldo aufweisen, die Selbstbesicherung zurückerstattet und keine Wiederherstellungsaktivitäten nach dem Neustart im Anschluss an einen Katastrophenfall erforderlich sind, könnte die Notwendigkeit einer verzögerten TARGET2-Schließung womöglich entfallen.

8.2 Situation einer T2S-Ausfallsicherung

Bei einer Störung der T2S-Plattform, die eine Ausfallsicherung auf einen anderen Standort oder eine andere Region auslöst, muss auf die Wiederherstellung der Plattform gewartet und gegebenenfalls die Schlusszeit bzw. die betreffende T2S-Phase verschoben werden (daher könnte je nach Tageszeit auch ein verzögerter TARGET2-Schluss erforderlich sein).

Die Zentralbanken sollten die Teilnehmer so früh wie möglich über die Lage informieren und empfehlen, dass keine neuen Nachrichten zur Belastung von/Gutschrift auf T2S-Geldkonten an die T2S-Plattform gesendet werden sollten (über die Direktverbindung zu T2S oder über die TARGET2-Kern- und/oder -Zusatzleistungen für T2S). Regelmäßige Lageaktualisierungen erfolgen über die verfügbaren Kommunikationswege (wie in Abschnitt 2.5.1 beschrieben).

Bei einer interregionalen Ausfallsicherung (von Region 1 auf Region 2) werden die Zentralbanken, nachdem die T2S-Plattform in Region 2 wiederhergestellt ist, die Wiederherstellung und Synchronisierung der Euro-Zwischenkonten mit Blick auf die Salden und den Umsatz gewährleisten müssen – was aber lediglich im unwahrscheinlichen Falle eines Neustarts nach einem Katastrophenfall mit Datenverlust erforderlich ist. Dabei werden die fehlenden Liquiditätsübertragungen ermittelt und die Teilnehmer von der entsprechenden Zentralbank über die geplanten Maßnahmen und die betroffene

Liquiditätsübertragung informiert.

Mit Blick auf die **Liquiditätsübertragungen von PM-Konten auf T2S-Geldkonten** könnten die folgenden Maßnahmen ergriffen werden:

a) Wurden die Liquiditätsübertragungen auf die Gemeinschaftsplattform, aber noch nicht auf die T2S-Plattform gebucht (d. h., es wurde keine camt.025-Quittung aus T2S empfangen) und haben die an T2S gesendeten Nachrichten noch den Status „provided“ oder „acknowledged“, wird der TARGET Services Coordination Desk (in der Funktion als T2S-Zwischenkontoinhaber) die Nachrichten über ICM (RTGS-Bildschirm > Zahlungen und Nachrichten (Payments and messages) > Nachricht wählen (Select messages) > Mögliche Nachrichten für erneutes Senden (Possible Messages for Repeat Sending)) erneut übermitteln.

b) Wurden die Liquiditätsübertragungen auf der Gemeinschaftsplattform und auch auf der T2S-Plattform gebucht (d. h., eine camt.025-Quittung aus T2S wurde empfangen), ist der Geschäftsfall aus der SSP-Perspektive abgeschlossen, und somit können Nachrichten über das ICM nicht erneut gesendet werden. Daher erfolgt technisch eine erneute Übersendung (d. h., die Nachrichten werden von der Middleware nochmals gesendet). Bei einer hohen Anzahl von Liquiditätsübertragungen könnte die Entscheidung getroffen werden, alle in den letzten zehn Minuten vor der Störung verarbeiteten Liquiditätsübertragungen erneut zu senden (die Doppelinput-Kontrolle auf der T2S-Seite verhindert, dass in Region 2 zuvor bereits verarbeitete Liquiditätsübertragungen in T2S ein zweites Mal verarbeitet werden).

In diesem Fall sollten T2S-Geldkontoinhaber, die den Nachrichtenerhalt mit Blick auf T2S-Gutschriften und/oder dem Erreichen einer Obergrenze abonniert haben, die Meldungen im Zusammenhang mit der zweiten Buchung (auf Region 2) nicht beachten.

Was die Liquiditätsübertragung von T2S-Geldkonten auf PM-Konten betrifft, so wird die für den begünstigten PM-Kontoinhaber zuständige Zentralbank das PM-Konto belasten und das Guthaben nach Autorisierung durch den PM-Kontoinhaber dem T2S-Zwischenkonto gutschreiben. In diesem Falle sollten – wenn sich der T2S-Geldkontoinhaber für Benachrichtigungen über Gutschriften und/oder Untergrenzen entschieden hat – die Meldungen im Zusammenhang mit der ersten (in Region 1 vor dem Katastrophenfall erfolgten) Liquiditätsübertragung ignoriert werden. Nach der Wiederherstellung könnte der T2S-Geldkontoinhaber die Liquiditätsübertragung an das PM-Konto erneut veranlassen.

9 Andere Ausfälle

Dieser Abschnitt behandelt Störungen auf der Ebene der Zentralbanken, der Nebensysteme und der Bankenebene (einschließlich des Falls einer unkontrollierten Nachrichtenflut) sowie auf der SWIFT-Ebene oder Ebene der TIPS-Netzwerkdienstleister. Während ein Ausfall der Gemeinschaftsplattform (SSP) alle Zentralbanken gleichermaßen betrifft und ein einheitliches Verfahren erforderlich macht, liegt die Vorgehensweise bei den in diesem Abschnitt beschriebenen Ausfällen weitgehend in der Verantwortung der jeweiligen Zentralbank, des betroffenen Nebensystems oder der jeweiligen Bank.

Im Allgemeinen ist das genaue Verfahren, auf das sich die Nutzer und ihre jeweilige Zentralbank geeinigt haben, auf nationaler Ebene festgelegt.

9.1 Störungen auf der Zentralbankebene

Im Allgemeinen werden Zahlungen direkt in der SSP-, der TIPS- und der T2S-Plattform abgewickelt. Ein teilweiser oder kompletter Ausfall einer Zentralbank führt demnach nicht dazu, dass die gesamte Bankengemeinschaft eines Landes den Zugriff auf TARGET2, TIPS oder T2S verliert. Allerdings kommen jeder Zentralbank spezielle Aufgaben und Pflichten innerhalb von TARGET2 zu. Wenngleich die Auswirkungen eines Zentralbank-Ausfalls in TARGET2, TIPS und/oder T2S beschränkt sein dürften, müssen für jede Störung adäquate Maßnahmen zur Verfügung stehen, damit die Bankengemeinschaft ordnungsgemäß bedient und das Risiko vermieden werden kann, dass ein Zentralbankproblem anderweitig überspringt.

Grundsätzlich wird jedes Problem, das in einer Zentralbank/einem PHA besteht und sich auf die Gemeinschaftsplattform und/oder die TIPS-Plattform und/oder die T2S-Plattform oder auf die Bankengemeinschaft auswirken könnte, so zeitnah wie möglich innerhalb der Zentralbanken besprochen. Entsprechend den jeweiligen nationalen Bestimmungen und Verfahren kann ein National Service Desk die Banken direkt über Probleme auf nationaler Ebene informieren.

9.1.1 Ausfall einer Zentralbank

Grundsätzlich ist das Übergreifen eines Problems zu vermeiden, indem die Auswirkungen so gering wie möglich gehalten werden. Dies bedeutet, dass jede Zentralbank zunächst auf ihre eigenen Contingency-Verfahren zurückgreift. Sollte dies nicht möglich oder nicht effizient sein, kann die Zentralbank Hilfe vom SSP Service Desk, dem TIPS Service Desk oder dem T2S Service Desk in Anspruch nehmen.

Ansprechpartner für die Nutzer ist der jeweilige National Service Desk. Ist dieser nicht verfügbar, sollten die Nutzer nach den nationalen Kommunikationsverfahren für Krisenfälle verfahren.

Die Auswirkungen einer Störung auf Zentralbankebene hängen von der Phase des Geschäftstags ab, wie

nachfolgend gezeigt wird:

Phase des Geschäftstags	Auswirkung / Verfahren bei Störungen
Tagesbeginn 18.45 Uhr – 19:00 Uhr	Für alle Störungen, die in diesem Zeitraum auftreten könnten, hat die jeweilige Zentralbank angemessene Back-up-Maßnahmen vorbereitet.
Nachtverarbeitung 19.00 Uhr – 7.00 Uhr	Nach der Liquiditätsbereitstellung haben etwaige Probleme auf Zentralbankebene keinen Einfluss auf den SSP-, TIPS- oder T2S-Betrieb.
Betriebsfenster 6.45 Uhr – 7.00 Uhr	Das Eurosystem nutzt das Betriebsfenster zur Vorbereitung der Tagverarbeitung. Bei Störungen gelten die Verfahren zur Störungsbehebung während der Tagverarbeitung.
Tagverarbeitung 7.00 Uhr – 18.00 Uhr	Störungen während der Tagverarbeitung könnten sich auf die Aktualisierung von Kreditlinien/Repogeschäften und auf die Ausführung der zentralbankbezogenen Geschäfte (geldpolitische Transaktionen, Bareinlagen und Abhebungen etc.) auswirken. Für all diese Fälle hat die jeweilige Zentralbank angemessene Back-up-Maßnahmen vorbereitet.
Tagesende 18.00 Uhr – 18.45 Uhr	Störungen während der Tagesendeverarbeitung wirken sich in der Regel nicht auf die Gemeinschaftsplattform, TIPS, T2S oder auf die Bankengemeinschaft aus.

Tabelle 12: Auswirkungen eines Zentralbankausfalls

9.1.2 Ausfall eines proprietären Heimatkontos (PHA)

Neben den oben beschriebenen Problemen, die durch den Ausfall einer Zentralbank entstehen können, kann der Ausfall eines PHA zu folgenden Problemen führen:

1) Liquiditätsversorgung zu Beginn des Geschäftstags ist nicht möglich
2) Liquiditätsübertragungen auf Innertagesbasis zwischen dem PHA und dem Zahlungsmodul (PM) sind nicht möglich
3) Mindestreservehaltung und die Inanspruchnahme der ständigen Fazilitäten sind nicht möglich
4) die Umbuchung von Sicherheiten (Relocation of collateral) könnte (falls die Zentralbank-Selbstbesicherung nicht rechtzeitig zurückerstattet wurde) nicht möglich sein.

Andere Ausfälle

Es wird darauf hingewiesen, dass auf PHA-Ebene festgestellte Probleme gänzlich der nationalen Verantwortung obliegen und von der jeweiligen Zentralbank einzeln behoben werden. Es ist äußerst wichtig, dass die Zentralbank sämtliche Vorkehrungen und Maßnahmen trifft, um die Auswirkungen eines PHA-Problems auf die Zahlungsabwicklung in der SSP möglichst gering zu halten.

Die Auswirkungen eines PHA-Ausfalls lassen sich wie folgt darstellen:

Phase des Geschäftstags	Auswirkung
Tagesbeginn und Liquiditätsbereitstellung 18.45 Uhr – 19.30 Uhr	Zu Beginn des Geschäftstags auftretende Störungen verhindern die automatische Übertragung von Liquidität von einem PHA auf ein PM-Konto. - Sind keine PHA-Daten verfügbar, ist die Ausführung von Transaktionen nicht möglich. Möglicherweise können Transaktionen (z. B. Daueraufträge) auf der Grundlage der Abschlusssalden der PM-Konten der betreffenden Teilnehmer abgewickelt werden oder wenn gegen Überlassung neuer Sicherheiten Liquidität auf dem PHA bereitgestellt wird. - Besondere Aufmerksamkeit gilt jenen Nutzern, die an der Nachtverarbeitung teilnehmen. Für diese muss die Liquidität vor 19.30 Uhr übertragen werden. Anderenfalls können die Krisenmanager beschließen, die folgende Phase zu verschieben, d. h. den Beginn der Nachtverarbeitung zu verzögern. - Daraus könnten sich Folgewirkungen für die Liquiditätsbereitstellung an die T2S-Geldkonten ergeben. Es liegt im Ermessen des National Service Desk, ob der nationalen Teilnehmergemeinschaft PHA-Probleme mitgeteilt werden. Im Falle von Auswirkungen auf TARGET2 werden Informationen auch über das T2 IS und das ICM kommuniziert.
Nachtverarbeitung 19.30 – 7.00 Uhr	Nach der Liquiditätsbereitstellung an die PM-Konten haben etwaige Probleme auf Zentralbankebene keinen Einfluss auf den Betrieb der SSP.
Betriebsfenster 6.45 Uhr – 7.00 Uhr	Das Eurosystem nutzt das Betriebsfenster zur Vorbereitung der Tagverarbeitung. Bei Störungen gelten die Verfahren zur Störungsbehebung während der Tagverarbeitung.

Tagverarbeitung 7.00 Uhr – 18.00 Uhr	Störungen während der Tagverarbeitung bedeuten, dass das PHA keine Transaktionen/Geschäfte ausführen kann. Daher sind z. B. die automatische Aktualisierung von Kreditlinien und Liquiditätsübertragungen während des Tages zwischen dem PHA und dem Zahlungsmodul (PM) dann nicht möglich. Überdies könnten sich Auswirkungen auf die Umbuchung von Sicherheiten (Relocation of collateral) zeigen (falls die Zentralbank-Selbstbesicherung nicht rechtzeitig zurückerstattet wurde). **PHA-Daten noch verfügbar**: Sind trotz einer PHA-Störung die Daten noch verfügbar, kann die Zentralbank geeignete Maßnahmen ergreifen, um die betreffenden Transaktionen durchzuführen. **PHA-Daten nicht verfügbar**: Sind keine PHA-Daten verfügbar, ist die Ausführung von Transaktionen nicht möglich. **Verlängerung des Annahmeschlusses**: Bei einem PHA-Ausfall gewähren die Krisenmanager keine Verlängerung des Annahmeschlusses für TARGET2.
Tagesende 18.00 Uhr – 18.45 Uhr	Am Tagesende auftretende PHA-Probleme können sich auf die Rückübertragung von Guthaben und die Liquiditätsüberträge zu Beginn des nächsten Geschäftstags auswirken. Den nationalen Zentralbanken stehen angemessene nationale Verfahren zur Verfügung, um auf solche Szenarien zu reagieren.

Tabelle 13: Auswirkungen eines PHA-Ausfalls

9.2 Betriebs- oder technische Störungen auf Teilnehmerebene[79]

Tritt beim Inhaber eines PM-Kontos oder TIPS- oder T2S-Geldkontos ein Problem auf, infolgedessen er keine Zahlungen abwickeln und/oder keine Liquiditätsübertragungen auf/von TIPS-/T2S-Geldkonten in TARGET2 vornehmen kann,[80] dann sollte er seine Zentralbank informieren und mit ihr in regelmäßigem Kontakt bleiben. Er sollte zudem versuchen, das Problem so weit wie möglich mit eigenen Mitteln zu beheben.

79 Finanzielle Ausfälle werden in den Abschnitten 3.6 und 3.7 behandelt.

80 Einschließlich eines Problems mit der SWIFT-Verbindung zur SSP und/oder mit der direkten Verbindung zur T2S-Plattform über einen der lizenzierten Anbieter von Mehrwertnetzwerkdiensten.

Hierzu kann der T2S-Geldkontoinhaber folgende Möglichkeiten nutzen:

- Liquiditätsübertragungen von T2S-Geldkonten zu PM-Konten über die T2S-Schnittstelle, wenn sich der PM-Hauptkontoinhaber für die TARGET2-Zusatzleistungen entschieden hat
- die T2S GUI für T2S-Geldkontoinhaber, die normalerweise A2A-Funktionen verwenden.

Hierzu kann der TIPS-Geldkontoinhaber folgende Möglichkeiten nutzen:

- Liquiditätsübertragungen von TIPS-Geldkonten zu PM-Konten über die TIPS-Schnittstelle
- die TIPS GUI für TIPS-Geldkontoinhaber, die normalerweise A2A-Funktionen verwenden.

Hierzu kann der PM-Kontoinhaber folgende Möglichkeiten nutzen:

- interne Contingency-Lösungen
- über den normalen ICM-Zugang die Funktionalität der Ersatzzahlungen, welche a) die Initiierung von Zahlungen auf das CLS-Konto, das EURO1-Sicherheitenkonto oder das EURO1-Deckungskonto ermöglichen (Contingency-Zahlungen) und b) die Initiierung von Zahlungen zur Umverteilung von Liquidität (Ersatzzahlungen zur Umverteilung von Liquidität[81])
- Liquiditätsübertragungen vom PM-Konto auf das TIPS-Geldkonto oder das T2S-Geldkonto über normalen ICM-Zugang (falls der PM-Kontoinhaber normalerweise die A2A-Funktionen nutzt)
- dieselben Funktionalitäten über eine Stand-alone-Verbindung, wenn die normale ICM-Verbindung nicht mehr verfügbar ist.

Sind die Mittel eines Teilnehmers erschöpft, oder können sie nicht effizient eingesetzt werden, kann der Teilnehmer auf den National Service Desk zurückgreifen, der in solchen Situationen eine begrenzte Anzahl von Zahlungen im Auftrag des entsprechenden Teilnehmers durchführen kann. Die genauen Contingency-Kommunikationsverfahren sind bilateral zwischen dem Teilnehmer und seiner Zentralbank festgelegt.

Der National Service Desk benachrichtigt die anderen Zentralbanken über die technischen Probleme eines Teilnehmers, sofern sich diese auf die Abwicklung von Nebensystemen auswirken oder systemische Risiken, vor allem mit möglichen grenzüberschreitenden Auswirkungen, hervorrufen könnten. Die Benachrichtigung der Bankengemeinschaft wird zwischen allen Zentralbanken koordiniert.

81 Ersatzzahlungen zur Umverteilung von Liquidität dienen ausschließlich der Umverteilung von überschüssiger Liquidität. Sie sollen vermeiden, dass die Liquidität auf dem PM-Konto des Teilnehmers verbleiben muss, das von einem technischen Ausfall betroffen ist. Sie sind von den zugrunde liegenden kommerziellen Zahlungen vollständig getrennt. Daher können die Kreditinstitute, an die Liquidität umverteilt wird, andere Parteien sein, als die Teilnehmer, für die die zugrunde liegenden Zahlungen bestimmt sind. Außerdem müssen die Institute, auf die Liquidität umgelenkt wird, keine direkten TARGET2-Teilnehmer sein, sofern die Mittel über TARGET2 transferiert werden.

Der Systemausfall eines einzelnen Teilnehmers sollte in keinem Fall zu einer Verschiebung des Annahmeschlusses führen.

Kasten 6 Back-up-Contingency-Zahlungen

Ersatzzahlungen über das ICM (sowohl im U2A- als auch im A2A-Modus) dürfen nur für die Verarbeitung von Zahlungen auf das CLS-Konto, das EURO1-Sicherheitenkonto oder das EURO1-Deckungskonto (Back-up-Contingency-Zahlungen) und für Zahlungen zur Umverteilung von Liquidität (Ersatzzahlungen zur Umverteilung von Liquidität) verwendet werden.

Im Rahmen dieser Beschränkungen liegt die Durchführung von Ersatzzahlungen im freien Ermessen der Banken, die diese benötigen und die auch das volle Kreditrisiko tragen. Contingency-Zahlungen wie auch Ersatzzahlungen zur Umverteilung von Liquidität sind ihrem Wesen nach vollgültige Zahlungsaufträge. Dies bedeutet, dass diese oder eine ähnliche Zahlung nach Wiederaufnahme des Normalbetriebs nicht erneut gesendet werden müssen.

Wenn die Funktionalität der Ersatzzahlungen verwendet wird, sind folgende Aspekte zu berücksichtigen:

- Bevor ein PM-Teilnehmer die Funktion verwenden kann, muss er deren Aktivierung bei der zuständigen Zentralbank beantragen. Die Aktivierung erfolgt mit sofortiger Wirkung.
- Auf Anfrage eines PM-Teilnehmers, der die ICM-Funktionalität verwendet, kann die zuständige Zentralbank andere TARGET2-Nutzer über solche Zahlungen zur Liquiditätsumverteilung informieren.
- Hatte ein Teilnehmer technische Probleme und beabsichtigt, die verspäteten ursprünglichen Zahlungen am nächsten Geschäftstag mit dem Datum des Geschäftstags der technischen Störung (der ursprünglichen Valuta) zu senden, ist dies der zuständigen Zentralbank am Tag des technischen Systemausfalls, d. h. vor dem Tag, an dem die Einzelzahlungen übermittelt werden, mitzuteilen. Dieser Antrag auf Aufhebung der Valutaprüfung muss die zuständige Zentralbank mindestens 30 Minuten vor dem Annahmeschluss von TARGET2 erreichen. Die Zentralbank sorgt dafür, dass die Valutaprüfung für diesen Sender am folgenden Geschäftstag deaktiviert wird, sodass die ursprünglichen Einzelzahlungen mit der ursprünglichen Valuta verarbeitet werden können. Die Abwicklung in TARGET2 erfolgt immer an dem Geschäftstag, an dem die Zahlung übermittelt wird; weicht die Valuta hiervon ab, so müssen alle Zinsanpassungen außerhalb des TARGET2-Systems vorgenommen werden.

- Sofern die Aufhebung der Valutaprüfung noch einen weiteren Tag benötigt wird, muss dies am vorhergehenden Geschäftstag mindestens 30 Minuten vor Annahmeschluss beantragt werden.
- Sobald der beantragende Teilnehmer alle entsprechenden Transaktionen abgeschlossen hat, informiert er seine Zentralbank darüber, und diese aktiviert die Valutaprüfung wieder.
- Bei der Initiierung von Ersatzzahlungen ist nicht nur auf den Saldo des PM-Kontos zu achten, sondern auch auf mögliche Belastungen des PM-Kontos, die nicht vom betreffenden Teilnehmer veranlasst werden, wie z. B. Zahlungen zur Verrechnung von Nebensystemen.
- Empfänger von Ersatzzahlungen sollten beachten, dass der BIC des Senders solcher Zahlungen dem des PM entspricht (TRGTXEPMXXX) und dass der Zahlungspflichtige/Auftraggeber der Zahlung nur anhand des BIC in Feld 52 der FIN-Nachricht ermittelt werden kann.

Ersatzzahlungen zur Umverteilung von Liquidität sollten auf der Grundlage einer vorher getroffenen individuellen bilateralen Vereinbarung erfolgen. Dabei sind die in den Richtlinien der Europäischen Bankenvereinigung zum Liquiditätsmanagement (European Interbank Liquidity Management Guidelines) definierten Marktgepflogenheiten zu befolgen.

Sicherheitsrelevante Vorfälle

Die Teilnehmer sind verpflichtet, ihren National Service Desk über alle (cyber-)sicherheitsrelevanten Vorfälle in ihrer technischen Infrastruktur und, sofern dies angemessen erscheint, über (cyber-)sicherheitsrelevante Vorfälle in der technischen Infrastruktur von Drittanbietern zu unterrichten.

Tritt ein solcher Vorfall ein (wird beispielsweise eine betrügerische Handlung oder ein Cyberangriff festgestellt), so kann der Teilnehmer auch seinen National Service Desk um Unterstützung ersuchen. Diese Unterstützung kann dazu dienen, die Auswirkungen des Vorfalls zu begrenzen (etwa durch den Schutz der Gelder) oder eine weitere Ausbreitung zu verhindern. Zwar betrifft die Bereitstellung von Informationen durch die Teilnehmer und die Unterstützung durch die Zentralbanken in erster Linie TARGET2-Aktivitäten, doch sind die Teilnehmer sind gehalten, ihren National Service Desk auch über Vorfälle zu unterrichten, die nicht unmittelbar mit TARGET2 in Verbindung stehen.

9.3 Ausfall eines Nebensystems

Tritt bei einem Nebensystem ein Problem auf, sollte es bis zur Behebung so weit wie möglich auf eigene Contingency-Verfahren zurückgreifen. Hauptziel sollte sein, alle Nachrichten an die SSP über die normalen Kanäle zu verarbeiten, d. h. über die Nebensystemschnittstelle (Ancillary System Interface – ASI) oder gegebenenfalls über die Standard-Zahlungsschnittstelle. Dabei müssen sowohl die

Verwendung der Zahlungsschnittstelle als auch die von einer Zentralbank gebotene Unterstützung im Vorfeld zwischen dem Nebensystem und seiner Zentralbank abgesprochen und vereinbart werden.

- Das Nebensystem kann in eigenem Ermessen von alternativen Möglichkeiten wie Back-up-Standorten und Multi-Zugangsportalen zu Multi-Netzwerkpartnern Gebrauch machen. Ebenso ist die Nutzung der Standard-Zahlungsschnittstelle zur SSP möglich, um „reine" („clean") Zahlungen zu leisten.
- Bei Bedarf kann die jeweilige Zentralbank das Nebensystem unterstützen, z. B. indem sie XML-Dateien verarbeitet oder in dessen Auftrag „reine" („clean") Zahlungen leistet. Es hängt von der einzelnen Zentralbank ab, ob das „AS Contingency Tool" für das Nebensystem angeboten wird oder nicht.
- In besonderen Ausnahmefällen, in denen ein Risiko für das gesamte Eurosystem besteht, kann die jeweilige Zentralbank des Nebensystems eine Verlängerung des Annahmeschlusses für TARGET2 beantragen, damit das Nebensystem mehr Zeit hat, die Störung zu beheben oder ihre Auswirkungen zu minimieren. Die Krisenmanager entscheiden, ob der Annahmeschluss verlängert wird.

Jede Zentralbank entscheidet selbst, welchen Support-Level sie ihren Nebensystemen vor allem während der Nachtverarbeitung zur Verfügung stellen möchte. Solche Contingency-Vereinbarungen müssen stets im Vorfeld zwischen dem Nebensystem und seiner Zentralbank vereinbart werden. Treten während der Nachtverarbeitung Störungen auf, sollte das Nebensystem grundsätzlich seine Zentralbank informieren und mit ihr die Contingency-Verfahren und die nationalen Kommunikationsmittel abstimmen. Darüber hinaus hat das Nebensystem seine Verrechnungsteilnehmer separat über das geplante Abwicklungsverfahren zu informieren.

Ein Nebensystem sollte seinen National Service Desk von Ausfällen in Kenntnis setzen. Nach eigenem Ermessen gibt der National Service Desk das Problem an die Zentralbanken weiter, vor allem wenn grenzüberschreitende Auswirkungen möglich sind. Die Benachrichtigung der Bankengemeinschaft wird zwischen allen Zentralbanken koordiniert.

Ähnlich wie andere Teilnehmer sind auch Nebensysteme verpflichtet, ihren National Service Desk über (cyber-)sicherheitsrelevante Vorfälle in ihrer technischen Infrastruktur und, sofern dies angemessen erscheint, über (cyber-)sicherheitsrelevante Vorfälle in der technischen Infrastruktur von Drittanbietern zu unterrichten und können den National Service Desk um Unterstützung bitten (wie in Abschnitt 9.2 dargestellt). Diese allgemeine Regelung gilt auch für Vorfälle, die nicht den TARGET2-Geschäftsbetrieb betreffen, da dies die Ergreifung von Vorsorgemaßnahmen ermöglichen würde.

9.3.1 Nebensysteme, die die Nebensystemschnittstelle nutzen

Einzahlungen (von TARGET2 an das Nebensystem) könnten nach einer der folgenden Methoden abgewickelt werden:

- Die jeweilige Zentralbank sendet im Auftrag des Nebensystems mit dem „AS Contingency Tool" eine XML-Datei an die SSP,[82]
- das Nebensystem sendet einen MT 204, sofern es die Zahlungsschnittstelle verwenden kann, d. h. wenn seine SWIFTNet-Verbindung unterbrochen ist, seine SWIFTNet FIN-Verbindung aber noch funktioniert, oder die betreffende Zentralbank sendet im Auftrag des Nebensystems einen MT 204 (in diesem Fall müssen alle erforderlichen Genehmigungen erteilt worden sein),
- die Verrechnungsbank könnte gebeten werden, „reine" („clean") PM-Zahlungen zugunsten des Nebensystems zu leisten, oder
- die Zentralbank der Verrechnungsbank führt die Zahlungen („mandated payments"[83]) im Auftrag der Verrechnungsbank und auf Grundlage der vom Nebensystem gelieferten Informationen aus.

Auszahlungen (vom Nebensystem an TARGET2) könnten nach einer der folgenden Methoden abgewickelt werden:

- Die jeweilige Zentralbank sendet im Auftrag des Nebensystems mit dem „AS Contingency Tool" eine XML-Datei an die SSP oder
- das Nebensystem leistet „reine" („clean") Zahlungen mithilfe der Zahlungsschnittstelle.

Verarbeitet die Zentralbank keine XML-Dateien im Auftrag des Nebensystems unter Nutzung des „AS Contingency Tool", kommt der Reihenfolge der Abwicklung bei den Abwicklungsverfahren 4 und 5 besondere Bedeutung zu.

- Abwicklungsverfahren 4: Die Zentralbank überprüft in Abstimmung mit dem Nebensystem, dass alle Einzahlungen vor Beginn der Auszahlungsphase abgewickelt sind. Können nicht alle Einzahlungen abgewickelt werden, erfolgt die Rückabwicklung, indem die Zentralbank eine Rückbuchung vom Nebensystem-Konto zum Bankkonto veranlasst (sofern die Einzahlung abgewickelt wurde) oder die Zahlung storniert (sofern sie noch aussteht).
- Abwicklungsverfahren 5: Dieses verläuft wie das Abwicklungsverfahren 4, nur werden hierbei

82 In diesem Fall können Ein- und Auszahlungen wie auch bei der normalen Abwicklung via ASI gemeinsam gesendet werden, sofern die Abwicklungsverfahren 3, 4, 5 oder 6 Anwendung finden.

83 „Mandated payments" sind Zahlungen, die von einer nicht an der Transaktion beteiligten Stelle (im Regelfall einer NZB oder einem Nebensystem im Zusammenhang mit einer Nebensystemverrechnung) im Auftrag einer anderen Stelle initiiert werden. Beispielsweise sendet eine NZB eine Überweisung (mit einer bestimmten Nachrichtenstruktur) im Auftrag eines ausgefallenen direkten Teilnehmers (nur in Contingency-Situationen). „Mandated payments" auf technische Konten sind nicht möglich.

keine Zahlungen rückabgewickelt, da die Abwicklung nach dem „Alles oder nichts“-Prinzip erfolgt ist.

- Für Nebensysteme mit einem Garantiekonto-Verfahren findet Abwicklungsverfahren 4 Anwendung, mit der Ausnahme, dass die Zentralbank bei Bedarf und in Abstimmung mit dem Nebensystem das Garantiekonto belastet, statt eine Einzahlung vorzunehmen.[84]

Bei Abwicklungsverfahren 6 ist die Überwachung der Verrechnungsphasen entscheidend:

- Die jeweilige Zentralbank kann im Auftrag des Nebensystems unter Nutzung des „AS Contingency Tool“ Abwicklungsverfahren und Zyklen anstoßen;

  die betreffende Zentralbank kann im Auftrag des Nebensystems mit dem „AS Contingency Tool“ oder direkt mittels des ICM (Funktion „stop procedure/cycle“) Abwicklungsverfahren und Zyklen beenden.

Simulation des Empfangs einer technischen „XML notification message“

Ein Problem bei der Zustellung oder Verarbeitung einer technischen „XML notification message“[85] kann zu einer Blockierung des laufenden und folgender Abwicklungsprozesse im Nebensystem führen. Daher sollten die Nebensysteme unbedingt in der Lage sein, den Empfang solcher Nachrichten zu simulieren. Dies sollte (nach Prüfung im ICM) auf eigene Initiative des Nebensystems geschehen oder auf Basis einer auf sicherem Weg übermittelten Bestätigung des Abwicklungsergebnisses durch den National Service Desk (die Einzelheiten sind bilateral zu vereinbaren). Das Nebensystem kann sich letztlich in Abstimmung mit dem National Service Desk für die geeignetste Methode entscheiden, d. h. den Empfang simulieren oder den Nicht-Erhalt anderweitig lösen.

9.3.2 Nebensysteme, die die Zahlungsschnittstelle nutzen

Einzahlungen (von TARGET2 zum Nebensystem) werden zwar nach wie vor auf normalem Wege abgewickelt, doch die Zentralbank muss das Nebensystem unter Umständen über nationale Kommunikationswege von eingehenden Zahlungen in Kenntnis setzen.

Auszahlungen (vom Nebensystem zu TARGET2) werden nach einer der folgenden Methoden vom Nebensystem abgewickelt:

a) Das Nebensystem kann „reine“ („clean“) Zahlungen über die Zahlungsschnittstelle (sofern es noch Zugang dazu hat) oder mittels Ersatzzahlungen über das ICM leisten.

b) Die Zentralbank sendet eine Zahlung („mandated payment“), die dem Nebensystem belastet und

84 Falls das Nebensystem die Garantien in Anspruch nimmt, sind besondere Verfahren erforderlich.

85 Zum Beispiel: ASTransferNotice, ASInitiationStatus, ReceiptAS(1), ReturnAccountAS.

der Verrechnungsbank gutgeschrieben wird. Die Zentralbank muss das Nebensystem unter Umständen über nationale Kommunikationswege von den abgewickelten Zahlungen in Kenntnis setzen.

9.4 Technische Suspendierung

Eine technische Suspendierung schützt die Gemeinschaftsplattform, die TIPS-Plattform und/oder die T2S-Plattform vorübergehend vor umfangreichen, unkontrollierten Nachrichteneingängen (z. B. „denial of service messages“, i. d. R. außerhalb des SWIFTNet FIN-Bereichs). In solchen Situationen muss sofort reagiert werden, um eine Störung des reibungslosen Funktionierens der SSP und/oder der T2S-Plattform zu vermeiden. Es handelt sich hierbei um eine rein technische Maßnahme, die dann zum Einsatz kommt, wenn eine Zentralbank, eine Bank oder ein Nebensystem eine so ungewöhnlich hohe Zahl von Nachrichten an die SSP und/oder die T2S-Plattform sendet, dass deren einwandfreier Betrieb möglicherweise gefährdet ist.

Stellt das Eurosystem solch eine außergewöhnlich hohe und umfangreiche Nachrichtenflut fest, die das reibungslose Funktionieren der Gemeinschaftsplattform und/oder der TIPS-Plattform und/oder der T2S-Plattform gefährdet, kann es den Sender vorsichtshalber technisch suspendieren. Die Ursachen für das unbeabsichtigte Senden werden sofort im Gespräch mit dem Sender erörtert, und sobald diese geklärt sind, hebt das Eurosystem die technische Suspendierung auf. Je nach Situation könnten die Krisenmanager vorsorglich eine Verlängerung der Annahmeschlusszeit erwägen.

9.5 Ausfall von SWIFT

Bei einem SWIFT-Ausfall wird ein alternatives Contingency-Netzwerk zur Bereitstellung eines Zahlungskanals verwendet. Das Contingency-Netzwerk bewirkt bei einem lokalen Ausfall oder einem Gesamtausfall von SWIFT eine deutliche Erhöhung der Ausfallsicherheit von TARGET2 sowie der Stabilität des Gesamtsystems. Auch ohne SWIFT-Zugang können Zentralbanken über das Contingency-Netzwerk im Auftrag ihrer Kunden (sehr) kritische Ersatzzahlungen und Zahlungen zur Umverteilung von Liquidität sowie Nebensystemdateien senden und Liquiditätsübertragungen zwischen PM-Konten und T2S-Geldkonten darüber durchführen. Darüber hinaus sind sie in der Lage, die Konten ihrer Teilnehmer über das Contingency-Netzwerk zu überwachen (einschließlich der T2S-Geldkonten, die mit den PM-Hauptkonten verknüpft sind, deren Inhaber sich für die TARGET2-Zusatzleistungen für T2S entschieden haben). Das Contingency-Netzwerk ist jedoch kein vollständiger Ersatz für das SWIFT-Netzwerk, da es keine Verbindung zwischen den Nutzern und ihren NZBen bietet und sich auf vereinbarte nationale Kommunikationsmittel stützt.

Das tägliche Volumen der abwickelbaren Zahlungen beläuft sich auf rund 3 000, wobei 2 300 (sehr)

kritische Zahlungen und 700 einzelne Nebensystemtransaktionen verarbeitet werden. Dabei wird zwischen sehr kritischen Zahlungen, die unbedingt abgewickelt werden müssen, und kritischen Zahlungen, vor deren Abwicklung die Zustimmung der Krisenmanager einzuholen ist, unterschieden. In Abschnitt 6.4.2 wird das Konzept (sehr) kritischer TARGET2-Zahlungen dargelegt.

Das Contingency-Netzwerk lässt sich für ein Land, für mehrere Länder oder für alle an TARGET2 angebundenen Länder aktivieren. Für einen einzigen Teilnehmer erfolgt keine Aktivierung des Contingency-Netzwerks.

Mit der Aktivierung des Contingency-Netzwerks wird für alle Teilnehmer, die über die betroffenen Zentralbanken angebunden sind, automatisch die Funktionalität der Ersatzzahlungen freigeschaltet.

9.5.1 Verarbeitung von Zahlungen

Die TARGET2-Nutzer informieren ihre Zentralbank über die im Contingency-Modus abzuwickelnden Zahlungen. Die Zahlungsaufträge werden nach Maßgabe der zuvor auf lokaler Ebene vereinbarten Contingency-Kommunikationsverfahren an den National Service Desk gesendet.

Der National Service Desk verarbeitet mithilfe seines über das Contingency-Netzwerk bestehenden Zugriffs auf die ICM-Ersatzbildschirme die Zahlungsaufträge nach dem Vier-Augen-Prinzip. Die Abwicklung der Ersatzzahlungen wird überwacht. Die einreichenden Parteien erhalten vom National Service Desk eine Rückmeldung entsprechend den lokalen Contingency-Kommunikationsverfahren.

Dabei ist Folgendes zu berücksichtigen:

- Teilnehmer mit Zugang zum SWIFT-Netzwerk und Teilnehmer mit internetbasiertem Zugang können weiterhin Zahlungen senden, müssen jedoch ihre Aktivitäten so weit wie möglich auf das Senden (sehr) kritischer Zahlungen beschränken, damit auf der Empfängerseite kein zusätzlicher Arbeitsaufwand entsteht.
- Da die Transaktionsreferenznummer für Zahlungen, die über die Ersatz-Funktionalität abgewickelt werden, vom System erzeugt wird, kann keine Kontrolle zur Vermeidung von Doppeleinreichungen, die sich unmittelbar nach Wiederherstellung der Verbindung zum SWIFT-Netzwerk ergeben können, erfolgen. Teilnehmer, die die Verarbeitung von Ersatzzahlungen beantragen, sollten ihre Zahlungen nach Ende des SWIFT-Ausfalls einer genauen Prüfung unterziehen.
- Für Zahlungen, die über das Contingency-Netzwerk abgewickelt werden, wird das allgemeine Format für Ersatzzahlungen verwendet. Die Zahlungen werden im SWIFT-Format MT 202 über SWIFTNet FIN (ohne Y-Copy) an den Empfänger gesendet. In Feld 72 ist das Codewort /BUP/ einzutragen. Sender der Zahlung ist der gemeinsame BIC des PM, d. h. TRGTXEPMXXX. Wie

für alle anderen Ersatzzahlungen erhält der Kunde nach Wiederherstellung der Verbindung zum SWIFT-Netzwerk eine Belastungsanzeige (MT 900), sofern er dies beantragt hat.

- Liquiditätsübertragungen von PM-Konten auf TIPS-Geldkonten oder T2S-Geldkonten können über das Contingency-Netzwerk abgewickelt werden. Liquiditätsübertragungen von T2S-Geldkonten auf die PM-Hauptkonten können nur verarbeitet werden, wenn sich der Inhaber des PM-Hauptkontos für die TARGET2-Zusatzleistungen für T2S entschieden hat.
- Es ist gewährleistet, dass die über das Contingency-Netzwerk übertragenen Nachrichten nicht zurückgewiesen werden.

9.5.2 Verarbeitung von Dateien aus Nebensystemen

Nebensysteme, die keinen Zugang zur SSP herstellen können, müssen die XML-Nachrichtendateien erzeugen und sie über die auf nationaler Ebene vereinbarten Contingency-Mechanismen (privates Netzwerk, E-Mail, Fax u. a.) an die jeweilige Zentralbank weiterleiten. Dateien für alle sechs in TARGET2 vorgesehenen AS-Abwicklungsverfahren werden auch vom Contingency-Netzwerk unterstützt. Dabei ist zu beachten, dass das Tagesvolumen der aus Nebensystemdateien verarbeiteten Zahlungen auf 700 Transaktionen begrenzt ist. Darüber hinaus ist die Größe jeder Datei auf maximal 1 MB limitiert. Dateien, die diese Größe überschreiten, werden zurückgewiesen.

Über das Contingency-Netzwerk erhält die Zentralbank Zugang zum ICM und lädt die Datei im Auftrag des Nebensystems hoch.

Folgende Spezifikationen sind in diesem Zusammenhang von Bedeutung:

- Bei den Modellen 4 und 5 ist sowohl die Bestätigung als auch die Ablehnung der Verwendung des Garantiekonto-Verfahrens möglich.
- Bei Modell 6 kann über den ICM-Bildschirm neben der Beendigung eines Nebensystemzyklus auch das Eröffnen eines Zyklus oder Verfahrens erfolgen.
- Doppelte Dateien, die über verschiedene Netzwerke gesendet wurden, werden von der Gemeinschaftsplattform erkannt und zurückgewiesen, sofern ihr Betreff identisch ist und sie von derselben initiierenden Partei stammen.
- Bei Dateien, die über das ICM hochgeladen wurden, wird keine Benachrichtigung (ASTransferNotice, ReturnAccount, MT 900/MT 910) an den Nutzer gesendet. Die Zentralbank kann den Status der über das ICM gesendeten Dateien verifizieren und das betreffende Nebensystem informieren.

9.6 Ausfall des TIPS-Netzwerkdienstleisters

Beim Ausfall eines TIPS-Netzwerkdienstleisters steht kein alternatives Contingency-Netzwerk zur Verfügung.

Die Zentralbanken können im Auftrag des PM-Kontoinhabers oder des TIPS-Geldkontoinhabers bestimmte Liquiditätsübertragungen zwischen PM-Konten und TIPS-Geldkonten anweisen/verarbeiten.

Sie können auch die Salden der TIPS-Geldkonten, die mit in ihren Büchern geführten PM-Konten verknüpft sind, überwachen.

9.7 Ausfall der TIPS-Schnittstelle (TIPSI)

Können aufgrund eines TIPS-Schnittstellenproblems keine Liquiditätsübertragungen zwischen PM-Konten und TIPS-Geldkonten durchgeführt werden, ist es für eine Zentralbank nicht möglich, im Auftrag einer Payment Bank zu handeln, da interne Liquiditätsübertragungen zwischen TIPS-Geldkonten nicht erlaubt sind. Serviceinterne Liquiditätsübertragungen (zwischen TIPS-Geldkonten und TIPS ASTAs) können jedoch noch abgewickelt werden.

9.8 Störung der Liquiditätsübertragung von TARGET2 an T2S und/oder von T2S an TARGET2

Sollte die Liquiditätsübertragung von TARGET2 an T2S und/oder von T2S an TARGET2 nicht reibungslos funktionieren, so kann der Teilnehmer seinen National Service Desk um Unterstützung bitten. In einem solchen Fall kann der National Service Desk im Auftrag des Antragstellers eine begrenzte Anzahl von Liquiditätsübertragungen zwischen TARGET2 und T2S durchführen. Die genauen Kommunikationswege sind bilateral zwischen dem Teilnehmer und seiner Zentralbank festgelegt.

10 Test der Contingency- und Business-Continuity-Verfahren

10.1 Geltungsbereich

TARGET2 umfasst die Gemeinschaftsplattform (SSP), proprietäre Heimatkonten (PHAs) und andere Anwendungen der Zentralbanken sowie Nebensysteme (AS) und sonstige Einheiten, die eine Verbindung zur SSP und/oder der T2S-Plattform ermöglichen bzw. mit ihr arbeiten.
Bei TIPS gibt es (wie in Abschnitt 7 erklärt) aufgrund der Fähigkeit zur Selbstregenerierung der TIPS-Plattform keine spezifischen Contingency-Verfahren.

Die Zentralbanken unterliegen dem Geltungsbereich der vom EZB-Rat verabschiedeten „Information security policy for TARGET2“ und haben somit dafür zu sorgen, dass ihre Infrastrukturen sicher und zuverlässig funktionieren. Dazu gehört auch, dass sie für alle als kritisch eingestuften Geschäftsfunktionen über angemessene Contingency- und Business-Continuity-Verfahren verfügen, die in regelmäßigen Abständen getestet werden.

Ein SWIFT-Ausfall ist nicht Bestandteil der Tests, da der EZB-Rat das Restrisiko eines solchen Ausfalls als hinnehmbar einstuft.

10.2 Ziel der Tests

Die regelmäßigen Tests der Contingency- und der Business-Continuity-Verfahren sollen gewährleisten, dass die bestehenden Verfahren und die vorhandene Infrastruktur immer noch ausreichen und geeignet sind, um potenzielle Notfallszenarien zu bewältigen. Überdies bieten die Tests den involvierten Teams die Möglichkeit, die Tätigkeiten zu trainieren, die in einem Notfallszenario durchgeführt werden müssten.

Anmerkung: Hierbei ist zwischen den Begriffen „Erprobung“ („trialling“) und „Test“ („testing“) zu unterscheiden. Eine Erprobung findet in der Produktionsumgebung statt, während Tests in einer Testumgebung durchgeführt werden.

10.3 Aufgaben und Zuständigkeiten

- Der **SSP Service Desk und der TIPS Service Desk** beteiligen sich an der Organisation und Planung der Business-Continuity-Tests, führen alle den 3ZB/4ZB zugewiesenen Aufgaben aus (sie treffen z. B. alle vor den Tests/den Erprobungen erforderlichen Vorbereitungen), überwachen die Durchführung der Tests/Erprobungen aktiv und unterstützen die Zentralbanken in

TARGET2/TIPS bei ihren Aktivitäten im Rahmen der Tests/Erprobungen.

- Die National Service Desks unterstützen bei der Organisation und Planung der Contingency- und Business-Continuity-Tests und führen alle ihnen zugewiesenen Aufgaben während der Durchführung der Tests/Erprobungen aus. Sie sollen die Tests/Erprobungen verfolgen, in die ihre nationalen Teilnehmer involviert sind (z. B. Tests mit kritischen Teilnehmern), und ihre Nutzergruppe entsprechend unterstützen.

Der TARGET Services Coordination Desk beteiligt sich bei Bedarf auf zwischenstaatlicher Ebene an der Organisation.

10.4 Testumgebung

Damit die Tests effektiv sind, sollten sie entweder in der Produktionsumgebung (d. h. als Erprobung) oder – sofern dies aufgrund des zusätzlichen operationellen Risikos als nicht sinnvoll erachtet wird – in einer möglichst ähnlichen Testumgebung durchgeführt werden.

Bei den Nutzertests wird davon ausgegangen, dass dieTestumgebungen SSP-CUST/TIPS CERT und die UTEST der T2S-Plattform der Produktionsumgebung (PROD) so weit wie möglich entsprechen.

Wenn neue Releases getestet werden, kann es mitunter vorkommen, dass die Testumgebungen CUST/CERT nicht auf derselben Version beruhen wie die SSP-/TIPS-Produktionsumgebung. Was die PHA-Umgebungen anbelangt, so muss jede Zentralbank, die ein proprietäres Heimatkonto anbietet, eine Testumgebung bereitstellen, die der Produktionsumgebung möglichst ähnlich ist.

Weitere Einzelheiten zu den Öffnungstagen, dem Geschäftstagesablauf und dem von den 3ZB/4ZB geleisteten Support für TARGET2/TIPS finden sich auf der Website der EZB.

10.5 Überblick über die Tests der Contingency- und Business-Continuity-Verfahren

In diesem Abschnitt werden sämtliche Anforderungen für Contingency- und Business-Continuity-Tests aufgeführt und für alle Tests Einzelheiten zu Umgebung, Häufigkeit, Organisatoren und Teilnahme genannt. Alle relevanten Tests werden in Abschnitt 10.7 und Abschnitt 10.8 genau beschrieben.

Test der Contingency- und Business-Continuity-Verfahren von TARGET2/TIPS					
Testname	**Umgebung**	**Häufigkeit**	**Für die Organisation des Tests zuständig**	**Für Zentral-banken verpflichtend**	**Für kritische Teilnehmer verpflichtend**
Test der Contingency-Verfahren					
ECONS I					

Regelmäßiger Test von ECONS I	Testumgebung	alle 6 Monate	NZB	ja (für Zentralbanken des Eurosystems und verbundene Zentralbanken mit kritischen Teilnehmern, kritischen Nebensystemen und Teilnehmern, die sehr kritische Zahlungen abwickeln)	ja (für kritische Teilnehmer, kritische Nebensysteme und Teilnehmer, die sehr kritische Zahlungen abwickeln)
Testlauf von ECONS I unter Produktionsbedingungen	Produktionsumgebung	1 x im Jahr	EZB		
Zweitägiger Test von ECONS I unter Einbeziehung von T2S	Testumgebung	1 x im Jahr	EZB		Nein
Kritische TARGET2-Teilnehmer					
Funktionalität der Ersatzzahlungen	Produktionsumgebung /alternativ Testumgebung	alle 6 Monate	NZB	ja (für Zentralbanken mit kritischen Teilnehmern, kritischen Nebensystemen und Teilnehmern, die sehr kritische Zahlungen abwickeln)	ja (für kritische Teilnehmer, kritische Nebensysteme und Teilnehmer, die sehr kritische Zahlungen abwickeln, sofern sie diese Funktion nutzen möchten)
Im Auftrag von (NZB und SSP Service Desk)	Produktionsumgebung /alternativ Testumgebung	alle 6 Monate	NZB	ja (für Zentralbanken mit kritischen Teilnehmern, kritischen Nebensystemen und Teilnehmern, die sehr kritische Zahlungen abwickeln, sofern die jeweilige Zentralbank diese Möglichkeit anbietet)	ja (für kritische Teilnehmer, kritische Nebensysteme und Teilnehmer, die sehr kritische Zahlungen abwickeln, sofern sie diese Funktion nutzen möchten); abhängig von den Contingency-Verfahren

					ihrer jeweiligen Zentralbank
Test der Business-Continuity-Verfahren					
Intraregionale Ausfallsicherung der Gemeinschaftsplattform	Produktionsumgebung	alle 6 Monate	SSP	nein	nein
Interregionale Ausfallsicherung der Gemeinschaftsplattform	Produktionsumgebung	alle 6 Monate	SSP	nein	nein
Neustart der Gemeinschaftsplattform nach einem Katastrophenfall	Testumgebung	alle 6 Monate	SSP	nein	nein
Intraregionale Ausfallsicherung von TIPS	Produktionsumgebung	alle 6 Monate	EZB	nein	nein
Für NZBen (*Test des Sekundärstandorts*)	Produktionsumgebung	1 x im Jahr	NZB	ja	nein
Für kritische Teilnehmer (*Test des Sekundärstandorts*)	Produktionsumgebung	1 x im Jahr	kritischer Teilnehmer	nein	ja

10.6 Testergebnisse und -berichte

Die Testergebnisse müssen als „erfolgreich“ oder „nicht erfolgreich“ klassifiziert werden. Werden die Testziele nicht oder nur teilweise erreicht, ist das Testergebnis als nicht erfolgreich anzusehen. Nicht erfolgreiche Tests sind innerhalb von drei Monaten zu wiederholen.

Nebensysteme und Teilnehmer melden die Testergebnisse gemäß den Anweisungen des National Service Desk.

Die National Service Desks liefern der EZB in regelmäßigen Abständen zusammenfassende Berichte und ermöglichen so die systemweite Überwachung und Beurteilung, die dann in die halbjährliche Berichterstattung zu TARGET2 einfließt und gegebenenfalls Folgemaßnahmen nach sich zieht.

10.7 Test der Contingency-Verfahren

10.7.1 ECONS I

ECONS I ist das gemeinsame Instrument zur Bewältigung von Notfallsituationen, wenn die normale PM-Funktionalität nicht verfügbar ist, (sehr) kritische Zahlungen aber trotzdem abgewickelt werden

müssen. ECONS I kann an bis zu fünf aufeinanderfolgenden Tagen von Zentralbanken, direkten PM-Teilnehmern mit SWIFT-basiertem Zugang und für Überwachungszwecke auch von Nebensystemen verwendet werden. Nebensystemdateien können unter Nutzung eines speziellen Verfahrens durch Zentralbanken abgewickelt werden, die im Auftrag von Nebensystemen handeln.

Im Folgenden werden die für ECONS I vorgesehenen Tests in der Test- und in der Produktionsumgebung beschrieben.

Umfang: In allen genannten Fällen sollten die Tests folgende Schritte umfassen:

a) eine Liquiditätsbereitstellung auf den ECONS-I-Konten der Teilnehmer:
   1) Der National Service Desk stellt die Liquidität den am Test teilnehmenden ECONS-I-Konten direkt bereit.
   2) Alternativ erfolgen Liquiditätszuführungen aus T2S.

   Damit die Tests so effektiv wie nur möglich sind und einer echten Notfallsituation nahekommen, umfasst der Test zwischen den Zentralbanken und ihren PM-Kontoinhabern auch die Bereitstellung zusätzlicher Liquidität in ECONS I.
b) (gegebenenfalls) das Hochladen von Nebensystemdateien durch den National Service Desk und
c) die Abwicklung von Zahlungen durch die PM-Kontoinhaber und die Zentralbanken. Die PM-Kontoinhaber suchen sich Geschäftspartner, mit denen sie Zahlungen austauschen können.

Wenn Zahlungen zwischen verschiedenen Mitgliedstaaten Teil des Szenarios sind und der Geschäftspartner für Testzwecke nicht verfügbar ist, ersetzt die entsprechende Zentralbank den ausländischen Geschäftspartner mit einem ihrer eigenen Konten.

Regelmäßige Tests von ECONS I (in der Testumgebung)

Regelmäßige Tests von ECONS I in der Testumgebung sollten **mindestens alle sechs Monate von den Zentralbanken und denjenigen TARGET2-Teilnehmern durchgeführt werden, die zwingend an ECONS I angebunden sind** (kritische Teilnehmer und kritische Nebensysteme sowie Teilnehmer, die sehr kritische Zahlungen in TARGET2 abwickeln).

Zu Testzwecken aktiviert der SSP Service Desk mittwochs zwischen 10.00 Uhr und 12.00 Uhr ECONS I in der Testumgebung SSP CUST. Tests außerhalb dieses Zeitraums müssen über den zuständigen National Service Desk beim SSP Service Desk beantragt werden.

Die Zentralbanken sollten gemeinsam mit ihren nationalen Nutzergruppen die Daten und Zeiträume

festlegen, an denen solche Tests möglich sind. Alternativ können sie auch eine regelmäßige wöchentliche Testoption anbieten. Stellt eine Zentralbank nur eine begrenzte Anzahl an Daten und Zeiträumen bereit, so muss sie sicherstellen, dass jeder kritische Teilnehmer ausreichend Gelegenheit hat (z. B. ein Testtag pro Quartal), um die entsprechenden Tests zeitlich einzuplanen.

Testlauf von ECONS I unter Produktionsbedingungen

Mindestens einmal im Jahr koordiniert der TARGET Services Coordination Desk einen eintägigen **Testlauf** von ECONS I unter Produktionsbedingungen und **in der Produktionsumgebung** (der Termin für diesen Testlauf wird von der Ebene 2 vorab festgelegt).

Die **Teilnahme** an diesem Test **ist für alle Zentralbanken und diejenigen TARGET2-Teilnehmer verpflichtend, die zwingend an ECONS I angebunden sind** (kritische Teilnehmer und kritische Nebensysteme sowie Teilnehmer, die sehr kritische Zahlungen in TARGET2 abwickeln). Für den Testlauf unter Produktionsbedingungen aktiviert der SSP Service Desk ECONS I parallel zum normalen Geschäftsbetrieb in der Produktionsumgebung. Volumentests werden nicht durchgeführt.

Zweitägiger Test von ECONS I unter Einbeziehung von T2S (in der Testumgebung SSP CUST)

Einmal im Jahr koordiniert der TARGET Services Coordination Desk einen zweitägigen Test von ECONS I in der Testumgebung, in den auch T2S einbezogen wird (der Termin für diesen Testlauf wird von der Ebene 2 vorab festgelegt).

Die **Teilnahme** an diesem Test ist für **alle Zentralbanken** verpflichtend.

10.7.2 Funktionalität der Ersatzzahlungen

Beabsichtigen kritische Teilnehmer, kritische Nebensysteme sowie Teilnehmer, die sehr kritische Zahlungen in TARGET2 abwickeln, Ersatzzahlungen zu nutzen, dann sollten sie diese Funktion mindestens zweimal pro Jahr nach zeitlicher Abstimmung mit ihrer jeweiligen Zentralbank in der Produktionsumgebung testen. Jeder Teilnehmer sollte hierfür die Aktivierung der Back-up-Funktion für Ersatzzahlungen im Live-Betrieb (in der Produktionsumgebung) bei der Zentralbank beantragen und die Versendung der entsprechenden Ersatzzahlungen als Niedrigwertzahlungen (unter 10 €, verschiedene Beträge) auf vorher festgelegte Konten testen. Die Zentralbanken können ihre Konten als Empfänger der Zahlungen anbieten, wenn kein anderer Geschäftspartner für Testzwecke verfügbar ist.

Falls Tests in der Produktionsumgebung als zu risikoträchtig erachtet werden, kann dieselbe Art von Tests alternativ in der Testumgebung vorgenommen werden. In diesem Fall gibt es für die Betragshöhe keine Begrenzung.

PM-Kontoinhaber können zwei verschiedene Arten von Ersatzzahlungen verwenden, um Zahlungen über das ICM zu veranlassen, wenn die normale Zahlungsabwicklung unterbrochen ist.

- Contingency-Zahlungen werden eingesetzt, um Einzahlungsverpflichtungen gegenüber CLS,

EURO1 oder STEP2 termingerecht zu erfüllen. Die Contingency-Zahlung ersetzt die ursprüngliche Zahlung.

- Ersatzzahlungen zur Umverteilung von Liquidität erlauben es einem PM-Kontoinhaber, Liquidität, die sich auf seinem Konto angesammelt hat, umzulenken und einen etwaigen Aufbau von Überschussliquidität zu vermeiden, welcher die Effizienz von TARGET2 beeinträchtigen und möglicherweise zu systemischen Risiken führen könnte.

Die Zentralbanken können nach Absprache mit ihren TARGET2-Nutzern beschließen, die Anzahl der Tage und die Zeiträume für die Durchführung solcher Tests zu begrenzen. Sie können diese Tests aber auch als ständiges Angebot bereithalten, das an jedem Tag, an dem die jeweilige Umgebung in Betrieb ist, in Anspruch genommen werden kann. Bei einer Begrenzung der Testzeit hat die Zentralbank darauf zu achten, dass jeder kritische Teilnehmer ausreichend Gelegenheit hat, um die jeweiligen Tests mindestens alle drei Monate durchführen zu können.
Nichtkritische Teilnehmer sollten in regelmäßigen Abständen ähnliche Tests mit ihrem jeweiligen National Service Desk vorsehen.

10.7.3 Agieren im Auftrag (NZB und SSP Service Desk)

Beabsichtigen **kritische Teilnehmer, kritische Nebensysteme sowie Teilnehmer, die sehr kritische Zahlungen in TARGET2 abwickeln, ein zusätzliches Angebot ihrer Zentralbank**[86] **(z. B. das „AS Contingency Tool“ oder „mandated payments“)** zu nutzen, dann sollten sie **mindestens zweimal pro Jahr** nach zeitlicher Abstimmung mit ihrer jeweiligen Zentralbank die folgenden Szenarien **im Live-Betrieb** (in der Produktionsumgebung) testen:

1) Die Zentralbanken sollten in der Lage sein, die kritischen Zahlungen im Auftrag ihrer kritischen Teilnehmer unter Verwendung der Funktionalität der Ersatzzahlungen auszuführen und dies gemeinsam mit ihnen zu testen.

2) Zentralbanken, die ihren Nebensystemen das „AS Contingency Tool“ anbieten, sollten dessen Funktionsfähigkeit testen.

3) Zentralbanken, die ihren kritischen Teilnehmern „mandated payments“ anbieten, sollten deren Funktionsfähigkeit testen.

Falls Tests in der Live-Umgebung als zu risikoträchtig erachtet werden, kann dieselbe Art von Tests alternativ in der Testumgebung vorgenommen werden.

[86] Dies hängt davon ab, welche Contingency-Verfahren ihre Zentralbank anbietet.

Die Zentralbanken können nach Absprache mit ihren TARGET2-Nutzern beschließen, die Anzahl der Tage und die Zeiträume für die Durchführung solcher Tests zu begrenzen. Sie können diese Tests aber auch als ständiges Angebot bereithalten, das an jedem Tag, an dem die jeweilige Umgebung in Betrieb ist, in Anspruch genommen werden kann. Bei einer Begrenzung der Testzeit hat die Zentralbank darauf zu achten, dass jeder kritische Teilnehmer ausreichend Gelegenheit hat, um die jeweiligen Tests mindestens alle drei Monate durchführen zu können.

Nichtkritische Teilnehmer sollten in regelmäßigen Abständen ähnliche Tests mit ihrem jeweiligen National Service Desk vorsehen.

10.8 Test der Business-Continuity-Verfahren

Die Business-Continuity-Verfahren der Gemeinschaftsplattform umfassen die bestehenden Verfahren und Infrastrukturen für die Gemeinschafts- und die T2S-Plattform, die bei einem Ausfall oder einer Notfallsituation eine Ausfallsicherung zum Ersatzstandort innerhalb derselben oder in einer anderen Region ermöglichen. NZBen, die ein PHA unterhalten, sowie kritische Teilnehmer sollten ähnliche Verfahren und Infrastrukturen besitzen. Darüber hinaus sind die Überwachungsanforderungen zur Gewährleistung der Business Continuity bei systemrelevanten Zahlungssystemen (Business continuity oversight expectations for systemically important payment systems – SIPS) zu beachten.

10.8.1 Intraregionale Ausfallsicherung der Gemeinschaftsplattform

Im Rahmen der Tests der interregionalen Ausfallsicherung wird überprüft, ob ein Standort durch die Verlagerung von Standort 1 zu Standort 2 in derselben Region wiederhergestellt werden kann.

Dieses Szenario wird **alle sechs Monate** an einem Wochenende **in der Produktionsumgebung** getestet. Je nachdem, in welcher Phase des Geschäftstags der Test durchgeführt wird, kann auch die Abwicklung getestet werden. Vergleichbare Tests können auch während eines normalen Geschäftstags und in den regulären Geschäftszeiten in der Testumgebung erfolgen.

10.8.2 Interregionale Ausfallsicherung der Gemeinschaftsplattform

Bei den Tests der interregionalen Ausfallsicherung wird diese anhand eines Szenarios ohne Datenverluste überprüft (d. h. durch Verlagerung des Standorts von Region 1 in Region 2).

Dieses Szenario wird **alle sechs Monate** an einem Wochenende **in der Produktionsumgebung** getestet. Je nachdem, in welcher Phase des Geschäftstags der Test durchgeführt wird, kann auch die Abwicklung getestet werden. Vergleichbare Tests können auch während eines normalen Geschäftstags und in den regulären Geschäftszeiten in der Testumgebung erfolgen.

10.8.3 Neustart der Gemeinschaftsplattform nach einem Katastrophenfall

Beim Test eines Neustarts nach einem Katastrophenfall wird die interregionale Ausfallsicherung anhand eines Szenarios mit Datenverlusten überprüft (d. h. durch Verlagerung des Standorts von Region 1 in Region 2).

Dieses Szenario wird mindestens **alle sechs Monate** während eines normalen Geschäftstags und in den regulären Geschäftszeiten **in der Testumgebung** getestet. Der SSP Service Desk simuliert den Ausfall des Systems in einer Region und die Wiederaufnahme der Geschäfte in einer anderen Region, wobei es zu einem Verlust von Daten kommt.

Teilnehmer können über den National Service Desk gebeten werden, an den Tests mitzuwirken.

10.8.4 Intraregionale Ausfallsicherung von TIPS

TIPS ist an den beiden Standorten von TARGET2 und T2S angesiedelt und wird auch von dort aus betrieben. **Alle sechs Monate ist in der Produktionsumgebung** (durch eine Erprobung) zu überprüfen, ob die Ausfallsicherung vom Primärstandort zum Ausweichstandort reibungslos funktioniert. Dies kann allerdings möglicherweise bei TIPS zu einer Betriebsunterbrechung von bis zu 15 Minuten führen.

Die National Service Desks teilen ihren TIPS-Teilnehmern die Termine mit, an denen die Tests geplant sind.

10.8.5 Für NZBen

Die Zentralbanken sollten stets über Business-Continuity-Verfahren gemäß den TARGET2-Sicherheitsanforderungen und -kontrollen (TARGET2 Security Requirements and Controls – T2SRC) verfügen.

Die Zentralbanken unterliegen dem Geltungsbereich der „Information security policy for TARGET2“ und haben somit dafür zu sorgen, dass ihre Infrastrukturen sicher und zuverlässig funktionieren.

Mindestens einmal im Jahr müssen die Zentralbanken ihre Business-Continuity-Verfahren testen, indem sie ihre **täglichen Arbeiten in der Produktionsumgebung** vom Sekundärstandort aus erledigen und von dort den Geschäftstag abschließen.

10.8.6 Kritische TARGET2-Teilnehmer

Jeder Teilnehmer, der vom Eurosystem im Hinblick auf das reibungslose Funktionieren von TARGET2 **als kritisch eingestuft wurde**, muss über eine Strategie zur Aufrechterhaltung des Geschäftsbetriebs verfügen, die folgende Elemente aufweist:

- Es müssen Business-Continuity-Pläne und Verfahren zu deren Einhaltung vorhanden sein.

- Es muss ein Ausweichstandort vorhanden sein.
- Das Risikoprofil des Ausweichstandorts muss sich von dem des Primärstandorts unterscheiden (erhebliche Entfernung zwischen den Standorten, anderes Energieversorgungsnetz, andere Hauptfernmeldeleitungen usw.).
- Im Falle einer größeren Betriebsstörung, die dazu führt, dass auf den Primärstandort nicht zugegriffen werden kann und/oder die für den Betrieb notwendigen Mitarbeiter nicht verfügbar sind, muss der kritische Teilnehmer in der Lage sein, den normalen Betrieb vom Ausweichstandort aus wiederaufzunehmen. Dabei muss es möglich sein, vom Ausweichstandort aus den Geschäftstag ordnungsgemäß abzuschließen und den/die folgenden Geschäftstag(e) zu beginnen.
- Es müssen Verfahren etabliert worden sein, die gewährleisten, dass die kritischsten Transaktionen während der Verlagerung vom Primärstandort zum Ausweichstandort ausgeführt werden können.
- Die Fähigkeit, Betriebsstörungen zu bewältigen, wird **mindestens einmal im Jahr** geprüft, und alle wichtigen Mitarbeiter werden angemessen geschult. Der Abstand zwischen den Tests sollte nicht länger als ein Jahr sein.

Unter Berücksichtigung der genannten Punkte lassen sich die Business-Continuity-Testanforderungen folgendermaßen zusammenfassen:

- **Mindestens einmal im Jahr** müssen die kritischen Teilnehmer ihre Business-Continuity-Verfahren testen, vom Sekundärstandort aus ihre kritischen Transaktionen **in der Produktionsumgebung** ausführen und von dort den Geschäftstag abschließen (siehe Abschnitt 10.5).

11 Change- und Release-Management-Verfahren

In diesem Abschnitt werden das jährliche TARGET2-Release-Management-Verfahren sowie das Änderungsverfahren bei Notfalländerungen und „Hot Fixes“ mit Blick auf die SSP beschrieben.
Darüber hinaus wird das Change-, Release- und Deployment-Management-Verfahren für TIPS (im Folgenden als CRM bezeichnet) dargestellt. Dieses Verfahren legt fest, wie funktionale Veränderungen in TIPS zu steuern sind. Veränderungen der geldbezogenen Funktionalitäten auf der T2S-Plattform sollten im Einklang mit dem Change- und Release-Management-Verfahren erfolgen, das in der T2S-Rahmenvereinbarung – Schedule 9 beschrieben wird.

11.1 Change- und Release-Management für TARGET2

11.1.1 Jährliches Release

Das Eurosystem ist bestrebt, das TARGET2-System stets an die verschiedenen Geschäftsänderungen auf dem Gebiet der Großbetragszahlungen anzupassen. Dieses kontinuierliche Interesse an einer Weiterentwicklung des Systems wird als notwendig erachtet, um das Niveau der angebotenen Dienstleistungen und die Zufriedenheit der Nutzer weiter zu erhöhen. Daher ist es äußerst wichtig, dass alle TARGET2-Nutzer in angemessener Form und zeitnah in den Prozess des Release Managements eingebunden werden.

TARGET2-Releases erscheinen im Allgemeinen jährlich, und zwar zeitgleich mit dem jährlichen SWIFT Standard Release im November. In Ausnahmefällen kann jedoch auch in einem Jahr ein zusätzliches (d. h. zweites) oder gar kein Release herausgegeben werden.

Das jährliche TARGET2-Release durchläuft ein langes, 21 Monate dauerndes Verfahren, damit alle Parteien genügend Zeit zur Erörterung, Priorisierung, Umsetzung und zum Testen haben. Außerdem werden den TARGET2-Nutzern alle Informationen so früh zur Verfügung gestellt, dass sie die Änderungen gut planen und budgetieren können.

11.1.2 Wichtige Termine

Alle in diesem Abschnitt genannten Termine sind unverbindlich und werden vom Eurosystem für jedes jährliche Release im Laufe des Februar des Jahres J-1 bestätigt. Das Eurosystem ist zwar bestrebt, die Termine weitestgehend einzuhalten, doch sind bei Bedarf und nach Absprache mit den Nutzern geringfügige Abweichungen möglich.

Jahr J-1	Mitte Februar	Bestätigung der endgültigen Termine
	Anfang März – Mitte April	Erste Konsultation der Nutzer
	Mitte September – Mitte Oktober	Zweite Konsultation der Nutzer
	Mitte November	Bekanntgabe des Release-Inhalts
Jahr J	Anfang März	Lieferung der UDFS
	Mitte April	Lieferung der Testpläne und -szenarien
	Ende August	Testbeginn durch die Nutzer
	Mitte November	Inbetriebnahme

Tabelle 14: Zeitplan für das jährliche Release

11.1.3 Einbindung der Nutzer

Im Rahmen der Erörterungen zum Inhalt des jährlichen TARGET2-Release werden zwei Konsultationsverfahren mit der Nutzergemeinschaft durchgeführt. Um alle TARGET2-Nutzer in die Ausarbeitung des Release-Inhalts einzubeziehen, setzen sich die nationalen Zentralbanken der an TARGET2 angeschlossenen Länder mit ihren jeweiligen nationalen Nutzergruppen in Verbindung.

- Im ersten Konsultationsverfahren werden Vorschläge aller Nutzer für funktionale Änderungen zusammengetragen. Diese Vorschläge sollen hinreichend detailliert sein und einer großen Zahl von Nutzern zugutekommen. Zur Vereinfachung der Konsultation werden als Diskussionsgrundlage eine Liste funktionaler Änderungen, die im Zuge früherer Releases vorgeschlagen wurden, sowie von Zentralbanken unverbindlich angeregte Modifikationen vorgelegt, die jeweils mit eindeutigen Referenznummern gekennzeichnet sind. In jedem Vorschlag sollten der jeweilige Geschäftsvorfall und die erwarteten funktionalen Änderungen präzise dargelegt werden. Das Eurosystem stellt für die Einreichung ein entsprechendes Formular zur Verfügung. Am Ende des ersten Konsultationsverfahrens prüft das Eurosystem sorgsam sämtliche Vorschläge der nationalen Nutzergruppen und nimmt einen Teil der vorgeschlagenen Änderungen in die engere Wahl; für diese wird eine weitere Kosten-Nutzen-Analyse durchgeführt.
- Im zweiten Konsultationsverfahren werden die Rückmeldungen der Nutzer zu den aus der ersten Konsultation hervorgegangenen und von den Zentralbanken in die engere Wahl genommenen Änderungen erfasst. In diesem Stadium sind keine weiteren Änderungsvorschläge mehr möglich. Gegebenenfalls werden auch Angaben zu den Kosten der vorgesehenen Maßnahmen gemacht. Die Rückmeldungen müssen auf der Grundlage zuvor festgelegter Standardbewertungskriterien erfolgen. Am Ende der zweiten Konsultation prüft das Eurosystem alle Rückmeldungen der Nutzer und kommt zu einer abschließenden Einschätzung in Bezug auf den Inhalt des jährlichen

TARGET2-Release. Dieser wird wenig später bekannt gegeben.[87]

Um den Nutzern die Darlegung ihrer Änderungswünsche zu erleichtern, wurde ein Formular für Änderungsvorschläge (Anhang IV) entworfen. Alle von den Nutzern vorgebrachten Änderungswünsche sind auf diesem Formular einzureichen. Jedes andere Formular wird abgewiesen und zurückgereicht.

11.1.4 Priorisierung und Entscheidungsfindung

Bei der Priorisierung der verschiedenen Vorschläge der Nutzer oder der endgültigen Entscheidung zum Release-Inhalt tragen die Zentralbanken folgenden Kriterien gebührend Rechnung:

- Für jede einzelne Änderung wird eine eingehende Kosten-Nutzen-Analyse durchgeführt. Dabei werden vor allem folgende Punkte in Betracht gezogen: die Rückmeldungen der Nutzergemeinschaft im Zuge der Konsultationsrunden, die durch die Änderung realisierte Verbesserung des Dienstleistungsangebots für den Bankensektor insgesamt, die erwartete Nutzung des neuen Merkmals, die damit verbundenen Investitionen und Betriebskosten, die Nachhaltigkeit der neuen Dienstleistung im Hinblick auf die Kostendeckung, die Komplexität der Entwicklungen sowie das mögliche Risiko, Regressionsfehler in das System einzubringen. Wann immer dies erforderlich ist, prüfen die Zentralbanken schließlich auch, inwieweit die Änderung mit der Politik oder Strategie des Eurosystems zu TARGET2 im Einklang steht.
- Die Zentralbanken sind bestrebt sicherzustellen, dass der Release-Inhalt insgesamt im Hinblick auf die Vorteile, die den verschiedenen Gruppen von Nutzern entstehen, ausgewogen ist und die für das jährliche Release festgelegten Höchstbelastungen für den Arbeitsaufwand und das Budget eingehalten werden.

Aus Transparenzgründen werden die Nutzer nach jedem Konsultationsschritt darüber informiert, warum eine Änderung ausgewählt oder verworfen wurde.

11.1.5 Notfalländerungen und Hot Fixes

In diesem Abschnitt sollen diejenigen Elemente des Change- und Release-Management-Verfahrens für die Gemeinschaftsplattform beschrieben werden, die eng mit dem täglichen TARGET2-Betrieb zusammenhängen und als solche nicht Bestandteil des alljährlichen Release-Management-Verfahrens sind.

Folgende Arten von Änderungen können in der Zeit zwischen den jährlichen Standard-Releases zu einer Modifikation der Gemeinschaftsplattform führen:

87 Das Eurosystem kann über Änderungen, die mit SWIFT zusammenhängen, zu einem späteren Zeitpunkt informieren, wenn der endgültige Inhalt des SWIFT FIN und CAMT Standard Release bekannt ist. Wenn durch das Release auch Fehler behoben werden, so werden diese Änderungen ebenfalls später bekannt gegeben.

1. Notfalländerungen
2. Kleinere Änderungen, die so schwerwiegend sind, dass sie als Hot Fix umgesetzt werden.

Alle weiteren Änderungen werden im Rahmen des normalen Change- und Release-Management-Verfahrens bei den jährlichen Releases berücksichtigt.

11.1.6 Notfalländerungen

Notfalländerungen kommen bei Systemfehlern zum Tragen, die einer sofortigen Änderung bedürfen, damit der Betrieb der SSP aufrechterhalten oder eine erhebliche Einschränkung der Service-Qualität verhindert wird. Solche Änderungen sind eng mit dem in Abschnitt 5 beschriebenen Verfahren zur Störungsbehebung verknüpft und können innerhalb eines TARGET2-Geschäftstags installiert werden. Beeinträchtigt eine Notfalländerung die von TARGET2-Nutzern verwendeten Funktionalitäten, so werden die Nutzer im Wege einer ICM-Nachricht darüber informiert.

11.1.7 Hot Fixes

Hot Fixes sind nur dann gerechtfertigt, wenn durch die ausbleibende Beseitigung eines Problems vor dem nächsten regulären Release erhebliche operationelle Probleme entstehen könnten, komplizierte Provisorien erforderlich wären und/oder es anderweitig zu einer deutlichen Zunahme der operationellen Risiken käme. Hot Fixes werden immer zuerst in der entsprechenden Testumgebung („CUST“ für TARGET2) installiert und dort – soweit möglich – getestet, bevor sie in der Produktionsumgebung eingesetzt werden. Falls dies aufgrund der Auswirkungen auf die Nutzer notwendig ist, werden alle Nutzer über eine ICM-Nachricht von dem bevorstehenden Hot Fix in Kenntnis gesetzt.

11.2 Change-, Release- und Deployment-Management in TIPS

Der Change-, Release- und Deployment-Manangement-Prozess – kurz CRM – definiert, wie Funktionsänderungen an TIPS gehandhabt werden. Das CRM deckt den gesamten Lebenszyklus eines Änderungsvorschlags (Change Request) ab, vom Zeitpunkt der formellen Einreichung des Vorschlags bis zu dessen Release in der Produktionsumgebung. Hierzu gehören auch die Planung und Vereinbarung des Inhalts eines Releases sowie das sich daraus ergebende Design, der Aufbau, die Konfiguration und das Testen der neuen Hard- und Softwarekomponenten.

11.2.1 CRM-Verfahren für TIPS

Die Change- und Release-Management-Prozesse bestimmen das Verfahren, mit dem vorgeschlagene Modifikationen und Verbesserungen an TIPS im Verlauf von dessen Lebenszyklus gehandhabt werden.

Der Prozess beginnt in dem Moment, in dem ein Änderungsvorschlag formell eingereicht wird, und endet, wenn er abgeschlossen wurde (also zurückgezogen, zurückgewiesen oder in einem Release umgesetzt wurde).

11.2.1.1 Wichtige Fristen

Änderungsvorschläge können jederzeit eingereicht werden, spätestens jedoch 19 Monate vor dem anvisierten Release.

Das Change-Management bestimmt den Lebenszyklus von vorgeschlagenen Modifikationen und Verbesserungen, die funktionale oder nicht funktionale Änderungen nach sich ziehen können.

Die EZB, alle an TARGET teilnehmenden Zentralbanken (aus Euro- und Nicht-Euro-Ländern), TIPS-Teilnehmer und der TIPS-Betreiber können formal Änderungsvorschläge einreichen.

Zu Beginn jedes Jahres informieren die Nationalen Service Desks ihre TIPS-Teilnehmer über die bevorstehende Frist.

Nach genauer Prüfung durch die involvierten Parteien sollten die Change Requests und Lösungen für Produktionsprobleme einem Release mindestens elf Monate vor der geplanten Live-Schaltung zugewiesen werden.

11.2.1.2 Release-Management

Das Release-Management ist ein spezifischer Prozess, mit dem Change Requests und Produktionsprobleme beurteilt und eingestuft werden, um den Umfang und den angestrebten Umsetzungstermin eines neuen TIPS-Releases zu bestimmen. Damit wird sichergestellt, dass sämtliche Aspekte einer Änderung – ob technischer oder nichttechnischer Natur – berücksichtigt werden. Hierzu gehört ggf. auch die Koordination mit den anderen TARGET-Services. Das Release-Management regelt alle Arten möglicher Releases:

- das jährliche Release, das nach dem dritten Wochenende im November erfolgt,
- ein optionales Release im Juni, sofern dies erforderlich ist, sowie
- Änderungen an gemeinsamen Komponenten (diese können außerhalb des üblichen TIPS-Releasekalenders erfolgen).

11.2.1.3 Deployment-Management

Im Rahmen des Deployment- oder Bereitstellungsmanagements wird das Roll-out von TIPS-Softwarereleases, konfigurierbaren Parameteränderungen und/oder etwaigen damit zusammenhängenden Änderungen von Betriebsdienstleistungen in der CERT-Umgebung und der Produktionsumgebung organisiert.

- Die Bereitstellung eines TIPS-Release erfolgt rollierend, indem die Änderungen ausschließlich auf einem Knoten aktiviert werden. Das Verhalten wird dann für einige Zeit vom TIPS Service Desk beobachtet, um festzustellen, ob es den Erwartungen entspricht. Ist dies der Fall, dann wird das Release auch auf den anderen Knoten bereitgestellt. Je nachdem, welcher Knoten eingehende Nachrichten verarbeitet, sind unterschiedliche Ergebnisse zu erwarten.

  Wichtiger Hinweis zum erwarteten Verhalten von TIPS während des rollierenden Upgrades

  Werden im Rahmen eines TIPS-Releases a) ein neuer Nachrichtentyp für TIPS oder b) neue Felder in einem bereits in TIPS verwendeten Nachrichtentyp bzw. Änderungen an Feldern eines bestehenden Nachrichtentyps eingeführt, so werden die Teilnehmer zur Vermeidung von Rückweisungen gebeten,

  1. den neuen Nachrichtentyp erst ab dem Tag nach Abschluss des rollierenden Upgrades für TIPS zu verwenden. Während des rollierenden Upgrades sollte weiterhin die alte Version der Nachricht versendet werden;

  2. ihre Systeme darauf vorzubereiten, während des rollierenden Upgrades sowohl alte als auch neue Versionen des Nachrichtentyps zu empfangen.

11.2.1.3.1Standardmäßiges Deployment-Verfahren

Das standardmäßige Verfahren zur Bereitstellung eines Releases folgt einem mehrstufigen Konzept: Das Release wird zunächst in der EAC-Umgebung, dann in der CERT-Umgebung und schließlich in der Produktionsumgebung bereitgestellt. Sofern von der TSWG nicht anders vereinbart, werden die Releases in der Woche, für die sie geplant sind, rollierend in der Produktionsumgebung bereitgestellt.

Vor der Bereitstellung wird das neue Release zunächst vom Eurosystem und dem EAT-Team der EZB in der EAC-Umgebung getestet. Anschließend folgen die Nutzertests in der CERT-Umgebung.

Abbildung 25: TIPS-Umgebungen für die Bereitstellung von Releases

11.2.2 Notfalländerungen und Hot Fixes

Notfalländerungen werden vom TIPS Service Desk direkt in der Produktionsumgebung bereitgestellt. Damit sollen schwerwiegende Störungen behoben oder umgangen und so mögliche Komplettausfälle sämtlicher oder einiger Dienste verhindert werden, für die es keine Ausweichlösung gäbe.

In diese Kategorie fallen

- Notfalländerungen sowie
- kleinere Änderungen, die als Hot Fix umgesetzt werden.

Alle weiteren Änderungen werden im Rahmen des normalen Change- und Release-Management-Prozesses bei den jährlichen Releases berücksichtigt.

11.2.2.1 Bereitstellung von Notfalländerungen

Beim Auftreten von Systemfehlern kann beschlossen werden, umgehend Änderungen durchzuführen, damit der Normalbetrieb von TIPS wiederaufgenommen werden kann. Solche Notfalländerungen erfolgen direkt in der Produktionsumgebung.

11.2.2.2 Release- und Deployment-Management für Hot Fixes

Hot Fixes sind Änderungen, die alle Softwarekorrekturen umfassen, welche aufgrund der Dringlichkeit der Fixes vor dem nächsten normalen Release umgesetzt werden müssen (d. h. die Behebung von Problemen in der Produktionsumgebung, die den Betrieb des Systems massiv stören können, erhebliche Ausweichlösungen nach sich ziehen könnten und/oder das operative Risiko auf sonstige Weise deutlich erhöhen würden). Da solche Änderungen aus Zeitgründen nicht im Rahmen des Change-Management-Prozesses oder des üblichen Release-Management-Prozesses erfolgen können, wird dafür ausschließlich der Release-Management-Prozess für Hot Fixes angewendet.

12 Datenschutz-Grundverordnung (DSGVO) – operative Verfahren in Bezug auf TARGET2 und TIPS

TARGET2 und TIPS sind technische Plattformen, die sowohl Stamm- als auch Transaktionsdaten verarbeiten und speichern, die zu Abrechnungszwecken empfangen werden. Teile der Daten, die im Zusammenhang mit der Transaktionsabwicklung oder zur Anlage von Stammdaten von TARGET2/TIPS-Nutzern übermittelt werden, können personenbezogene Daten enthalten. Somit unterliegen beide Plattformen der Datenschutz-Grundverordnung (Verordnung (EU) 2016/679) sowie der europäischen Datenschutzverordnung (Verordnung (EU) 2018/1725).

In den folgenden zwei Fällen wird das Eurosystem betroffene Personen über die Verarbeitung ihrer personenbezogenen Daten in TARGET2/TIPS informieren und entsprechende Unterstützung leisten:

1. bei Anträgen betroffener Personen zur Identifizierung etwaiger von den TARGET2/TIPS-Plattformen verarbeiteter personenbezogener Daten,
2. bei Verletzungen des Schutzes personenbezogener Daten in TARGET2/TIPS.

Anträge betroffener Personen

Grundsätzlich sollten sich betroffene Personen bei Fragen zur Verarbeitung ihrer personenbezogenen Daten zunächst an ihre Geschäftsbank wenden. Die Geschäftsbank wird ihnen ggf. mitteilen, dass ihre personenbezogenen Daten an die jeweilige Zentralbank übermittelt wurden, um eine reibungslose Abwicklung der Zahlungen in TARGET2/TIPS zu gewährleisten. Die betroffenen Personen können sich dann entsprechend bei der Zentralbank erkundigen. Anfragen können auch unmittelbar an die zuständige nationale Zentralbank oder die EZB gerichtet werden.

Dazu muss ein formales Auskunftsersuchen (Anhang V) an die betreffende Zentralbank gestellt werden. Gemäß der DSGVO können die Zentralbanken zusätzliche Daten anfordern, um den zur Identifizierung und zum Abruf der personenbezogenen Daten erforderlichen Aufwand zu begrenzen, z. B. die genaue Schreibweise des Namens, die IBAN/BIC, den Referenzzeitraum und die Art der Transaktion. Auskunftsersuchen sind stets gemäß den Gesetzen und Vorschriften des Landes zu stellen, in dem die gemeinsam datenverantwortliche Partei („Partial Joint Controller“) ansässig ist, an den sie gerichtet sind. Sofern nicht anders angegeben, sollte die Antwort über den gleichen Kommunikationsweg zugestellt werden wie das Ersuchen.

Die Identität der ersuchenden Person wird gemäß den Gesetzen und Vorschriften des Landes überprüft, in dem der „Partial Joint Controller“ ansässig ist, an den das Ersuchen gerichtet ist.

Die als „Partial Joint Controller“ Zentralbank lässt der Auskunft ersuchenden Person innerhalb eines Kalendermonats nach Eingang des Ersuchens ein Status-Update oder eine sonstige Rückmeldung zukommen. Dieser Zeitraum kann je nach Komplexität und Anzahl der insgesamt eingegangenen Ersuchen zu personenbezogenen Daten gegebenenfalls auf bis zu drei Monate verlängert werden. In diesem Fall wird die betroffene Person innerhalb eines Kalendermonats nach Eingang des ursprünglichen Ersuchens über die Verzögerung und den Grund hierfür informiert.

Beschließt der „Partial Joint Controller“, einem Ersuchen nicht nachzukommen, weil dieses eindeutig unbegründet oder der zur Beantwortung erforderlichen Aufwand unverhältnismäßig hoch ist, wird die ersuchende Person hierüber innerhalb eines Kalendermonats nach Eingang des Ersuchens informiert. Dabei wird die Abweisung begründet und dargelegt, inwiefern das Ersuchen unbegründet oder unverhältnismäßig ist.

Verletzungen des Schutzes personenbezogener Daten

Wenn ein Verstoß vorliegt, der zu einer Verletzung des Schutzes personenbezogener Daten geführt hat und damit die Rechte und Freiheiten von Einzelpersonen gefährdet, sind sämtliche „Partial Joint Controllers“ verpflichtet, alle potenziell betroffenen Personen unverzüglich über die Datenschutzverletzung zu informieren und ihnen die möglichen Auswirkungen darzulegen, um potenzielle negative Folgen abzumildern. Dabei sind auch die Art des Datenverstoßes und der Umfang des potenziellen Verlusts bzw. der unerlaubten Verbreitung der Daten sowie deren mögliche Auswirkungen zu benennen.

13 TARGET2-Ausgleichsregelung

13.1 Allgemeines

Wenn in TARGET2 eine technische Störung auftritt, können die Teilnehmer gemäß der TARGET2-Ausgleichsregelung in Anhang II der Harmonisierten Bedingungen für die Eröffnung und Führung eines PM-Kontos sowie in Anhang II der Harmonisierten Bedingungen für die Eröffnung und Führung eines T2S-Geldkontos Ausgleichsforderungen geltend machen. Die Ausgleichsregelung gilt jedoch nicht für TIPS.

Vorbehaltlich einer anders lautenden Entscheidung des EZB-Rats findet die TARGET2-Ausgleichsregelung keine Anwendung, wenn die technische Störung von TARGET2 durch äußere Ereignisse verursacht wurde, die außerhalb der Einflussnahmemöglichkeit der betreffenden Zentralbanken liegen, oder das Ergebnis von Handlungen oder Unterlassungen Dritter ist.

Ausgleichszahlungen gemäß der TARGET2-Ausgleichsregelung stellen den einzigen Ausgleichsmechanismus dar, der im Falle einer technischen Störung von TARGET2 angeboten wird. Die TARGET2-Teilnehmer können jedoch auf anderem rechtlichen Wege Ausgleichsforderungen geltend machen. Mit der Annahme eines Ausgleichsangebots im Rahmen der TARGET2-Ausgleichsregelung verzichtet der TARGET2-Teilnehmer unwiderruflich auf alle Ansprüche hinsichtlich der Zahlungsaufträge, für die er das Ausgleichsangebot angenommen hat (einschließlich aller Ansprüche auf Ausgleich für Folgeschäden), gegenüber jeder Zentralbank. Mit Erhalt der entsprechenden Ausgleichszahlung sind alle diese Ansprüche vollständig und endgültig abgegolten. Der Teilnehmer stellt die betreffenden Zentralbanken bis in Höhe des Betrags frei, den er im Rahmen der TARGET2-Ausgleichsregelung erhalten hat, und zwar hinsichtlich aller sonstigen Ausgleichsforderungen, die ein anderer Teilnehmer oder Dritter für den betreffenden Zahlungsauftrag oder die betreffende Zahlung geltend macht.

Ein Ausgleichsangebot stellt kein Haftungseingeständnis der betreffenden Zentralbank oder einer anderen Zentralbank in Bezug auf eine technische Störung von TARGET2 dar.

Nähere Informationen finden sich in Anhang II der Harmonisierten Bedingungen für die Eröffnung und Führung eines PM-Kontos sowie in Anhang II der Harmonisierten Bedingungen für die Eröffnung und Führung eines T2S-Geldkontos.

13.2 Verfahrensregeln

- Ausgleichsforderungen sind mit dem Antragsformular geltend zu machen, das auf der Website der betreffenden Zentralbank in englischer Sprache zur Verfügung steht. Zahler müssen für jeden

Zahlungsempfänger, Zahlungsempfänger für jeden Zahler ein gesondertes Antragsformular einreichen. Die Angaben im Antrag sind durch ausreichende Informationen und Unterlagen zu belegen. Je Zahlung oder Zahlungsauftrag darf nur ein Antrag eingereicht werden.

- Teilnehmer müssen ihre Anträge innerhalb von vier Wochen nach einer technischen Störung von TARGET2 bei der zuständigen Zentralbank einreichen. Weitere Informationen oder Belege, die die betreffende Zentralbank anfordert, sind innerhalb einer Frist von zwei Wochen nach Anforderung einzureichen.
- Die betreffende Zentralbank prüft die Anträge und leitet sie an die EZB weiter. Vorbehaltlich eines anders lautenden, den Teilnehmern mitzuteilenden Beschlusses des EZB-Rats werden alle eingegangenen Anträge innerhalb von 14 Wochen nach Auftreten der technischen Störung beurteilt.
- Die betreffende Zentralbank teilt den jeweiligen Teilnehmern das Ergebnis der Beurteilung mit. Wird aufgrund dieser Beurteilung ein Ausgleichsangebot gemacht, so müssen die betreffenden Teilnehmer das Angebot in Bezug auf jede/n in ihrem Antrag enthaltene/n Zahlung oder Zahlungsauftrag innerhalb von vier Wochen nach Übermittlung des Angebots durch Unterzeichnung eines Standard-Annahmeschreibens, dessen jeweils aktuelle Fassung auf der Website der betreffenden Zentralbank abrufbar ist, annehmen oder ablehnen. Geht der betreffenden Zentralbank innerhalb von vier Wochen kein Annahmeschreiben zu, so gilt dies als Ablehnung des Ausgleichsangebots durch die jeweiligen Teilnehmer.
- Die betreffende Zentralbank leistet die Ausgleichszahlungen nach Erhalt des Annahmeschreibens des TARGET2-Nutzers. Auf Ausgleichszahlungen werden keine Zinsen erstattet.

Anhang I SSP Interregionale Ausfallsicherung mit Datenverlust

Wiederherstellungsprozess

Gemäß den drei Anbieter-Zentralbanken (3ZB) ist ein Wiederherstellungsprozess in Region 2 nur dann erforderlich, wenn beide Standorte in Region 1 gleichzeitig ausfallen und es daher zu einem Datenverlust kommt. **Durch die Wiederherstellung soll gewährleistet werden, dass alle in Region 1 verarbeiteten Nachrichten auch in Region 2 angezeigt werden.** Zu diesem Zweck werden alle Nachrichten, die in Region 1 in den zwei Minuten vor der Störung verarbeitet wurden, wiederholt und mit den in Region 2 angezeigten Nachrichten abgestimmt, um möglicherweise fehlende Nachrichten zu identifizieren.

Möglicherweise fehlen könnten beispielsweise FIN-Nachrichten (Zahlungen und Liquiditätsübertragungen einschließlich solcher, die über die T2S-Schnittstelle (T2SI) an bzw. von T2S-Geldkonten gesendet wurden, sowie FileAct-Nachrichten (die von einem Nebensystem über eine Nebensystemschnittstelle (ASI) gesendet wurden), oder InterAct-Nachrichten (XML-Nachrichten, die auf eines der SSP-Module oder an die T2SI gesendet wurden).

Der Wiederherstellungsprozess sollte in folgenden Schritten ablaufen:

1) FIN-Nachrichten können wiederholt und der FIN-Nachrichtenverkehr abgestimmt werden (dies würde etwa 80 % des fehlenden Nachrichtenverkehrs ausmachen).

   Nach Abruf der FIN-Nachrichten (wobei Nachrichten im Zusammenhang mit T2S-Geldkonten unberücksichtigt bleiben) werden alle zusammengehörenden FIN-Nachrichten (sich entsprechende Nachrichten MT 096 und MT 097) in Region 2 verbucht, während alle nicht zusammengehörenden Nachrichten in Region 2 in eine Warteschlange gestellt werden. Zusammengehörende FIN-Nachrichten, die in Region 1 als final eingestuft wurden, jedoch aufgrund der fehlenden Erfassung nicht in Region 2 verbucht werden konnten, werden als neu ausstehende Zahlungen („newly pending payments“) angezeigt. Der SSP Service Desk kennzeichnet alle ausstehenden Zahlungen als sehr dringend („highly urgent“) und stellt sie ganz vorne in die Warteschlange der sehr dringenden Zahlungen ein.

2) Der SSP Service Desk informiert den TARGET Services Coordination Desk über die Beendigung des vorangegangenen Schritts.

3) Zur Synchronisierung des Umsatzes und der Salden zwischen PM-Konten und T2S-Geldkonten stimmt der TARGET Services Coordination Desk die Positionen auf beiden Euro-Zwischenkonten

ab und identifiziert die fehlenden Zahlungen (die im TARGET2-Zwischenkonto auf der T2S-Plattform verarbeitet wurden und im T2S-Zwischenkonto auf der SSP fehlen).[88]

Nach Durchführung der Identifizierung informiert der TARGET Services Coordination Desk die Zentralbanken über die fehlenden Liquiditätsübertragungen; jene sollten ihrerseits die betroffenen Teilnehmer über die beeinträchtigten Liquiditätsübertragungen sowie über die zu ergreifenden Maßnahmen unterrichten.

Folgende Schritte sind denkbar:

- Bei **Liquiditätsübertragungen von PM-Konten auf T2S-Geldkonten**, die auf T2S und der SSP (Region 1) vor dem Katastrophenfall, jedoch nicht auf der SSP (Region 2) nach dem Katastrophenfall gebucht wurden, wird die für den Inhaber des belasteten PM-Kontos zuständige Zentralbank das betreffende PM-Konto belasten und die Gutschrift nach Autorisierung durch den PM-Geldkontoinhaber auf das T2S-Zwischenkonto vornehmen. Hat sich der Inhaber des PM-Kontos für Anzeigen der Kontobelastungen entschieden, sollte die Nachricht im Zusammenhang mit der erneuten Buchung über den vorherigen Schritt ignoriert werden.

- Bei **Liquiditätsübertragungen von T2S-Geldkonten auf PM-Konten**, die in T2S und auf der SSP (Region 1) vor dem Katastrophenfall, jedoch nicht in der SSP (Region 2) nach dem Katastrophenfall gebucht wurden, wird die für das belastete T2S-Geldkonto zuständige Zentralbank die ausgehenden liquiditätsübertragungsbezogenen Nachrichten ermitteln und sie erneut senden (über GUI Screen Cash > Liquidity > Immediate Liquidity Transfers > Search/List Screen > Related Outbound Messages > Resend). Falls sich der Inhaber des PM-Kontos für Gutschriftsanzeigen entschieden hat, sollte die Nachricht zu der über den vorangegangenen Schritt erneut erfolgten Buchung ignoriert werden.

- Bei **Liquiditätsübertragungen von PM-Konten auf TIPS-Geldkonten**, die auf TIPS und der SSP (Region 1) vor dem Katastrophenfall, jedoch nicht auf der SSP (Region 2) nach dem Katastrophenfall gebucht wurden, wird die für den Inhaber des belasteten PM-Kontos zuständige Zentralbank das betreffende PM-Konto belasten und die Gutschrift nach Autorisierung durch den PM-Geldkontoinhaber auf das TIPS-Zwischenkonto vornehmen. Hat sich der Inhaber des PM-Kontos für Anzeigen der Kontobelastungen entschieden, sollte die Nachricht im Zusammenhang mit der erneuten Buchung über den vorherigen Schritt ignoriert werden.

88 TARGET2 und T2S sollten den Geschäftstag nicht abschließen, bevor nicht die Zwischenkonten synchronisiert wurden. Doch am Tagesende könnte T2S, falls die Salden der T2S-Geldkonten bei null stehen, die Selbstbesicherung zurückbezahlt ist und die TARGET2-Zwischenkonten null betragen, den Geschäftstag abschließen, selbst wenn die SSP nach einem Katastrophenfall vor einem Neustart steht. Dabei sollte aber sichergestellt werden, dass zuvor alle erforderlichen Nachrichten von T2S erneut an die SSP gesendet werden (die Nachrichten sollten in die Warteschlange gestellt und dann von der SSP verarbeitet werden).

- Bei **Liquiditätsübertragungen von TIPS-Geldkonten auf PM-Konten**, die in TIPS und auf der SSP (Region 1) vor dem Katastrophenfall, jedoch nicht in der SSP (Region 2) nach dem Katastrophenfall gebucht wurden, wird die für das belastete TIPS-Geldkonto zuständige Zentralbank die ausgehenden liquiditätsübertragungsbezogenen Nachrichten ermitteln und sie erneut senden. Falls sich der Inhaber des PM-Kontos für Gutschriftsanzeigen entschieden hat, sollte die Nachricht zu der über den vorangegangenen Schritt erneut erfolgten Buchung ignoriert werden.

Die vorgenannten Schritte sollten innerhalb von zwei Stunden nach dem Beschluss einer Ausfallsicherung abgeschlossen sein.

4) Nach Beendigung der vorherigen Schritte sollte eine Telefonkonferenz der TARGET2-Settlement-Manager abgehalten werden, um sich über die Initiierung des erneuten Versands der InterAct- und FileAct-Nachrichten (die rund 20 % des fehlenden Nachrichtenverkehrs ausmachen) abzustimmen. Der SSP Service Desk öffnet die Gemeinschaftsplattform für SWIFTNet-Dienste, also FileAct und InterAct.

5) Die Nebensysteme sollten sämtliche innerhalb zehn Minuten vor der Störung in Region 1 versendeten FileAct-Nachrichten, bzw. die vom Nebensystem als fehlend identifizierten Dateien, mit demselben Betreff erneut verschicken. Des Weiteren müssen die Nebensysteme, Banken und Zentralbanken ihren InterAct-Nachrichtenverkehr der letzten beiden Minuten vor dem Vorfall wiederholen (außer bei Nachrichten in Verbindung mit Liquiditätsübertragungen an/von T2S-Geldkonten). Neue FileAct- und InterAct-Nachrichten sollten hingegen nicht versendet werden. Durch die Öffnung der Gemeinschaftsplattform für SWIFTNet erhalten die Teilnehmer auch Zugang zum Informations- und Steuerungsmodul (ICM), um den Bearbeitungsstatus zu prüfen.

6) Durch die Bearbeitung der fehlenden FileAct- und InterAct-Nachrichten dürften sich die neu ausstehenden Zahlungen („newly pending payments“) weiter verringern. Alle verbleibenden neu ausstehenden Zahlungen sollten von den Zentralbanken „forciert“ werden; hierdurch wird bestätigt, dass diese Zahlungen in Region 1 final waren und in Region 2 final bleiben sollten. Auf diese Weise würde jedes sich daraus ergebende Restrisiko beim Eurosystem liegen. Entsprechend sollten alle verbleibenden neu ausstehenden AS-Transaktionen, die in Region 1 final waren, in Region 2 final bleiben und daher „forciert“ werden. Um die Existenz „neu ausstehender AS-Transaktionen“ anzuzeigen, müsste das Nebensystem Belege an die entsprechende Zentralbank liefern, wonach diese Transaktionen in Region 1 final waren (z. B. eine Kopie der erhaltenen Benachrichtigung).

7) Nachdem der SSP Service Desk dem TARGET Services Coordination Desk bestätigt hat, dass alle neu ausstehenden Zahlungen abgewickelt wurden, wird eine Telefonkonferenz zwischen den Krisenmanagern abgehalten, um deren Zustimmung zur Öffnung der Gemeinschaftsplattform für FIN-Nachrichten zu erhalten. Alle in der Warteschlange stehenden FIN-Zahlungen werden

abgewickelt. Dann können die Nutzer auch neue FileAct- und InterAct-Nachrichten senden. Wurde ECONS I genutzt, dann findet der Saldenübertrag für SWIFTNet FIN-Nachrichten von ECONS I zum PM nach Schließung von ECONS I und nach Öffnung der Gemeinschaftsplattform statt.

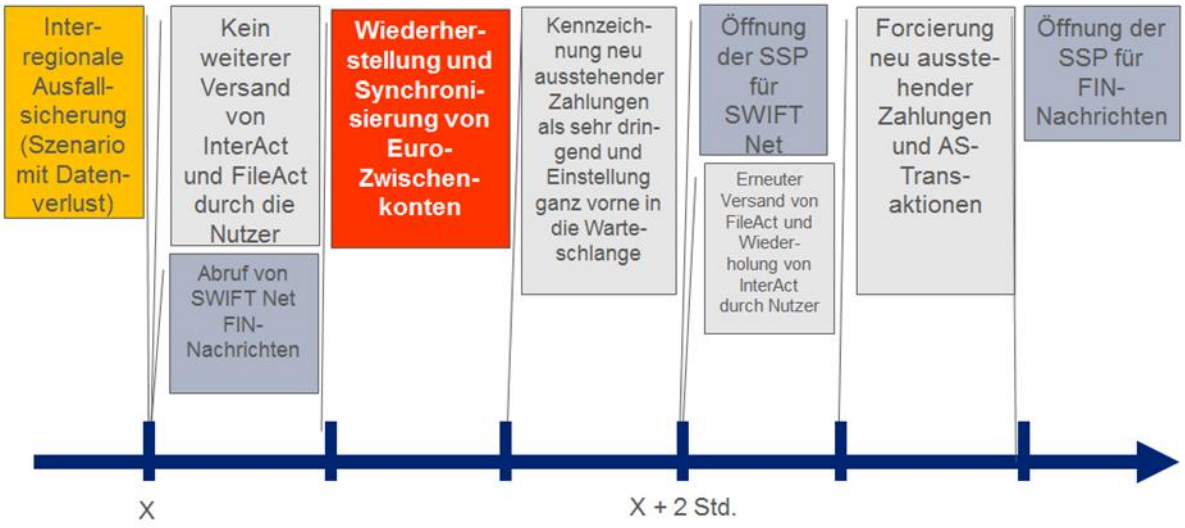


Abbildung 26: Abläufe nach einer interregionalen Ausfallsicherung mit Datenverlust

Anhang II Störungsbericht für TARGET2-Nutzer

Vertraulichkeit Die in diesem Dokument enthaltenen Informationen werden vom Eurosystem ausschließlich dazu verwendet, die Ausfallsicherheit des TARGET2-Systems insgesamt zu erhöhen. Innerhalb des Eurosystems werden diese Informationen nur an Personen weitergegeben, die sie aus dienstlichen Gründen benötigen.

Name der verantwortlichen Zentralbank:	

Angaben zu den Ansprechpartnern	
Name des TARGET2-Nutzers:	
Name des Ansprechpartners:	
Titel/Funktion:	
Telefonnummer:	
E-Mail-Adresse:	

Grundsätzliche Angaben zum Vorfall	
Identifikationsnummer des Vorfalls (wird von der verantwortlichen Zentralbank vergeben):	CC/JJJJMMTT/Nr.

Status:	☐ Vorläufig	☐ Final[1]
Art der fehlerhaften Komponente:	☐ Hardware ☐ Netzwerk[3] ☐ Menschliches Versagen	☐ Software[2] ☐ Infrastruktur[4]
Datum und Uhrzeit des Störungsbeginns (MEZ):	ttmmjjjj / ss.mm	
Datum und Uhrzeit des Störungsendes (MEZ):	ttmmjjjj / ss.mm	
Dauer:	ss.mm	

Beschreibung des Vorfalls (Die Zusammenfassung sollte möglichst allgemeinsprachlich auf eine für die Unternehmensleitung angemessene Art verfasst werden. Die Zusammenfassung sollte beispielsweise folgende Elemente enthalten: • eine allgemeine Beschreibung des Vorfalls und seiner Auswirkungen, • die betroffenen Dienstleistungen bzw. Systeme und • die externen Auswirkungen (z. B. andere betroffene TARGET2-Nutzer)

Einzelheiten zur Störungsursache (insbesondere zur Kernursache des Vorfalls (wer, was, wo, wann, wie?))

Abhilfemaßnahmen (dieser Abschnitt sollte Punkte enthalten wie z. B.: • Maßnahmen zur Behebung des Vorfalls und • Maßnahmen zur Verhinderung einer Wiederholung des Vorfalls (Umsetzung geplant bis…))

1 Ein Störungsbericht gilt als „final“, wenn das Umsetzungsdatum der Abhilfemaßnahme angezeigt wird.

2 Software bezieht sich auf Systemsoftware (einschließlich Datenbanksystemen) und Anwendersoftware.

3 Dies betrifft lediglich das interne Netzwerk. Ausfälle des externen Netzwerks sind unter Infrastruktur aufzuführen.

4 Die Infrastruktur umfasst Grundstücke und Gebäude sowie unterstützende Dienstleistungen (wie Klimatisierung, Stromversorgung, Telekommunikation (einschließlich SWIFT)).

_____

Datum und Unterschrift

Name des Unterzeichners (in Druckbuchstaben):

Titel:

Dieses Formular ist an die oben genannte Zentralbank zurückzusenden:

Anschrift:	
Kontaktperson:	

Anhang III Selbstzertifizierungserklärung

Einleitung

Der Ausschuss für Zahlungsverkehr und Marktinfrastrukturen (Committee on Payments and Market Infrastructures – CPMI) und die Internationale Organisation der Wertpapieraufsichtsbehörden (International Organization of Securities Commissions – IOSCO) geben Prinzipien für Finanzmarktinfrastrukturen (PFMI)[5] heraus. Darin werden den Betreibern von Zahlungssystemen bestimmte Verantwortlichkeiten zugewiesen, denen sie nachkommen müssen. So bezieht sich etwa das Prinzip 17 auf Aspekte im Zusammenhang mit der Sicherheit und der Zuverlässigkeit des Betriebs von Finanzmarktinfrastrukturen wie beispielsweise systemrelevanten Zahlungssystemen.

Um die Betriebsrisiken im Zusammenhang mit den Teilnehmern zu steuern, besagt Prinzip 17, dass „*eine FMI für ihre Teilnehmer die Einführung von betrieblichen Mindestanforderungen erwägen sollte. So könnte eine FMI je nach Rolle und Systemrelevanz eines Teilnehmers Betriebs- und Business-Continuity-Anforderungen für ihre Teilnehmer definieren.*" Die Anforderungen haben zum Ziel, potenzielle teilnehmerbedingte betriebliche Schwachstellen für die FMI zu beseitigen und im Einklang mit der entsprechenden CPMI-Strategie das mit der Endpunktsicherheit zusammenhängende Betrugsrisiko bei Großbetragszahlungen zu verringern.[6]

Vor diesem Hintergrund hat das Eurosystem in seiner Funktion als Betreiber des TARGET2-Systems eine Reihe von Anforderungen zum Umgang mit Risiken für die Informationssicherheit und Cyberresilienz[7] erarbeitet, die alle direkten TARGET2-Teilnehmer (Zentralbanken, kritische und nichtkritische Teilnehmer/Nebensysteme) unter Berücksichtigung ihrer internen Systeme im Zusammenhang mit der in diesem Dokument definierten Zahlungstransaktionskette (Payment Transaction Chain – PTC) erfüllen müssen. Darüber hinaus wurde festgelegt, dass TARGET2-Teilnehmer, die Zugang zu ihrem PM-Konto ermöglichen [über eine indirekte Teilnahme, erreichbare BIC-Inhaber oder einen Multi-Adressaten-Zugang] das Risiko, das durch eine solche (indirekte) Teilnahme entsteht, steuern und dass sie die ihnen auferlegten Sicherheitsanforderungen somit erfüllen.

Außerdem hat das Eurosystem eine Reihe von Anforderungen definiert, die das Business-Continuity-Risiko reduzieren sollen und ausschließlich für die internen Systeme von Teilnehmern gelten, die laut den Regeln des TARGET2-Leitfadens als kritisch eingestuft wurden. Alle Teilnehmer müssen im Rahmen einer Selbstzertifizierung dokumentieren, inwieweit sie die nachstehenden Anforderungen umsetzen.

---

5 Eine umfassende Beschreibung der internationalen Standards für Finanzmarktinfrastrukturen ist auf der Website der BIZ abrufbar: https://www.bis.org/cpmi/info_pfmi.htm.

6 Eine vollständige Beschreibung der CPMI-Strategie zur Verringerung des mit der Endpunktsicherheit zusammenhängenden Betrugsrisikos bei Großbetragszahlungen findet sich in dem Bericht „Reducing the risk of wholesale payments fraud related to endpoint security" auf der Website der BIZ: https://www.bis.org/cpmi/publ/d178.htm.

7 Gemäß CPMI-IOSCO „Guidance on Cyber Resilience for Financial Market Infrastructures" vom Juni 2016 ist Cyberresilienz als die Fähigkeit eines FMI definiert, Cyberangriffe zu antizipieren, abzuwehren und zu begrenzen sowie den Betrieb nach einem Cyberangriff rasch wiederherzustellen.

Anforderungen zum Informationssicherheits- und Business-Continuity-Management

Informationssicherheitsmanagement (gilt für alle Teilnehmer)

Das Set-up der internen Systeme (Back-Office-Systeme, Front-Office-Systeme, Middleware, interne Netzwerke und Infrastruktur für die Anbindung an externe Netzwerke), die von den Teilnehmern zur Vornahme von Transaktionen in TARGET2 verwendet werden kann wegen verschiedener Architekturen zur Anbindung an TARGET2 sehr unterschiedlich aussehen.

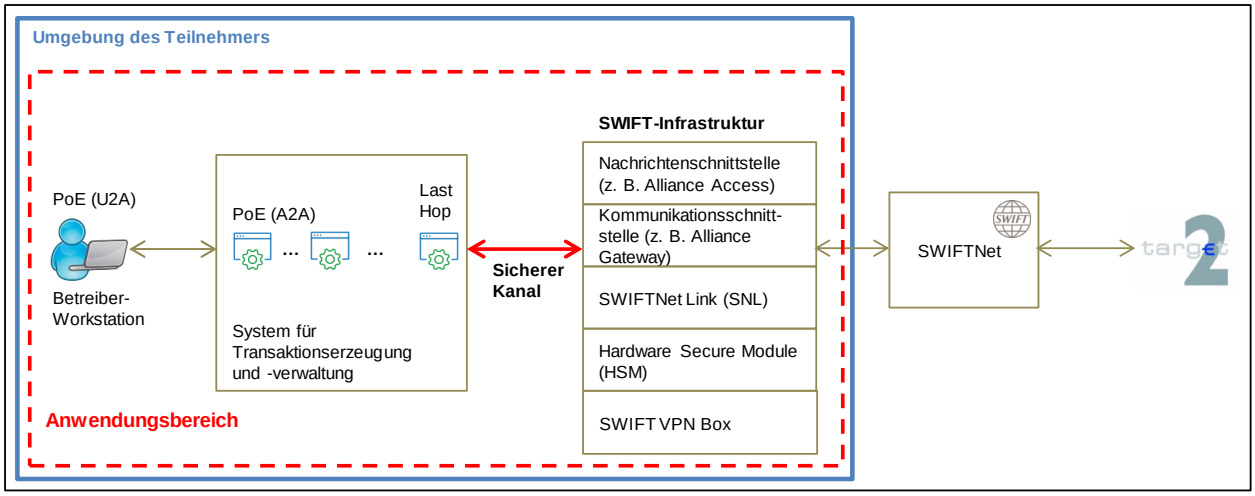
Folglich kann auch der Anwendungsbereich der Sicherheitsanforderungen aufgrund der vom Teilnehmer implementierten spezifischen Architektur variieren. Zur Festlegung des Anwendungsbereichs sollte der Teilnehmer die Bestandteile der Zahlungstransaktionskette identifizieren. Konkret beginnt diese an einem Point of Entry (PoE), d. h. einem in die Erzeugung von Transaktionen involvierten System (z. B. Workstations, Front-Office- und Back-Office-Anwendungen, Middleware) und endet bei dem System, das für die Übermittlung der Nachricht an SWIFT zuständig ist (z. B. SWIFT VPN Box), bzw. im Internet (sofern ein internetbasierter Zugang besteht).

Es bleibt den einzelnen Organisationen überlassen, zu beurteilen, ob alle oder nur ein Teil der Sicherheitsanforderungen für sie gelten. Der Wortlaut in der englischen Originalfassung der Anforderungen richtet sich nach der im Standard ISO/IEC 27000:2018(en) verwendeten Terminologie.

Zu Anschauungszwecken werden nachfolgend drei mögliche Architekturen mit Hinweis auf die jeweiligen Zahlungstransaktionskette und möglichen PoEs beschrieben.

Teilnehmer mit SWIFT-Infrastruktur innerhalb der eigenen Umgebung

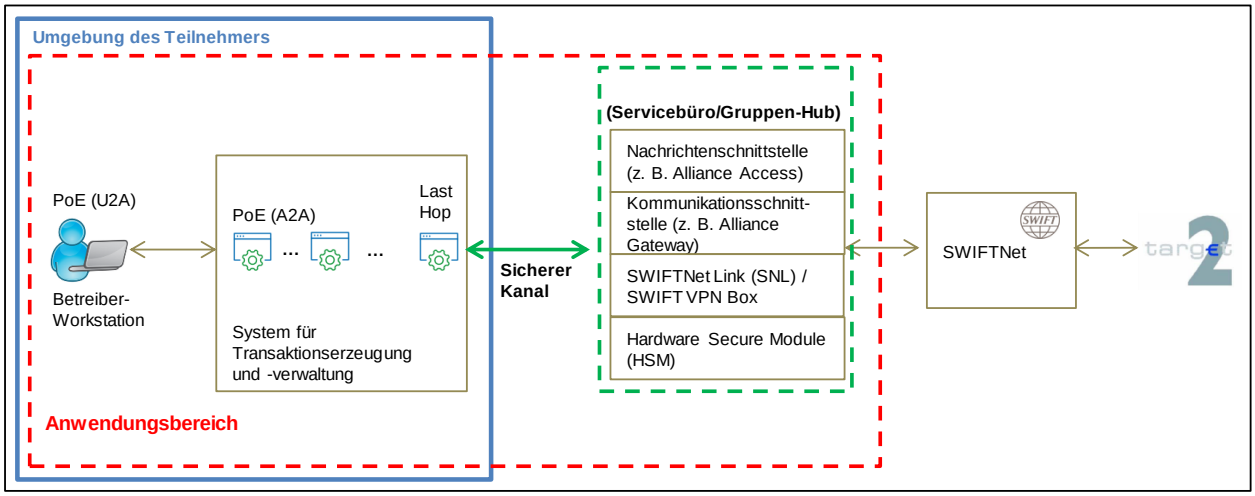
Die zur Anbindung an TARGET2 verwendete SWIFT-Infrastruktur befindet sich innerhalb der Umgebung des Teilnehmers (siehe Abbildung).



Der Anwendungsbereich umfasst: a) die vom Betreiber verwendete Workstation, b) die für die Erzeugung oder Verwaltung von Transaktionen zuständigen Systeme (z. B. Middleware, Front-Office- und Back-Office-Anwendungen), c) den sicheren Kanal zwischen der SWIFT-Infrastruktur und dem letzten Teilstück (Last Hop), d) die SWIFT-Infrastruktur und e) die physische Umgebung des Teilnehmers.

Teilnehmer mit Anbindung über ein SWIFT- Servicebüro oder einen Gruppen-Hub

Da keine Komponente der SWIFT-Infrastruktur in der Umgebung des Teilnehmers angesiedelt ist, kommunizieren Middleware und Back-Office-Anwendungen direkt mit dem *SWIFT-Servicebüro oder dem Gruppen-Hub* und nutzen hierfür einen von diesem bereitgestellten sicheren Kanal (z. B. GUI-Anwendung, Middleware-Produkt).



Der Anwendungsbereich umfasst: a) die vom Betreiber verwendete Workstation, b) die für die Erzeugung oder Verwaltung von Transaktionen zuständigen Systeme (z. B. Middleware, Front-Office- und Back-Office-Anwendungen), c) den sicheren Kanal zwischen der SWIFT-Infrastruktur (diese ist im vorliegenden Beispiel beim SWIFT-Servicebüro oder beim Gruppen-Hub angesiedelt) und dem letzten Teilstück, und d) die physische Umgebung des Teilnehmers.

Einige der geltenden Sicherheitsanforderungen können vom *SWIFT-Servicebüro oder dem Gruppen-Hub* abgedeckt werden. Die Unterzeichner der Selbstzertifizierungserklärung bleiben jedoch weiterhin für die Einhaltung der Sicherheitsanforderungen verantwortlich, d. h., sie müssen dafür Sorge tragen, dass diese Anforderungen „in ihrem Namen“ erfüllt werden. Allgemein müssen die TARGET2-Teilnehmer sicherstellen, dass ihre unterzeichnete Selbstzertifizierungserklärung ein zutreffendes und genaues Bild der Sicherheitslage ihrer Organisation vermittelt; dies schließt auch extern erbrachte Dienstleistungen ein.

Bei international tätigen Kreditinstituten kann die für die Anbindung an TARGET2 verwendete Infrastruktur bei der Zentrale angesiedelt sein und dort betrieben werden und dann von mehreren lokalen Zweigstellen innerhalb eines bestimmten Gruppen-Hubs genutzt werden.

In diesem Fall gilt für die Zentrale der Anwendungsbereich, der unter „*Teilnehmer mit SWIFT-Infrastruktur innerhalb der eigenen Umgebung*“ genannt ist. Dennoch sind einige Sicherheitsanforderungen auch für die lokalen Zweigstellen relevant .[8] Beispielsweise sind Kontrollen der physischen Sicherheit sowohl von dem TARGET2-Teilnehmer, bei dem die gemeinsame technische Infrastruktur angesiedelt ist, als auch von den Zweigstellen zu erfüllen. Der TARGET2-Teilnehmer, bei dem die gemeinsame technische Infrastruktur angesiedelt ist, muss Kontrollen zum Schutz des Rechenzentrums durchführen, während die Zweigstellen dafür Sorge zu tragen haben, dass die für die Anbindung an die gemeinsame technische Infrastruktur verwendeten Komponenten (z. B. die vom Betreiber verwendete Workstation) angemessen geschützt sind.

Auch für TARGET2-Teilnehmer, die ein *SWIFT-Servicebüro* in Anspruch nehmen, gilt der gleiche Grundsatz: sie müssen nach wie vor beurteilen, welche Kontrollen in ihren Anwendungsbereich fallen und welche nicht (und gegebenenfalls sicherstellen, dass das jeweilige SWIFT-Servicebüro diese Anforderungen erfüllt).

Teilnehmer mit TARGET2-Anbindung über das Internet

Der Teilnehmer verbindet sich über das Internet mit TARGET2 und verwendet für die Authentifizierung und Signierung von Transaktionen ein auf einem USB-Token gespeichertes Zertifikat.

[8] Diese Regeln und dieser Anwendungsbereich gelten auch, wenn die zur Anbindung an TARGET2 verwendete technische Infrastruktur von einer Zentrale mit Sitz außerhalb des EWR gemanaged wird.

Der Anwendungsbereich umfasst: a) die vom Betreiber verwendete Workstation und b) die physische Umgebung des Teilnehmers.

Anforderung 1.1: Informationssicherheitspolitik

Die Geschäftsführung legt einen klaren sicherheitspolitischen Kurs fest, der im Einklang mit den Geschäftszielen steht. Sie verpflichtet sich zur Informationssicherheit und fördert diese, indem sie eine Strategie für die Informationssicherheit formuliert, verabschiedet und aufrechterhält, die darauf abzielt, die Informationssicherheit und die Cyberresilienz innerhalb der gesamten Organisation in Bezug auf Identifikation, Bewertung und Behandlung von Risiken bei der Informationssicherheit und Cyberresilienz zu managen. Die Strategie sollte mindestens folgende Abschnitte beinhalten: Ziele, Umfang (darunter Bereiche wie Organisation, Personal, Verwaltung der Informationswerte etc.), Grundsätze und Zuweisung von Verantwortlichkeiten.

Anforderung 1.2: Interne Organisation

Zur Umsetzung der Informationssicherheitsstrategie innerhalb der Organisation ist ein Informationssicherheitsrahmenwerk zu schaffen. Die Geschäftsführung hat die Einrichtung des Informationssicherheitsrahmenwerks zu koordinieren und überprüfen, damit die organisationsweite Umsetzung der Informationssicherheitspolitik (gemäß Anforderung 1.1) gewährleistet ist. Hierzu zählt auch die Zuteilung ausreichender Ressourcen und die Zuweisung entsprechender Sicherheitsverantwortlichkeiten.

Anforderung 1.3: Externe Parteien

Wenn eine Organisation mit externen Parteien zusammenarbeitet bzw. deren Produkte oder Dienstleistungen in Anspruch nimmt und/oder von diesen abhängig ist, sollte dies nicht die Sicherheit der Informationen und der informationsverarbeitenden Einrichtungen beeinträchtigen. Der Zugang externer Parteien zu den informationsverarbeitenden Einrichtungen der Organisation ist in jedem Fall zu kontrollieren. Sofern externe Parteien oder Produkte und Dienstleistungen externer Parteien auf die informationsverarbeitenden Einrichtungen zugreifen müssen, muss eine Risikoprüfung erfolgen, um die sicherheitsrelevanten Auswirkungen zu ermitteln und die Kontrollanforderungen zu bestimmen. Die Kontrollen sind mit der externen Partei jeweils einzeln zu vereinbaren und vertraglich festzulegen.

Anforderung 1.4: Verwaltung von Informationswerten

Sämtliche Informationswerte, Geschäftsprozesse und zugrundeliegenden Informationssysteme (wie Betriebssysteme, Infrastrukturen, Fachsoftware, Standardprodukte, Dienste und von Nutzern entwickelte Anwendungen) der Zahlungstransaktionskette sind zu erfassen und einem Eigentümer namentlich zuzuordnen. Zum Schutz der Informationswerte ist zudem festzulegen, wer für die Aufrechterhaltung und die Durchführung angemessener Kontrollen in den Geschäftsprozessen und den zugehörigen IT-Komponenten zuständig ist. **ANMERKUNG:** Der Eigentümer kann, soweit angemessen, die Durchführung bestimmter Kontrollen delegieren. Er ist jedoch weiterhin verantwortlich, was den ordnungsgemäßen Schutz der Informationswerte betrifft.

Anforderung 1.5: Klassifizierung von Informationswerten

Die Informationswerte sind nach ihrer Kritikalität für den reibungslosen Betrieb durch den Teilnehmer zu klassifizieren. Aus der Klassifizierung muss ersichtlich sein, ob, mit welcher Priorität und in welchem Umfang die Informationswerte zu schützen sind, während sie in den jeweiligen Geschäftsprozessen verwendet werden. Hierbei sind auch die zugrunde liegenden IT-Komponenten zu berücksichtigen. Mithilfe eines von der Geschäftsführung genehmigten Systems zur Klassifizierung von Informationswerten werden für die gesamte Lebensdauer eines Informationswerts (einschließlich Löschung und Vernichtung) angemessene Schutzkontrollen definiert und die Notwendigkeit spezieller Maßnahmen im Umgang mit bestimmten Informationen kommuniziert.

Anforderung 1.6: Personelle Sicherheit

Die Verantwortlichkeiten bezüglich der Sicherheit werden bereits vor der Einstellung neuer Mitarbeiter in einer entsprechenden Stellenbeschreibung benannt und in den jeweils geltenden vertraglichen Bedingungen festgehalten. Alle Bewerber, Vertragspartner und Dritte sind hinreichend zu überprüfen, besonders bei sensiblen Stellen bzw. Aufträgen. Mitarbeiter, Vertragspartner und Dritte, die informationsverarbeitende Einrichtungen nutzen, müssen eine Vereinbarung unterzeichnen, in der ihre Sicherheitsrollen und Verantwortlichkeiten festgelegt sind. Es wird gewährleistet, dass alle Mitarbeiter, Vertragspartner und Dritte hinreichend für den Sicherheitsaspekt sensibilisiert sind. Zur Minimierung möglicher Sicherheitsrisiken sind ihnen Fortbildungen und Schulungen zu Sicherheitsverfahren und dem korrekten Einsatz der informationsverarbeitenden Einrichtungen zu ermöglichen. Es ist ein formelles Disziplinarverfahren für Mitarbeiter zu schaffen, das bei Verletzung von Sicherheitsbestimmungen zur Anwendung kommt. Das Ausscheiden eines Mitarbeiters, Vertragspartners oder Dritten bzw. dessen Wechsel innerhalb der Organisation muss durch Zuweisung entsprechender Verantwortlichkeiten im Hinblick auf etwaige Sicherheitsaspekte gesteuert werden, und es ist zu gewährleisten, dass sämtliche Betriebsmittel zurückgegeben und alle Zugangsberechtigungen entzogen werden.

Anforderung 1.7: Physische und umgebungsbezogene Sicherheit

Kritische oder sensible informationsverarbeitende Einrichtungen sind in Sicherheitsbereichen unterzubringen, die durch eine genau festgelegte Sicherheitszone sowie entsprechende Sicherheitsbarrieren und Zutrittskontrollen geschützt sind. Sie müssen physisch vor unrechtmäßigem Zutritt sowie Zerstörung und Manipulation geschützt sein. Der Zutritt ist nur Personen zu gewähren, die unter die Anforderung 1.6 fallen. Es sind Verfahren und Standards zu etablieren, um physische Medien, auf denen Informationswerte gespeichert sind, auf Transportwegen zu schützen.

Die Betriebsmittel sind vor physischen und umgebungsbezogenen Bedrohungen zu schützen. Um das Risiko eines unerlaubten Zugriffs auf Informationen zu mindern sowie Schäden an und Verluste von Betriebsmitteln und Informationen zu verhindern, ist es erforderlich, dass sämtliche (auch außerhalb des Standorts verwendeten) Betriebsmittel geschützt und Vorkehrungen zum Schutz vor Entwendung von Eigentum getroffen werden. Zur Abwehr physischer Bedrohungen und zum Schutz der unterstützenden

Infrastruktur wie der Stromversorgung und der Verkabelung können Sondermaßnahmen erforderlich sein.

Anforderung 1.8: Betriebsmanagement

Für die Verwaltung und den Betrieb von informationsverarbeitenden Einrichtungen, die durchgängig alle zugrunde liegenden Systeme der Zahlungstransaktionskette abdecken, sind Verantwortlichkeiten und Verfahren festzulegen.

Was die Betriebsprozesse einschließlich der technischen Administration der IT-Systeme betrifft, so ist gegebenenfalls eine Aufteilung der Verantwortlichkeiten vorzunehmen, um das Risiko eines fahrlässigen oder vorsätzlichen Systemmissbrauchs zu verringern. Ist eine solche Aufteilung aus dokumentierten objektiven Gründen nicht möglich, sind kompensierende Kontrollen im Anschluss an eine formale Risikoanalyse zu implementieren. Es müssen Kontrollen eingerichtet werden, um das Eindringen von Schadsoftware (Malware) in die Systeme der Zahlungstransaktionskette zu verhindern und aufzudecken. Außerdem müssen Kontrollen (inkl. der Nutzersensibilisierung) etabliert werden, um Malware abzuwehren, aufzuspüren und zu entfernen. Mobiler Programmcode darf nur verwendet werden, wenn er aus vertrauenswürdigen Quellen stammt (z. B. signierte COM-Komponenten von Microsoft sowie Java Applets). Die Browsereinstellungen (z. B. Verwendung von Erweiterungen und Plug-ins) sind strengen Kontrollen zu unterziehen.

Die Geschäftsführung hat Strategien zur Datensicherung und -wiederherstellung zu implementieren. Zu den Strategien zur Datenwiederherstellung zählt auch ein Wiederherstellungsplan, der in regelmäßigen Abständen, jedoch mindestens jährlich, zu testen ist.

Zudem sind die für die Sicherheit des Zahlungsverkehrs kritischen Systeme zu überwachen und die Informationssicherheit ist zu dokumentieren. Durch den Einsatz von Betreiberprotokollen ist sicherzustellen, dass Probleme im Bereich der Informationssysteme erkannt werden. Die Betreiberprotokolle sind in regelmäßigen Abständen – je nach der Kritikalität des Betriebsprozesses – stichprobenartig zu überprüfen. Eine Systemüberwachung ist durchzuführen, um die Effizienz der als kritisch für die Sicherheit des Zahlungsverkehrs eingestuften Kontrollmechanismen zu überprüfen und die Einhaltung der Zugangsregelungen zu verifizieren.

Der Informationsaustausch zwischen Organisationen muss auf Basis einer formellen Austauschrichtlinie im Rahmen von zwischen den betroffenen Parteien geschlossenen Austauschvereinbarungen erfolgen. Hierbei sind die einschlägigen Rechtsvorschriften einzuhalten. Werden Software-Komponenten von Dritten im Informationsaustausch mit TARGET2 verwendet (z. B. wenn wie im oben beschriebenen zweiten Anforderungsszenario des Anhangs zur TARGET2-Selbstzertifizierung Software von einem Servicebüro bezogen wird), so muss hierfür eine formale Vereinbarung mit dem Dritten geschlossen werden.

Anforderung 1.9: Zugangskontrolle

Der Zugang zu Informationswerten ist durch die fachlichen Anforderungen („Kenntnis nur soweit nötig“[9]) und im Einklang mit den bestehenden internen Richtlinien der Organisation (einschließlich der Informationssicherheitsstrategie) zu begründen. Es sind eindeutige Regeln für die Zugriffskontrolle auf Basis des Prinzips der minimalen Rechtevergabe[10] festzulegen, die die Erfordernisse des jeweiligen Geschäftszwecks und der IT-Prozesse exakt widerspiegeln. Soweit relevant (z. B. zur Backup-Verwaltung), müssen die logischen mit den physischen Zugriffskontrollen übereinstimmen, es sei denn, es bestehen adäquate Ausgleichskontrollen (z. B. Verschlüsselung, Anonymisierung personenbezogener Daten).

Um die Zuweisung von Rechten zum Zugriff auf Informationssysteme und -dienste der Zahlungstransaktionskette zu kontrollieren, müssen formelle, dokumentierte Verfahren etabliert werden. Diese Verfahren müssen den gesamten Lebenszyklus des Nutzerzugangs abdecken – angefangen von der Erstregistrierung neuer Nutzer bis hin zur endgültigen Abmeldung von Nutzern, die keinen Zugang mehr benötigen.

Besondere Beachtung erfordert gegebenenfalls die Zuweisung von Zugriffsrechten, die so kritisch sind, dass der Missbrauch dieser Zugriffsrechte zu einer schwerwiegenden Beeinträchtigung der betrieblichen Prozesse des Teilnehmers führen kann (z. B. Zugriffsrechte, die die Systemadministration, das Umgehen von Systemkontrollen oder den direkte Zugriff auf Geschäftsdaten ermöglichen).

Es müssen angemessene Kontrollen eingerichtet werden, um die Nutzer an bestimmten Punkten des Netzwerks der Organisation, beispielsweise für den lokalen oder Fernzugang auf Systeme der Zahlungstransaktionskette, zu identifizieren, zu authentifizieren und zu berechtigen. Um die Zurechenbarkeit zu gewährleisten, dürfen persönliche Konten nicht geteilt werden.

Passwörter dürfen nicht einfach zu erraten sein. Deshalb müssen Regeln (z. B. hinsichtlich der Komplexität und zeitlich begrenzten Gültigkeit) festgelegt und durch spezielle Kontrollen durchgesetzt werden. Es ist ein Protokoll für die sichere Wiederherstellung bzw. Zurücksetzung von Passwörtern aufzustellen.

Es muss eine Leitlinie zur Anwendung kryptografischer Kontrollen entwickelt und umgesetzt werden, um die Vertraulichkeit, Authentizität und Integrität von Informationen zu schützen. Zur Unterstützung derartiger Verfahren muss die Verwaltung kryptografischer Schlüssel geregelt sein.

Ebenso sind Regelungen für das Lesen vertraulicher Informationen am Bildschirm oder auf Papier zu treffen, z. B. durch eine Strategie des aufgeräumten Schreibtisches (Clear Desk Policy) oder leeren Bildschirms (Clear Screen Policy), um das Risiko eines unberechtigten Zugriffs zu reduzieren.

[9] Der Grundsatz „Kenntnis nur soweit nötig“ bezieht sich auf die Identifikation der Gesamtheit derjenigen Informationen, auf die eine einzelne Person Zugriff haben muss, um ihre Aufgaben zu erledigen.

[10] Der Grundsatz der minimalen Rechtevergabe bezieht sich auf den Zuschnitt des Zugriffs einer Person auf IT-Systeme derart, dass dieser ihrer fachlichen Zuständigkeit entspricht.

Im Falle des Arbeitens im Homeoffice muss das Risiko, das mit der Arbeit in einer ungeschützten Umgebung einhergeht, berücksichtigt werden, und es sind angemessene technische und organisatorische Kontrollen einzurichten.

Anforderung 1.10: Beschaffung, Entwicklung und Wartung von Informationssystemen

Vor der Entwicklung und/oder Implementierung von Informationssystemen sind die Sicherheitsanforderungen zu ermitteln und zu vereinbaren.

Zur Gewährleistung einer korrekten Verarbeitung müssen geeignete Kontrollen in die Anwendungen integriert werden, auch in solche, die von Nutzern entwickelt wurden. Die Validierung von Ein- und Ausgabedaten und intern verarbeiteten Daten ist Bestandteil dieser Kontrollen. Zusätzliche Kontrollen sind eventuell für Systeme erforderlich, die sensible, wertvolle oder kritische Informationen verarbeiten oder diese beeinflussen. Solche Kontrollen sind auf Basis der Sicherheitsanforderungen und einer Risikoeinschätzung in Übereinstimmung mit den bestehenden Leitlinien (z. B. der Informationssicherheitsstrategie und der Leitlinie für kryptografische Kontrollen) zu bestimmen.

Die betrieblichen Anforderungen an neue Systeme sind festzulegen, zu dokumentieren und vor ihrer Abnahme und Verwendung zu testen. Es müssen geeignete Kontrollen zur Gewährleistung der Netzwerksicherheit, einschließlich Segmentierung und sicherer Verwaltung, implementiert werden. Dies sollte in Abhängigkeit von der Kritikalität der Datenströme und vom Risikograd der Netzwerkbereiche in der Organisation erfolgen. Zum Schutz sensibler Daten, die über öffentliche Netzwerke geleitet werden, sind spezifische Kontrollmechanismen erforderlich.

Der Zugang zu Systemdateien und Quellcode ist zu kontrollieren; IT-Projekte und Supportmaßnahmen sind in sicherer Form durchzuführen. Es ist dafür Sorge zu tragen, dass sensible Daten in Testumgebungen nicht frei zugänglich sind. Projekt- und Supportumgebungen sind einer strengen Kontrolle zu unterstellen. Dies gilt auch für Änderungen in der Produktionsumgebung. Bei wesentlichen Änderungen an der Produktionsumgebung ist eine Risikoeinschätzung durchzuführen.

Zudem müssen regelmäßige Sicherheitstests der produktiven Systeme durchgeführt werden. Diese sind auf Grundlage der Ergebnisse einer Risikoeinschätzung vorab zu planen und müssen mindestens Schwachstellenprüfungen umfassen. Sämtliche während der Sicherheitstests festgestellten Mängel sind zu prüfen. Maßnahmenpläne zur Schließung von ermittelten Sicherheitslücken müssen erstellt und zeitnah abgearbeitet werden.

Anforderung 1.11: Informationssicherheit bei Beziehungen zu Anbietern[11]

Um den Schutz der den Anbietern zugänglichen internen Informationssysteme des Teilnehmers zu gewährleisten, sind mit dem Anbieter zur Begrenzung der mit seinem Zugang verbundenen Risiken

[11] Als Anbieter ist hier jede dritte Partei (einschließlich ihrer Mitarbeiter) zu verstehen, mit der das Institut eine vertragliche Vereinbarung zur Erbringung einer Dienstleistung abgeschlossen hat und die (einschließlich ihrer Mitarbeiter) im Rahmen des Dienstleistungsvertrags entweder direkt vor Ort oder über einen Fernzugang Zugriff auf Informationen und/oder Informationssysteme und/oder informationsverarbeitende Einrichtungen des Instituts im Anwendungsbereich oder in Verbindung mit dem Anwendungsbereich der TARGET2-Selbstzertifizierung erhält.

Informationssicherheitsanforderungen zu dokumentieren und in einer formalen Vereinbarung festzuhalten.

Anforderung 1.12: Umgang mit Informationssicherheitsvorfällen und diesbezügliche Verbesserungen

Um einen konsistenten und wirksamen Ansatz für den Umgang mit Informationssicherheitsvorfällen (wozu auch die Meldung von Sicherheitsereignissen und -schwachstellen zählt) sicherzustellen, sollten sowohl auf fachlicher als auch auf technischer Ebene Rollen, Verantwortlichkeiten und Verfahren festgelegt und getestet werden, damit nach Informationssicherheitsvorfällen eine rasche, wirksame, geordnete Wiederherstellung der Sicherheit erfolgen kann; dies schließt auch Szenarien im Zusammenhang mit Cybervorfällen ein (z. B. Betrug durch einen externen Angreifer oder einen Insider). Das in diese Verfahren eingebundene Personal ist angemessen zu schulen.

Anforderung 1.13: Überprüfung der Erfüllung technischer Anforderungen

Die internen Informationssysteme eines Teilnehmers (z. B. Back-Office-Systeme, interne Netzwerke und Verbindungen zu externen Netzwerken) sind regelmäßig darauf zu bewerten, ob sie dem bestehenden Regelungsrahmen der Organisation (z. B. der Informationssicherheitsstrategie und der Leitlinie für kryptografische Verfahren) entsprechen.

Anforderung 1.14: Virtualisierung

Gast-VMs (virtuelle Maschinen) müssen sämtliche Sicherheitsanforderungen erfüllen, die auch für physische Hardware und Systeme gelten (z. B. Härtung, Protokollierung). Als Anforderungen für Hypervisoren sind vorgeschrieben: Härtung des Hypervisors und des Host-Betriebssystems, regelmäßige Patches und strikte Trennung der unterschiedlichen Umgebungen (z. B. Produktions- und Entwicklungsumgebung). Auf Basis einer Risikoanalyse sind eine zentralisierte Steuerung, Protokollierung, Überwachung und Verwaltung der Zugriffsrechte, insbesondere für Konten mit privilegierten Berechtigungen, zu implementieren. Verwaltet ein Hypervisor mehrere Gast-VMs, müssen diese ein ähnliches Risikoprofil haben.

Anforderung 1.15: Cloud Computing

Die Verwendung öffentlicher und/oder hybrider Cloud-Lösungen in der Zahlungstransaktionskette muss durch eine formale Risikoanalyse begründet sein, bei der die technischen Kontrollen und Vertragsbestimmungen der Cloud-Lösung geprüft werden.

Bei Nutzung einer Hybridlösung wird davon ausgegangen, dass das Gesamtsystem die höchste Kritikalitätsstufe im Vergleich zu den übrigen angebundenen Systemen aufweist. Alle am Standort befindlichen Komponenten der Hybridlösung sind von den übrigen Standortsystemen zu trennen.

Business-Continuity-Management (gilt nur für kritische Teilnehmer)

Die folgenden Anforderungen (2.1 bis 2.6) beziehen sich auf das Business-Continuity-Management. Jeder TARGET2-Teilnehmer, der vom Eurosystem im Hinblick auf das reibungslose Funktionieren von

TARGET2 als kritisch eingestuft wurde, muss über eine Strategie zur Aufrechterhaltung des Geschäftsbetriebs verfügen, die folgende Elemente aufweist:

Anforderung 2.1: Es müssen Business-Continuity-Pläne erstellt werden und Verfahren zu deren Einhaltung vorhanden sein.

Anforderung 2.2: Es muss ein Ausweichstandort vorhanden sein.

Anforderung 2.3: Das Risikoprofil des Ausweichstandorts muss sich von dem des Primärstandorts unterscheiden. Hierdurch soll vermieden werden, dass beide Standorte von derselben Störung gleichzeitig betroffen sind. So muss beispielsweise der Ausweichstandort an ein anderes Energieversorgungsnetz und eine andere Hauptfernmeldeleitung als der Primärstandort angeschlossen sein.

Anforderung 2.4: Im Falle einer größeren Betriebsstörung, die dazu führt, dass auf den Primärstandort nicht zugegriffen werden kann und/oder für den Betrieb notwendige Mitarbeiter nicht verfügbar sind, muss der kritische Teilnehmer in der Lage sein, den normalen Betrieb vom Ausweichstandort aus wiederaufzunehmen und dort den Geschäftstag ordnungsgemäß abzuschließen und den/die folgenden Geschäftstag(e) zu beginnen.

Anforderung 2.5: Durch etablierte Verfahren muss eine Wiederaufnahme der Transaktionsverarbeitung am Ausweichstandort innerhalb einer angemessenen Zeitspanne nach der ursprünglichen Unterbrechung des Dienstes und in Abhängigkeit von der Kritikalität des von der Unterbrechung betroffenen Geschäftsvorgangs gewährleistet werden.

Anforderung 2.6: Die Fähigkeit, Betriebsstörungen zu bewältigen, ist mindestens einmal jährlich zu überprüfen, und alle wichtigen Mitarbeiter sind in geeigneter Weise zu schulen. Der Abstand zwischen den Tests darf nicht länger als ein Jahr sein.

Selbstzertifizierende Institute

TARGET2-Teilnehmer können sich entweder direkt oder über eine gemeinsame technische Infrastruktur mit TARGET2 verbinden. Im letzteren Fall liegt es schlussendlich in der Hauptverantwortung des jeweiligen TARGET2-Teilnehmers, genau zu prüfen, welche Sicherheitsanforderungen für die spezifische technische Infrastruktur sowie die organisatorische Struktur seines Instituts gelten.

Jeder TARGET2-Teilnehmer (d. h. kritische und nichtkritische Teilnehmer/Nebensysteme) muss der Zentralbank, mit der er eine Geschäftsbeziehung unterhält, eine Selbstzertifizierungserklärung vorlegen. Werden Teile der für den TARGET2-Zugang eingesetzten Verfahren und/oder technischen Infrastruktur von verschiedenen TARGET2-Teilnehmern gemeinsam genutzt, so hat jeder dieser Teilnehmer bei der betreffenden Zentralbank eine eigene Selbstzertifizierungserklärung einzureichen.

Wenn ein TARGET2-Teilnehmer seinen Geschäftsbetrieb ganz oder teilweise an einen Dritten (z. B.

ein SWIFT-Servicebüro oder einen Gruppen-Hub)[12] ausgelagert hat, muss er sicherstellen, dass dieser Dritte die vom Eurosystem für TARGET2-Teilnehmer festgelegten Sicherheitsanforderungen erfüllt.
Falls eine oder mehrere Sicherheitsanforderungen nicht anwendbar sind, sollte der TARGET2-Teilnehmer dies in der nachstehenden Tabelle zur Prüfung der Umsetzung (Compliance Check) vermerken. Außerdem ist in der entsprechenden Rubrik der Selbstzertifizierung (mit der Bezeichnung „Umsetzungsfortschritt“) zu erläutern, warum eine bestimmte Sicherheitsanforderung nicht anwendbar ist.
Die TARGET2-Teilnehmer werden gebeten, sich in Zweifelsfällen mit der Zentralbank, mit der sie eine vertragliche Beziehung unterhalten, in Verbindung zu setzen, um den Umfang ihrer Selbstzertifizierung zu klären.

Unterzeichner

Die Selbstzertifizierungserklärung ist von einer Führungskraft auf Vorstands- oder vergleichbarer Ebene[13] zu unterzeichnen, die innerhalb der Organisation des TARGET2-Teilnehmers für das Risikomanagement im Bereich der Informationssicherheit verantwortlich ist.

Bei kritischen TARGET2-Teilnehmern ist die Selbstzertifizierung zusätzlich vom (externen oder internen) Revisor dieses Teilnehmers zu unterzeichnen.

Prüfung der Umsetzung (Compliance Check)

In der Selbstzertifizierungserklärung muss der TARGET2-Teilnehmer für jede der vom Eurosystem festgelegten Anforderungen angeben, ob er sie umgesetzt oder nicht umgesetzt hat bzw. ob diese nicht anwendbar ist.
Im Falle der Nichtumsetzung einer bestimmten Anforderung sind in der entsprechenden Rubrik der Selbstzertifizierung (mit der Bezeichnung „Umsetzungsfortschritt“) die größten Risiken[14] zu

---

12 Ein *Servicebüro* ist eine Organisation, die selbst SWIFT-Nutzer sein kann (aber nicht sein muss) und SWIFT Nutzern einen technischen Zugang zum SWIFT-Netz ermöglicht. SWIFT-Nutzer und Servicebüro sind organisatorisch nicht miteinander verbunden. Zu den von einem Servicebüro angebotenen Diensten gehören die Bereitstellung und der Betrieb von SWIFT-Nachrichten- und/oder SWIFT-Konnektivitätskomponenten im Auftrag von SWIFT-Nutzern. Ein *Gruppen-Hub* ist eine Organisation, die selbst SWIFT-Nutzer sein kann (aber nicht sein muss) und SWIFT-Nutzern einen technischen Zugang zum SWIFT-Netz ermöglicht; die SWIFT-Nutzer gehören dabei zur gleichen Organisation wie der Gruppen-Hub.
Weitere Informationen zu Servicebüro und Gruppen-Hub siehe SWIFT, Shared Infrastructure Programme, Terms and Condition 2019: www2.swift.com/knowledgecentre/rest/v1/publications/shr_infra_prog_trm_cond_2019/1.0/shr_infra_prog_trm_cond_2019.pdf?logDownload=true

13 Solche Führungskräfte sind hochrangige Vertreter eines Unternehmens, die unternehmensweite Entscheidungen treffen. Beispiele für hochrangige Führungskräfte sind der Chief Executive Officer (CEO), Chief Operating Officer (COO) und Chief Information Officer (CIO). Sofern entsprechende Funktionen vorhanden sind, könnte der Unterzeichner auch ein Chief Risk Officer (CRO) oder Chief Information Security Officer (CISO) sein.

14 Hierzu gehören beispielsweise: unzureichende Vorkehrungen gegen Denial-of-Service-Angriffe oder das Fehlen einer unterbrechungsfreien Stromversorgung.

beschreiben. Darüber hinaus sollten ein Aktionsplan zur Behebung des Problems beigefügt sowie der vorgesehene Termin für die Umsetzung jeder einzelnen Maßnahme benannt werden. Die zuständige Zentralbank muss diese Angaben auswerten und die zeitnahe Durchführung der Maßnahmen zur Risikominderung überwachen. Zudem wird das Leitungsorgan des Eurosystems, das für den sicheren und zuverlässigen Betrieb von TARGET2 zuständig ist, über das Ergebnis der Selbstzertifizierung sowie über den Umsetzungsfortschritt der zur Risikominderung ergriffenen Maßnahmen unterrichtet.

Umsetzungsgrad

TARGET2-Teilnehmer sind verpflichtet anzugeben, inwieweit die vom Eurosystem in seiner Funktion als TARGET2-Systembetreiber festgelegten Anforderungen zum Informationssicherheitsmanagement umgesetzt wurden.
Bei der Beurteilung der Frage, inwieweit die TARGET2-Teilnehmer die Vorgaben insgesamt einhalten, verwendet der TARGET2-Betreiber einen quantitativen Ansatz (die Umsetzung der Business-Continuity-Anforderungen wird nur bei kritischen Teilnehmern geprüft). Dabei werden folgende Kriterien zugrunde gelegt:

- **Vollständige Umsetzung:** Die TARGET2-Teilnehmer erfüllen 100 % der Anforderungen (d. h. alle 15 Anforderungen an die Informationssicherheit und alle 6 Business-Continuity-Anforderungen (nur bei kritischen Teilnehmern)).
- **Geringfügige Nichtumsetzung:** Die TARGET2-Teilnehmer erfüllen weniger als 100 %, aber mindestens 66 % der Anforderungen (d. h. 10 Anforderungen an die Informationssicherheit und 4 Business-Continuity-Anforderungen (nur bei kritischen Teilnehmern)).
- **Gravierende Nichtumsetzung:** Die TARGET2-Teilnehmern erfüllen weniger als 66 % der Anforderungen (d. h. weniger als 10 Anforderungen an die Informationssicherheit oder weniger als 4 Business-Continuity-Anforderungen (nur bei kritischen Teilnehmern)).

TARGET2-Teilnehmern, die nachweisen, dass eine bestimmte Anforderung nicht auf sie anwendbar ist, wird im Rahmen der obigen Beurteilung in Bezug auf die betreffende Anforderung eine Umsetzung bescheinigt.

Meldung im Auftrag eines anderen TARGET2-Teilnehmers

Ein TARGET2-Teilnehmer kann eine eigene Selbstzertifizierung bei der betreffenden Zentralbank einreichen und gleichzeitig auch im Auftrag anderer TARGET2-Teilnehmer deren Umsetzungsgrad melden. Solche Meldungen sind möglich, wenn die beiden folgenden Bedingungen erfüllt sind:

c) Alle Teilnehmer gehören zur selben „Gruppe“ im Sinne der Definition in Anhang II („Harmonisierte Bedingungen für die Teilnahme an TARGET2“) der

TARGET2-Leitlinie und nutzen dieselbe technische Infrastruktur für die Einreichung von Zahlungen.

TARGET2-Teilnehmer, die durch eine einzige Selbstzertifizierungserklärung erfasst sind, , nutzen für die Einreichung von Zahlungen in TARGET2 dieselbe Infrastruktur, unabhängig davon, ob sie ihre Geschäftsbeziehung bei derselben Zentralbank unterhalten oder nicht.

Sollte sich in einer Gruppe ein kritischer Teilnehmer befinden, so obliegt es diesem kritischen Teilnehmer, die Selbstzertifizierungserklärung bei der betreffenden Zentralbank einzureichen. Zugleich nimmt er auch die Meldungen für die anderen TARGET2-Teilnehmer seiner Gruppe vor.

d) Alle Teilnehmer, die durch eine einzige Selbstzertifizierungserklärung erfasst werden, setzen sämtliche anwendbaren Anforderungen vollständig um.

Innerhalb einer Bankengruppe kann es vorkommen, dass einige TARGET2-Teilnehmer als kritisch und andere als nichtkritisch eingestuft werden. Deshalb wird in der Selbstzertifizierungserklärung (mithilfe des Feldes „Meldung für“ zu jeder Art von Anforderung) unterschieden, welche Teilnehmer nur die Anforderungen an die Informationssicherheit und welche Teilnehmer darüber hinaus die Business-Continuity-Anforderungen umsetzen müssen.

Wenn eine bestimmte Anforderung von einigen Teilnehmern umgesetzt wird, während sie für andere Teilnehmer nicht anwendbar ist, sollten in der Selbstzertifizierungserklärung für diese Anforderung beide Felder (d. h. „Anforderung umgesetzt“ und „Anforderung nicht anwendbar“) angekreuzt werden. In einem separaten Feld in der Erklärung ist genauer zu erläutern, weshalb eine bestimmte Anforderung für einen bestimmten Teilnehmer nicht anwendbar ist.

Im Falle der Nichtumsetzung einer oder mehrerer Anforderungen durch einen TARGET2-Teilnehmer muss dieser seine eigene Selbstzertifizierungserklärung bei der betreffenden Zentralbank einreichen. Die Vorgehensweise, dass jeder Teilnehmer einer Gruppe, der eine Anforderung nicht umsetzt, eine eigene Selbstzertifizierungserklärung abgeben muss, ist auch einzuhalten, wenn die fehlende Anforderung für alle Teilnehmer der Gruppe identisch ist.

Selbstzertifizierungserklärung

Kontaktdaten

Nachstehend sind der Name des TARGET2-Teilnehmers, der die Selbstzertifizierungserklärung einreicht, und die Kontaktdaten der Person anzugeben, die als Ansprechpartner zur Verfügung steht, wenn weitere Informationen benötigt werden.

Name des TARGET2-Teilnehmers	
Anschrift	
BIC	
Kontaktperson (Name in Druckbuchstaben)	
Kontaktperson (Telefon)	
Kontaktperson (E-Mail)	

Verwendung eines Servicebüros oder Gruppen-Hubs

Neben einer direkten Anbindung an die TARGET2-Gemeinschaftsplattform kann die Anbindung auch über ein SWIFT-Servicebüro oder einen SWIFT-Gruppen-Hub erfolgen.

Ist Ihre Organisation über ein Servicebüro an die TARGET2-Gemeinschaftsplattform angeschlossen?	Ja ☐	Nein ☐
Wenn ja, geben Sie bitte den Namen und den BIC des Servicebüros an.		

Ist Ihre Organisation über einen Gruppen-Hub an die TARGET2-Gemeinschaftsplattform angeschlossen?	Ja ☐	Nein ☐
Wenn ja, geben Sie bitte den Namen und den BIC des Gruppen-Hubs an.		

Anforderungen an das Informationssicherheitsmanagement (gilt für alle TARGET2-Teilnehmer[15])

	Anforderung umgesetzt	Anforderung nicht umgesetzt	Anforderung nicht anwendbar
Anforderung 1.1	☐	☐	☐
Anforderung 1.2	☐	☐	☐
Anforderung 1.3	☐	☐	☐
Anforderung 1.4	☐	☐	☐
Anforderung 1.5	☐	☐	☐
Anforderung 1.6	☐	☐	☐
Anforderung 1.7	☐	☐	☐
Anforderung 1.8	☐	☐	☐
Anforderung 1.9	☐	☐	☐
Anforderung 1.10	☐	☐	☐
Anforderung 1.11	☐	☐	☐
Anforderung 1.12	☐	☐	☐
Anforderung 1.13	☐	☐	☐
Anforderung 1.14	☐	☐	☐
Anforderung 1.15	☐	☐	☐
Welcher Standard für das Informationssicherheitsmanagement (z. B. ISO 27001, COSO, ISACA, COBIT, NIST) wird in Ihrer Organisation verwendet?			

[15] Alle TARGET2-Teilnehmer müssen also die Anforderungen dieser Tabelle an das Informationssicherheitsmanagement erfüllen. Bitte kreuzen Sie die entsprechenden Kästchen an und beantworten die Fragen in diesem Abschnitt.

Nutzt Ihre Organisation hinsichtlich der Zahlungstransaktionskette relevante Dienste, die von einem Cloud-Anbieter zur Verfügung gestellt werden (d. h. öffentliche oder hybride Cloud-Lösungen oder externe Dokumentenablagesysteme)?	

Meldung der Anforderungen zum Informationssicherheitsmanagement im Auftrag anderer TARGET2-Teilnehmer (soweit anwendbar)	
BIC des Teilnehmers	Jeweilige Zentralbank des Teilnehmers

Business-Continuity-Anforderungen (gilt ausschließlich für kritische Teilnehmer)

	Anforderung umgesetzt	**Anforderung nicht umgesetzt**	**Anforderung nicht anwendbar**
Anforderung 2.1	☐	☐	☐
Anforderung 2.2	☐	☐	☐
Anforderung 2.3	☐	☐	☐
Anforderung 2.4	☐	☐	☐
Anforderung 2.5	☐	☐	☐
Anforderung 2.6	☐	☐	☐

Meldung der Business-Continuity-Anforderungen im Auftrag anderer TARGET2-Teilnehmer (soweit anwendbar)	
BIC des Teilnehmers	Jeweilige Zentralbank des Teilnehmers

Umsetzungsfortschritt

Dieser Abschnitt ist auszufüllen, wenn bei einem Teilnehmer a) eine Nichtumsetzung einer Sicherheitsanforderung festgestellt wurde oder b) eine Anforderung als „nicht anwendbar“ gekennzeichnet wurde.

Geben Sie bitte für jede in der obigen Tabelle als „nicht anwendbar“ gekennzeichnete Anforderung eine kurze Begründung hierfür an. Anmerkungen:
Welche Risiken wurden infolge der Nichtumsetzung der Anforderungen 1.1 bis 1.15 bzw. 2.1 bis 2.6 ermittelt? (Bitte antworten Sie für jede als „nicht umgesetzt“ bezeichnete Anforderung getrennt.) Anmerkungen:
Welche Schritte werden eingeleitet, um eine vollständige Umsetzung aller Anforderungen zu erreichen? (Bitte antworten Sie für jede als „nicht umgesetzt“ bezeichnete Anforderung getrennt.) Anmerkungen:

Bis zu welchem Datum soll die vollständige Umsetzung erreicht werden? Anmerkungen:

Zertifizierung

Die Unterzeichner bestätigen, dass sie die in dieser Selbstzertifizierungserklärung aufgeführten Anforderungen gelesen und verstanden haben. Die Erklärung ist jährlich zu erneuern. In der Zwischenzeit ist jede festgestellte Nichtumsetzung unverzüglich der zuständigen Zentralbank zu melden.

Die Unterzeichner bestätigen, dass die in der Erklärung enthaltenen Informationen ein zutreffendes und genaues Bild der aktuellen Situation vermitteln. Sie bestätigen ferner, dass die Erklärung unter ihrer Leitung und Kontrolle erstellt wurde und die ausgewiesenen Angaben von qualifiziertem Personal ordnungsgemäß erhoben und ausgewertet wurden. Alle Angaben sind nach bestem Wissen und Gewissen der Unterzeichner zutreffend, korrekt und vollständig. Den Unterzeichnern ist bekannt, dass die Einreichung dieser Daten eine wesentliche Verpflichtung ist und die Einreichung falscher, ungenauer oder irreführender Angaben einen Verstoß gegen Artikel 34 Absatz 2 Buchstabe c der TARGET2-Leitlinie darstellt, was ein Grund für den Ausschluss des betreffenden Instituts von TARGET2 ist.

Die Unterzeichner bestätigen zudem, dass es in ihrer Organisation einen Mechanismus gibt, der sicherstellt, dass die Einhaltung der Anforderungen im folgenden Jahr gewährleistet bleibt. Sofern die Maßnahmen noch nicht vollständig umgesetzt wurden, bestätigen die Unterzeichner, dass angemessene Vorkehrungen getroffen werden, die eine vollständige Umsetzung spätestens bis zum Ende des nächsten Kalenderjahrs ermöglichen.

Reicht ein Teilnehmer die Erklärung und Meldung für einen anderen oder mehrere andere TARGET2-Teilnehmer ein, bestätigen die Unterzeichner die vorstehenden Punkte für alle in der Erklärung aufgeführten Teilnehmer. Den Unterzeichnern ist bekannt, dass die Einreichung dieser Information eine wesentliche Verpflichtung des Teilnehmers ist, für den sie die Unterschrift leisten, und dass die

Einreichung falscher, ungenauer oder irreführender Angaben einen Verstoß gegen Artikel 34 Absatz 2 Buchstabe c der TARGET2-Leitlinie darstellt, was ein Grund für den Ausschluss des betreffenden Instituts von der Teilnahme an TARGET2 ist.

Unterschrift

Name des Amtsträgers (in Druckbuchstaben)	
Titel/Funktion (Führungskraft auf Vorstandsebene o. Ä.)	
Datum	
Unterschrift	

Unterschrift des Revisors – nur von kritischen TARGET2-Teilnehmern auszufüllen

Name des Prüfers (in Druckbuchstaben)	
Titel (Angabe, ob interner oder externer Revisor)	
Datum	
Unterschrift	

Diese Selbstzertifizierungserklärung bitte zurücksenden an

Name der Zentralbank	
Anschrift	
Kontaktperson	

Anhang IV Formular für Änderungsvorschläge

Memo für Vorschläge zur Änderung der SSP/TIPS-Plattform
Absender: _____ NZB des Absenders: _____
Datum: _____

Angaben zur Änderung	
Bezeichnung der Änderung	Kurze Erläuterung
Priorität nach Einschätzung des Nutzers	Mögliche Optionen: hoch, mittel, niedrig
Betroffene Module	Sofern bekannt. Mögliche Optionen: PM, ICM, SD, HAM, SFM, RMM, ASI, TIPS, TIPS-Schnittstelle, T2S-Schnittstelle (Mehrfachnennungen möglich)
Beschreibung der Änderung	
Derzeitiges Systemverhalten	• Bezieht sich der Vorschlag auf eine bestehende oder eine neue Dienstleistung? • Angabe der betroffenen bestehenden Dienstleistung (Hinweise zu den UDFS und/oder zum ICM-Benutzerhandbuch erbeten)
Vorgeschlagene Änderung – Funktionsbeschreibung	• Funktionsbeschreibung der neuen/verbesserten Dienstleistung • Angabe, ob Nutzung der vorgeschlagenen Änderung optional oder obligatorisch wäre (sofern zutreffend)
Geschäftsvorfall und erwartetes Ergebnis nach Umsetzung der Änderung	Beschreibung des dem Vorschlag zugrunde liegenden Geschäftsvorfalls sowie des Nutzens durch die Umsetzung
Begleitdokumente	
1 Dokument	Weitere Anlagen wie Bildschirmausdrucke, Flussdiagramme usw.
2 Dokument	Erläuternde Beispiele

Anmerkung: Im Feld „Vorgeschlagene Änderung“ sollte die Funktionsbeschreibung so genau wie möglich sein, mit klaren Regeln, die keinen Raum für Interpretationen lassen.

Anhang V Auskunftsersuchen

Ersuchen um Auskunft über die Verarbeitung personenbezogener Daten gemäß Artikel 17 der Verordnung (EU) 2018/1725 und Artikel 15 der Verordnung (EU) 2016/679

Um Auskunft darüber erteilen zu können, ob in einer vom Eurosystem betriebenen Finanzmarktinfrastruktur (TARGET2, T2S und TIPS) personenbezogene Daten über Sie gespeichert werden, benötigt das Eurosystem von Ihnen folgende Informationen:

1. Allgemeine Fragen

Bitte geben Sie an, ob Sie ihr Auskunftsersuchen an das Eurosystem

- (•) als Privatperson (in eigenem Namen)
- ( ) oder im Auftrag einer Privatperson (d. h. für jemand anderen) stellen. In diesem Fall fügen Sie bitte eine Vollmacht bei.

Falls das Auskunftsersuchen nicht Ihre eigenen personenbezogenen Daten betrifft, geben Sie bitte in Abschnitt 2 den Eigentümer der personenbezogenen Daten an.

Bitte beachten Sie, dass Sie zunächst Ihre Identität nachweisen oder – falls Sie im Auftrag einer anderen Person handeln – eine Vollmacht vorlegen müssen, damit Ihr Ersuchen bearbeitet wird und Sie eine Auskunft bzw. die angefragten Daten erhalten. Ihre Identität wird anhand der geltenden Gesetze und Vorschriften des Landes überprüft, in dem die Datenverarbeitung erfolgt ist (d. h. des Landes, in dem die als "Partial Joint Controller" datenverantwortliche Partei ansässig ist, an die das Auskunftsersuchen gerichtet ist).

2. Informationen, die zur allgemeinen Identifizierung und Abgrenzung erforderlich sind

Die unter Punkt A bis C geforderten Informationen dienen als Abgrenzungs-/Identifikationskriterien und ermöglichen eine zeitnahe und effiziente Suche Ihrer personenbezogenen Daten in den Datenbanken der Finanzmarktinfrastrukturen des Eurosystems.

Bitte beachten Sie, dass Auskunftsersuchen zurückgewiesen werden können und nicht bearbeitet werden müssen, wenn sie als offensichtlich unbegründet oder unverhältnismäßig erachtet werden. Fehlende Informationen zur Abgrenzung des Gegenstands Ihres Ersuchens (d. h. fehlende Angaben unter Punkt A bis C) können zu einem unverhältnismäßig hohen Aufwand und somit zu einer Zurückweisung ihres Ersuchens führen.

A. Namen

Vorname(n) in der exakt gleichen Schreibweise, die im Zusammenhang mit der Angelegenheit verwendet wurde, zu der Sie Auskunft ersuchen

_____

Nachname(n) in der exakt gleichen Schreibweise, die im Zusammenhang mit der Angelegenheit verwendet wurde, zu der Sie Auskunft ersuchen

_____

B. Referenzzeitraum

Geben Sie das Kalenderjahr an, in dem die Transaktion initiiert wurde (falls möglich, grenzen Sie den Zeitraum noch genauer ein). Wenn Ihr Auskunftsersuchen mehr als eine Transaktion betrifft, geben Sie bitte für alle Transaktionen einen Referenzzeitraum an:

_____

C. Bitte wählen Sie aus, um welche Art(en) von Transaktion(en) es sich handelt:

- ○ Wertpapierabwicklung (T2S)
- ○ Überweisung (TARGET2)
- ○ Instant-Zahlung (TIPS)

D. Optionale Informationen

Folgende Angaben (sofern Sie diese z. B. über Ihre Geschäftsbank erhalten können) können uns helfen, Ihre personenbezogenen Daten noch leichter zu identifizieren:

T2S/TARGET2/TIPS-Referenznummer:

_____

T2S/TARGET2/TIPS-Kontonummer: _____

Transaktionsbetrag: _____

ISIN (Wertpapierabwicklung):

_____

IBAN und/oder BIC der auftraggebenden und der empfangenden Geschäfts- oder Depotbank (wenn Sie um Auskunft zu mehr als einer Transaktion ersuchen, geben Sie bitte die entsprechenden IBANs/BICs für alle Transaktionen an):

Auftraggeberbank: _____

Empfängerbank: _____

Anhang VI Glossar und Abkürzungsverzeichnis

A B C D E F G H I J K L M N P R S T U V W X Y Z

-A- *Glossar*

Akkreditierte Zertifizierungsstelle (accredited certification authority):
Eine oder mehrere Zentralbanken, die vom EZB-Rat dazu bestimmt wurden, im Rahmen des internetbasierten Zugangs bei der Ausstellung, Verwaltung, dem Widerruf und der Erneuerung elektronischer Zertifikate für das Eurosystem tätig zu werden.

Algorithmus (algorithm):
Ein Algorithmus ist eine mathematische Methode, um eine reibungslose, schnelle und liquiditätssparende Verarbeitung der Zahlungen in einer Warteschlange zu gewährleisten, beispielsweise, indem gegeneinander aufrechenbare Zahlungsströme berücksichtigt werden.

AMI-Pay:
Advisory Group on Market Infrastructures for Payments

AMI-SeCo:
Advisory Group on Market Infrastructures for Securities and Collateral

Anbieter-NZBen der TIPS-Plattform (TIPS platform-providing NCBs):
Die Anbieter-NZBen der TIPS-Plattform sind die Deutsche Bundesbank, die Banco de España, die Banque de France und die Banca d'Italia. Diese Zentralbanken sind für die Errichtung und den Betrieb der TIPS-Plattform für das Eurosystem verantwortlich.

Application-to-Application (A2A):
Verbindungsmodus, der den Informationsaustausch zwischen der Softwareanwendung der SSP bzw. der T2S-Plattform bzw. der TIPS-Plattform und der/den Softwareanwendung(en) der Nutzer ermöglicht.

AS Contingency Tool:
Ein Instrument für das Nebensystem zur Vereinfachung der Generierung und Verarbeitung von XML-Nachrichten. Es steht ausschließlich Zentralbanken zur Verfügung.

Ausfallsicherung (failover):
Eine Ausfallsicherung bezeichnet die Möglichkeit, technisch von einem Standort auf einen zweiten umzuschalten. Innerhalb der Konfiguration der Gemeinschaftsplattform gibt es zwei Ausfallsicherungssituationen:

- Intraregionale Ausfallsicherung: Überwechseln von einem Standort zu einem zweiten Standort innerhalb derselben Region
- Interregionale Ausfallsicherung: Überwechseln von einer Region zu einer anderen Region.

-B- *Glossar*

Batch:
Ein Batch ist ein Stapel von Aufträgen (Zahlungs- und/oder Wertpapierübertragungsaufträgen), der als Einheit verarbeitet wird.

Berechtigung (privilege):
Ein gewährtes oder verweigertes Recht, innerhalb einer Anwendung bestimmte Funktionen auszuführen oder auf bestimmte Daten zuzugreifen und/oder diese zu aktualisieren.

BIC:
Business Identifier Code

BIC1:
Ein Nicht-SWIFT-BIC, der an der achten Stelle eine „1“ trägt. Ein BIC1 kann nicht in der Kopfzeile einer SWIFT-Nachricht verwendet werden.

BIC8:
Die ersten acht Stellen des BIC. Bei Adressierungen bezeichnen sie den Zielort.

BIC11:
Neben den ersten acht Stellen des BIC wird ein dreistelliger optionaler Code zur Bezeichnung von Zweigstellen oder sonstigen Referenzangaben eines Instituts verwendet.

BIC-Directory:
Von SWIFT veröffentlichtes Verzeichnis der Identifikationscodes von Kreditinstituten.

Bruttoausgleich in Echtzeit (real-time gross settlement – RTGS):
Unter einem Bruttoausgleich in Echtzeit versteht man die kontinuierliche Übertragung von Geldern oder Wertpapieren in Echtzeit. Dabei wird jede Transaktion einzeln und ohne Netting ausgeführt.

Bruttoausgleichssystem (gross settlement system):
Übertragungssystem, bei dem jede Übertragung von Vermögenswerten oder Wertpapieren einzeln abgewickelt wird.

Business Continuity (Aufrechterhaltung des Geschäftsbetriebs):
Vorkehrungen im Zahlungsverkehrssystem zur Gewährleistung des vereinbarten Leistungsspektrums auch bei Ausfall einer oder mehrerer Systemkomponenten oder bei Auftreten eines außergewöhnlichen externen Ereignisses. Die Vorkehrungen zur Business Continuity umfassen sowohl Präventiv- als auch Notfallmaßnahmen.

-C- *Glossar*

CBT (computer-based terminal – CBT):
Computergestütztes Terminal für den SWIFT-Zugang

Clearing:
Als Clearing bezeichnet man das Verfahren zur Berechnung der gegenseitigen Verbindlichkeiten von Marktteilnehmern für den Austausch von Wertpapieren und Geld. Es kann auch die Übermittlung, die Abstimmung und in einigen Fällen die Bestätigung von Zahlungs- oder Wertpapieraufträgen umfassen.

Clearinghaus (clearing house):
Eine Verrechnungsstelle, die ein Clearing-System betreibt, welches aus einer Reihe von Regeln und Verfahren besteht, über das Finanzinstitute Daten und/oder Dokumente in Verbindung mit Zahlungen oder Wertpapierübertragungen an einem einzigen Ort vorlegen und untereinander austauschen. Zu den Verfahren gehört häufig auch ein Mechanismus zur Berechnung der gegenseitigen Positionen der Teilnehmer, möglicherweise auf Nettobasis, um den Ausgleich ihrer Verbindlichkeiten im Abwicklungssystem zu erleichtern.

Client Collateralisation:
Kredit, den ein T2S-Geldkontoinhaber seinen Kunden in T2S im Rahmen eines Besicherungsmechanismus zur Verfügung stellt.

Closed Group of Users (CGU):
Eine Untergruppe von Kunden, die zur Verwendung der jeweiligen Dienste und Produkte des jeweiligen Anbieters von Mehrwertnetzwerkdiensten beim Zugang zur T2S-Plattform zusammengefasst werden.

Closed User Group (CUG):
Eine Untergruppe von Kunden, die zur Verwendung der jeweiligen SWIFT-Dienste und -Produkte beim Zugang zum Zahlungsmodul zusammengefasst werden.

Contingency-Netzwerk (contingency network):
Ein vom Eurosystem betriebenes alternatives Netzwerk zur Weiterleitung des Zahlungsverkehrs bei einem Ausfall der SWIFT-Dienste.

Contingency-Situation (contingency):
Eine Contingency-Situation bezeichnet einen eingeschränkten Geschäftsbetrieb bei einem Systemausfall. Systemisch wichtige Zahlungen werden in Contingency-Situationen auf Basis vereinbarter Contingency-Verfahren und Contingency-Kommunikationsverfahren abgewickelt.

Continuous Linked Settlement (CLS):
CLS ist ein globales Abwicklungssystem für Devisentransaktionen. Es bietet den Teilnehmern die gleichzeitige Verarbeitung beider Seiten der Transaktion und schaltet somit das Erfüllungsrisiko aus.

CRISP (consumption report and invoicing support process):
CRISP ist ein optionales Kundenbetreuungssystem der Gemeinschaftsplattform, das den nationalen Zentralbanken für die Rechnungserstellung zur Verfügung steht.

CRSS (customer related services system):
CRSS ist eine der beiden technischen Konfigurationen der Gemeinschaftsplattform. Die andere ist das Zahlungsabwicklungs- und Kontoführungssystem PAPSS. Bei dieser technischen Konfiguration sind die ausschließlich den nationalen Zentralbanken vorbehaltenen Grundleistungen und optionalen Leistungen vollständig oder teilweise implementiert.

CRSS-Hauptmeldefunktionen (CRSS core reporting functions):
Mit Wirkung vom November 2012 wurden die „Core Requirements on Statistics and Storage“ (CROSS) und das „Customer Relationship and Knowledge of Systems“ (CRAKS1) zu „CRSS Core Reporting Functions“ (CRSS-Hauptmeldefunktionen) zusammengefasst. Sie beinhalten die Dienstleistungen der Gemeinschaftsplattform für Zentralbanken, die diese u. a. für die Archivierung und Speicherung von Aktivitäten, für Rechnungskalkulationen, für die Bereitstellung von Statistiken zu Innertageskrediten und für Profilangaben verbindlich nutzen. Der Support für die Customer Relationships and Knowledge of Payments Systems wird durch CRAKS3, ebenfalls im CRSS verfügbar, erbracht.

CSD-Teilnehmer (CSD participant):
Kunde eines Zentralverwahrers (Central Securities Depository – CSD).

Customer Relationship Management:
Dieser Begriff bezieht sich auf die Verwaltung kundenorientierter Angaben im Zusammenhang mit den

Nutzern (Teilnehmern, Nebensystemen und anderen Kunden, beispielsweise Zentralbankkunden im Heimatkontomodul) durch die Zentralbanken.

-D- *Glossar*

Daueauftrag (standing order):
Auftrag, regelmäßig einen bestimmten Betrag von einem Konto auf ein anderes Konto zu überweisen.

Dedizierte Liquidität (dedicated liquidity):
Liquidität, die auf einem Unterkonto oder einem Spiegelkonto gehalten wird, um die Abwicklung von Transaktionen im Nebensystem zu ermöglichen.

Dediziertes Konto (dedicated account):
Konto im Zahlungsmodul, auf dem dedizierte Liquidität für die Abwicklung im Nebensystem gehalten wird. Dies kann entweder ein Unterkonto (Schnittstellen-Modell) oder ein Spiegelkonto (integriertes Modell) sein.

Dediziertes Zwischenkonto (dedicated transit account):
Ein im RTGS-System und in T2S geführtes Geldkonto, das vom verantwortlichen Systembetreiber unterhalten wird und der Übertragung von Geldern dient. Das in T2S geführte Zwischenkonto wird als dediziertes RTGS-Zwischenkonto (RTGS dedicated transit account) und das im RTGS-System geführte Zwischenkonto als dediziertes T2S-Zwischenkonto (T2S dedicated transit account) bezeichnet.

Direkt angeschlossener T2S-Geldkontoinhaber (directly connected T2S DCA holder):
Ein T2S-Geldkontoinhaber, dem von der jeweiligen Zentralbank ein direkter Zugang zu T2S gewährt wurde, um die T2S-Dienstleistungen zu nutzen. Die Zentralbank fungiert nicht als technische Schnittstelle (andernfalls wäre der Geldkontoinhaber ein „indirekt angeschlossener T2S-Geldkontoinhaber“).

Direkter Teilnehmer (direct participant):
Teilnehmer eines Systems, der direkt mit anderen Teilnehmern dieses Systems Transaktionen durchführt. Er kann alle in dem System erlaubten Tätigkeiten ohne Intermediär vornehmen. In einigen Systemen können direkte Teilnehmer auch Transaktionen im Auftrag indirekter Teilnehmer durchführen.

Dokumente, die den T2S-Umfang definieren (T2S scope-defining set of documents):
Der Umfang von T2S ist in folgenden Dokumenten definiert: User Requirements Document (URD), User Detailed Functional Specifications (UDFS), GUI Business Functionality, GFS Functional Chapter, Dedicated Link Connectivity Specifications und Data Migration Tool Specifications and Related Procedures.

-E- *Glossar*

Earmarking:
Kennzeichnung einer bestimmten Menge von Wertpapieren auf einem Wertpapierkonto, die nur für bestimmte Arten von Transaktionen oder Prozessen zugelassen ist. Ein CSD-Teilnehmer kann beispielsweise eine Wertpapierposition auf einem Wertpapierkonto oder alle auf dem Konto verbuchten Wertpapiere als besicherungsfähige Sicherheiten kennzeichnen.

EBA Clearing:
Unternehmen, das im Auftrag seiner Mitglieder das EURO1-, STEP2-, STEP2-Card-Clearing- und das RT1-(Instant-Zahlungs-)System unterhält.

Ebene 1 (level 1):
EZB-Rat

Ebene 2 (level 2):
Zentralbanken des Eurosystems

Ebene 3 (level 3):
Anbieter-Zentralbanken der Gemeinschaftsplattform

Echtzeit-Bruttosystem (RTGS-System) (real-time gross settlement system):
Ein Echtzeit-Bruttosystem ist ein Abwicklungssystem, bei dem Verarbeitung und Ausgleich in Echtzeit und auf Bruttobasis erfolgen. Ein RTGS-System kann ein zentrales Warteschlangenverfahren für Aufträge bereitstellen, die nicht zum Zeitpunkt der Einreichung bearbeitet werden können (beispielsweise weil nicht genügend Liquidität vorhanden oder das Liquiditätslimit ausgeschöpft ist).

ECONS I
Ein gemeinsames obligatorisches Instrument der Zentralbanken zur Bewältigung von Notfallsituationen, um kritische und sehr kritische Zahlungen abwickeln zu können.

(Effekten-)Girosystem (book-entry system):
System, das die Übertragung von Wertpapieren und anderen Finanzinstrumenten gestattet, ohne effektive Stücke zu bewegen (z. B. die elektronische Übertragung von Wertpapieren).

Einlagefazilität (deposit facility):
Ständige Fazilität des Eurosystems, die den Geschäftspartnern die Möglichkeit bietet, Guthaben bis zum nächsten Geschäftstag zu einem vorher festgesetzten Zinssatz bei einer nationalen Zentralbank anzulegen.

Endgültige Abwicklung (final settlement):
Die endgültige Abwicklung ist die Erfüllung einer Verpflichtung durch eine Übertragung von Geldern und von Wertpapieren, die unwiderruflich, unumkehrbar und unaufhebbar geworden ist.

EPC (European Payments Council):
Europäischer Zahlungsverkehrsrat

Ersatzzahlungen (backup payments):
Wenn das System eines PM-Kontoinhabers nicht mehr verfügbar ist, kann dieser mithilfe von Ersatzzahlungen seinen Zahlungsverpflichtungen gegenüber CLS und EURO1 nachkommen und eine Liquiditätskonzentration auf seinem PM-Konto verhindern. Solche Ersatzzahlungen werden über das Informations- und Steuerungsmodul (ICM) initiiert. Dabei stehen zwei Arten von Ersatzzahlungen zur Verfügung:

- Contingency-Zahlungen zur Erfüllung von Einzahlungsverpflichtungen gegenüber CLS, dem EURO1-Sicherheitenkonto oder dem EURO1-Deckungskonto (TARGET2/EURO1-Liquiditätsbrücke)
- Ersatzzahlungen zur Umverteilung von Liquidität, durch die überschüssige Liquidität, die sich auf dem PM-Konto des betreffenden Teilnehmers angesammelt hat, verteilt wird.

ESZB (ESCB):
Europäisches System der Zentralbanken

EU:
Europäische Union

EURO1:
Großbetragszahlungssystem des privaten Sektors für einzelne taggleiche Transaktionen in Euro auf gesamteuropäischer Ebene.

Eurosystem:
Die EZB und die nationalen Zentralbanken der EU-Mitgliedstaaten, deren Währung der Euro ist, wie in Artikel 1 der Satzung des ESZB und der EZB festgelegt.

EWR (EEA):
Europäischer Wirtschaftsraum

External Guarantee Limit:
Vom T2S-Geldkontoinhaber für seinen Kunden festgelegte Obergrenze für Kredite, die außerhalb von T2S besichert werden. Das External Guarantee Limit und das Unsecured Credit Limit sind aus der Sicht von T2S identisch. Sie unterscheiden sich nur hinsichtlich der Reihenfolge ihrer Inanspruchnahme,

wobei die Client Collateralisation genutzt wird, nachdem das External Guarantee Limit ausgeschöpft wurde.

EZB (ECB):
Europäische Zentralbank

-F- *Glossar*

Fernzugangsteilnehmer (remote participant):
Direkter Teilnehmer der Gemeinschaftsplattform, der in dem Land, über das er an der Gemeinschaftsplattform teilnimmt, keine Vertretung hat.

FIFO-Prinzip (First In, First Out):
Zahlungsaufträge werden in der Reihenfolge ihres Eingangs ausgeführt (d. h., der zuerst eingegangene Zahlungsauftrag wird als erstes bearbeitet, der zuletzt eingegangene Auftrag zum Schluss). Maßgeblich ist der Zeitstempel des Zahlungsauftrags bei Eingang in der SWIFT-Schnittstelle der Gemeinschaftsplattform.

FIFO-Überhol-Prinzip (FIFO by-passing):
Das System versucht, den ersten Auftrag in der Warteschlange zu bearbeiten. Ist dies aufgrund fehlender Deckung nicht möglich, versucht das System, stattdessen den nächsten Auftrag abzuwickeln. Dieser Vorgang wird FIFO-Überhol-Prinzip genannt.

-G- *Glossar*

Garantiekonto (guarantee funds account):
Konto auf der Gemeinschaftsplattform, das zur Bereitstellung oder zur Anforderung von Liquidität für den Saldenausgleich eines Nebensystems bei Ausfall der Verrechnungsbank(en) gehalten wird.

Garantiekonto-Verfahren (guarantee fund mechanism):
Verfahren, um nach vorab festgelegten Regeln zusätzlich benötigte Liquidität bereitzustellen, wenn die Abwicklung über ein Nebensystem allein anhand der Liquidität der Verrechnungsbank nicht möglich ist.

Gemeinschaftsplattform (single shared platform – SSP):
TARGET2 basiert auf einer einzigen technischen Plattform, der Gemeinschaftsplattform, die sowohl das Zahlungsabwicklungs- und Kontoführungssystem PAPSS als auch das Kundenbetreuungssystem CRSS umfasst.

Gespeicherter Zahlungsauftrag (warehoused payment):
Zahlungsauftrag, der bis zu fünf TARGET2-Geschäftstage im Voraus eingereicht wird. Die Zahlungsnachricht wird dann bis zur Tagverarbeitung der Gemeinschaftsplattform an dem betreffenden Tag gespeichert.

Grafische Benutzeroberfläche (Graphical User Interface – GUI):
Schnittstelle, die dem Nutzer eine Interaktion mit der T2S-Softwareanwendung ermöglicht, indem grafische Elemente (z. B. Fenster, Menüs, Schaltflächen und/oder Icons) auf einem Computerbildschirm per Tastatur und Maus angesteuert werden.

-H- *Glossar*

Hauptbuch (general ledger):
Das Hauptbuch ist das zentrale Rechnungslegungsdokument eines Unternehmens, das auf dem Prinzip der doppelten Buchführung beruht.

Heimatkonto (home account):
Von nationalen Zentralbanken gehaltenes Konto außerhalb des Zahlungsmoduls, z. B.

- für Einrichtungen, die nicht den Status eines direkten Teilnehmers haben können
- für Einrichtungen, die PM-Konten eröffnen dürfen und indirekte PM-Teilnehmer sind (oder die weder als direkte noch als indirekte Teilnehmer am Zahlungsmodul teilnehmen)
- für PM-Kontoinhaber zum Zwecke der Abwicklung von Vorgängen, die nicht im Zahlungsmodul verarbeitet werden.

Die Heimatkonten werden über das Heimatkontomodul oder über ein proprietäres Heimatkontosystem verwaltet.

Heimatkontomodul (home accounting module – HAM):

Das Heimatkontomodul ist ein optionales Modul. Beschließt eine Zentralbank, dieses Modul zu verwenden, stehen ihr und ihren Kunden verschiedene standardisierte Kontodienste zur Verfügung.

-I- *Glossar*

ICM-Nachricht (broadcast via ICM):
Die Übermittlung einer Information, die allen Teilnehmern oder einer bestimmten Gruppe von Teilnehmern zeitgleich im ICM zur Verfügung gestellt wird.

Informations- und Steuerungsmodul (information and control module – ICM):

Das Informations- und Steuerungsmodul ist eine obligatorische und einheitliche funktionale Schnittstelle zwischen den direkten Teilnehmern und dem Zahlungsmodul (PM) sowie den anderen optionalen Modulen wie dem:

- Heimatkontomodul (HAM)
- Modul für die Mindestreserveverwaltung (RM)
- Modul für die ständigen Fazilitäten (SF)
- Stammdatenmodul (SD)

Innertageskredit (intraday credit):
Kreditgewährung mit einer Laufzeit von weniger als einem Geschäftstag. In einem Überweisungssystem mit Zahlungsausgleich zum Tagesabschluss werden Innertageskredite stillschweigend durch das empfangende Kreditinstitut verlängert, wenn dieses einen Zahlungsauftrag akzeptiert und auf dieser Grundlage agiert, auch wenn es die Mittel erst am Ende des Geschäftstags endgültig erhält. Innertageskredit gibt es als besicherten Überziehungskredit, Kreditgeschäft gegen Pfand oder mit Rückkaufsvereinbarung.

Innertagesliquidität (intraday liquidity):
Liquidität, die während des Geschäftstags zugänglich ist und in der Regel genutzt wird, um Finanzinstituten Zahlungen auf Innertagesbasis zu ermöglichen.

Integrität (integrity):
Schutz vor zufälliger oder betrügerischer Verfälschung im Weiterleitungs- oder Speicherprozess bzw. das Wissen, ob Verfälschungen vorgenommen wurden oder nicht.

Internetbasierter Zugang (internet-based access):
Vereinbarung, im Rahmen derer ein Teilnehmer ein PM- oder HAM-Konto mit ausschließlichem Zugang über das Internet unterhält; in diesem Fall werden Zahlungs- und Kontrollnachrichten an die Gemeinschaftsplattform über das Internet übermittelt.

ISO 20022:
Internationaler Nachrichtenstandard für Finanzdienstleistungen, der von der International Organization for Standardization (ISO) festgelegt wurde.

-J- *Glossar*

Juristische Person (legal entity):
Kreditinstitut, das über einen oder mehrere Teilnehmer/Konten im Zahlungsmodul und/oder Heimatkontomodul direkt an der Gemeinschaftsplattform teilnimmt (auch Nebensysteme, wenn diese als direkte Teilnehmer teilnehmen). Dies ermöglicht eine Gruppierung allgemeiner Informationen zu diesem Kreditinstitut im Stammdatenmodul.

-K- *Glossar*

Kontengruppe (group of accounts):
Siehe *Liquiditätspooling*.

Korrespondenzzentralbank-Modell (correspondent central banking model – CCBM):
Vom Europäischen System der Zentralbanken (ESZB) eingerichtetes Verfahren mit dem Ziel, den Geschäftspartnern die grenzüberschreitende Nutzung von Sicherheiten, die in einem anderen Land hinterlegt sind, für eine Kreditaufnahme bei der nationalen Zentralbank in dem Land, in dem sie selbst niedergelassen sind, zu ermöglichen. Beim Korrespondenzzentralbank-Modell fungieren die nationalen Zentralbanken in Bezug auf Wertpapiere in ihren nationalen Wertpapierabwicklungssystemen füreinander als Verwahrer.

Kreditinstitut (credit institution – CI):
Eine „Bank“ im Sinne der Definition der Europäischen Union. Laut erster Bankenrichtlinie der EG ist ein Kreditinstitut ein Unternehmen, dessen Tätigkeit darin besteht, Einlagen oder andere rückzahlbare Gelder des Publikums entgegenzunehmen und Kredite für eigene Rechnung zu gewähren.

Kreditlinie (credit line):
Die maximale besicherte Überziehung eines PM-Kontos. Die jeweiligen PM-Kontoinhaber können sich anhand des Informations- und Steuerungsmoduls über Veränderungen ihrer Kreditlinien informieren. Veränderungen der Kreditlinien werden unverzüglich umgesetzt. Bei einer Herabsetzung der Kreditlinie bleibt diese Änderung vorerst schwebend, wenn die Senkung zu einer ungedeckten Überziehung führen würde. Die Änderung wird wirksam, sobald die Überziehung durch die gesenkte Kreditlinie gedeckt wird.

Krisenmanager (crisis manager):
In jeder Zentralbank gibt es einen Krisenmanager, der für die Bewältigung außergewöhnlicher Ereignisse zuständig ist.

Kritische Zahlung (critical payment):
Siehe Kasten 4.

-L- *Glossar*

Ländercode (country code – CC):
Ein aus zwei Buchstaben bestehendes Kürzel zur Identifizierung des Landes, in dem die betreffende Einrichtung ansässig ist. Ländercodes werden beispielsweise im SWIFT BIC (fünfte und sechste Stelle) des BIC8 und BIC11 verwendet.

Lastschrift (direct debit):
Autorisierte Belastung des Bankkontos des Zahlungspflichtigen, die vom Zahlungsempfänger ausgelöst wird.

Lieferung gegen Zahlung (delivery versus payment – DVP):
Verbindung zwischen dem Wertpapierübertragungs- und dem Überweisungssystem, die sicherstellt, dass die Lieferung dann und nur dann erfolgt, wenn die Zahlung zustande kommt.

Lieferung mit Gegenwertverrechnung (delivery with payment – DWP):
Ein Weisungs- und Abwicklungsverfahren, das die Lieferung von Wertpapieren und die Leistung der entsprechenden Zahlung erfordert.

Lieferung ohne Gegenwertverrechnung (delivery free of payment – DFP oder DFOP):
Lieferung von Wertpapieren, bei der keine Übertragung entsprechender Mittel erfolgt.

Limit:
Betrag, den ein direkter PM-Teilnehmer bereit ist, für normale Zahlungen an einen anderen direkten Teilnehmer (bilaterales Limit) oder die anderen direkten Teilnehmer (multilaterales Limit, sofern kein bilaterales Limit gesetzt wurde) zu zahlen, ohne vorher Zahlungen (also Gutschriften) erhalten zu haben. Direkte Teilnehmer können ständige oder aktuell laufende bilaterale (bzw. multilaterale) Limite festsetzen.

Normale Zahlungen können nur abgewickelt werden, wenn das jeweilige Limit nicht überschritten wird. Das Setzen von Limiten ist nur gegenüber PM-Kontoinhabern auf der Gemeinschaftsplattform möglich (bei einer Kontengruppe: nur gegenüber dem virtuellen Konto). Gegenüber teilnehmenden Zentralbanken kann kein Limit gesetzt werden. Eingehende dringende Zahlungen eines direkten Teilnehmers, gegenüber dem ein bilaterales/multilaterales Limit gesetzt wurde, beeinflussen auch die bilaterale/multilaterale Position.

Liquiditätspooling (liquidity pooling functionality):
Dienstleistung basierend auf dem Konzept, dass es direkten Teilnehmern ermöglicht werden soll, ihre PM-Konten zu einer Kontengruppe zusammenzulegen. Eine solche Kontengruppe besteht aus einem Konto oder mehreren Konten eines oder mehrerer direkter PM-Teilnehmer mit einer Kapital- und/oder Management-Verbindung. Die folgenden beiden Optionen werden angeboten: virtuelle Konten (nur für Teilnehmer aus dem Euro-Währungsgebiet) und konsolidierte Information (steht auch Teilnehmern aus Ländern außerhalb des Euro-Währungsgebiets zur Verfügung).

Liquiditätsübertragung (liquidity transfer):
Überweisung von Geldern zwischen Konten desselben direkten Teilnehmers oder zwischen zwei Konten einer Kontengruppe.

Die Liquiditätsübertragung stellt auch ein Standard-Abwicklungsverfahren (Verfahren 1) dar, bei dem Liquidität von einem technischen Konto auf das PM-Konto einer Verrechnungsbank oder umgekehrt transferiert wird.

Auf der Gemeinschaftsplattform gibt es zwei Arten der Liquiditätsübertragung:

- Laufender Auftrag: Der Transfer wird sofort nach Auftragseingang ausgeführt, sofern ausreichend Liquidität verfügbar ist.
- Dauerauftrag: Feste Beträge werden regelmäßig zu einem bestimmten Zeitpunkt transferiert, z. B. Liquiditätszuführungen von HAM-Konten auf PM-Konten zu Beginn des Geschäftstags. Die Änderung eines Dauerauftrags wird am folgenden Geschäftstag wirksam.

Auf der T2S-Plattform gibt es drei Arten der Liquiditätsübertragung:

- Auftrag zur sofortigen Liquiditätsübertragung (immediate liquidity transfer order): Weisung, einen bestimmten Geldbetrag in Echtzeit, d. h. unmittelbar bei Eingang der Weisung, von einem Geldkonto auf ein anderes Geldkonto zu übertragen.
- Vorab erstellter Auftrag zur Liquiditätsübertragung (predefined liquidity transfer order): Weisung, einen bestimmten Geldbetrag von einem Geldkonto auf ein anderes Geldkonto zu übertragen, wobei die Weisung einmalig zu einem festgelegten Zeitpunkt oder bei Eintreten eines bestimmten Ereignisses auszuführen ist.
- T2S-Dauerauftrag zur Liquiditätsübertragung (T2S standing liquidity transfer order): Weisung, einen bestimmten Geldbetrag von einem Geldkonto auf ein anderes Geldkonto zu übertragen, wobei die Weisung so lange regelmäßig zu einem festgelegten Zeitpunkt oder bei Eintreten eines bestimmten Ereignisses im T2S-Verarbeitungszyklus auszuführen ist, bis der Auftrag geändert wird.

-M- *Glossar*

MAC:
Message Authentication Code

Mandated Payment:
Zahlung, die von einer nicht an der Transaktion beteiligten Stelle (typischerweise einer nationalen Zentralbank oder einem Nebensystem in Verbindung mit einem AS-Abwicklungsverfahren) im Auftrag einer anderen Stelle veranlasst wird. Beispielsweise versendet eine nationale Zentralbank eine mit einer spezifischen Nachrichtenstruktur versehene Überweisung im Auftrag eines ausgefallenen direkten Teilnehmers (nur in Contingency-Situationen). „Mandated payments" auf technische Konten sind nicht möglich.

Mindestreservepflicht (reserve requirement):
Verpflichtung der Kreditinstitute im Euro-Währungsgebiet, auf einem Mindestreservekonto Mindestreserven bei ihrer nationalen Zentralbank zu unterhalten. Die Mindestreservepflicht wird in Bezug auf bestimmte Positionen in der Bilanz der Kreditinstitute bestimmt. Die Mindestreserveguthaben der Institute werden zum Satz für die Hauptrefinanzierungsgeschäfte des Eurosystems verzinst.

Mindestreservezins- und -strafzinskonto (RM interest and penalty account):
Von einer nationalen Zentralbank gehaltenes (optionales) Konto für Buchungen im Zusammenhang mit der Zahlung von Zinsen auf Mindestreserven sowie mit der Zahlung von Strafzinsen eines Kreditinstituts, das die Mindestreserveanforderungen nicht erfüllt hat.

Modul für die Mindestreserveverwaltung (reserve management module – RM):
Dieses Modul ermöglicht es den nationalen Zentralbanken, einige Funktionen im Zusammenhang mit der Verwaltung der Mindestreserven zu nutzen. So können die Zentralbanken beispielsweise die Erfüllung des Mindestreserve-Solls überprüfen oder die an Kreditinstitute zu zahlenden Zinsen auf die Mindestreserveguthaben berechnen.

Modul für die ständigen Fazilitäten (standing facilities module – SF):
Das Modul für die ständigen Fazilitäten ist ein optionales Modul, das die Verwaltung der ständigen Übernachtfazilitäten (Einlagefazilität, Spitzenrefinanzierungsfazilität) ermöglicht.

-N- *Glossar*

Nachrichtentyp (message type – MT):
Als Nachrichtentyp bezeichnet man eine spezielle Art von SWIFT-Nachrichten, die durch eine dreistellige Zahlenfolge gekennzeichnet ist. Die erste Ziffer gibt die Nachrichtenkategorie an, aus der sich der allgemeine Zweck der Nachricht ablesen lässt. Die zweite Ziffer zeigt die Nachrichtengruppe und die dritte Ziffer die jeweilige Nachrichtenfunktion an.

Nachtverarbeitung (night-time processing):
Zeitraum, in dem AS-Transaktionen abgewickelt werden (Abwicklungsverfahren 6). Die Nachtverarbeitung dauert von 19.30 Uhr bis 7.00 Uhr (mit Ausnahme des Wartungszeitraums von 22.00 Uhr bis 1.00 Uhr).

National Service Desk:
Kontaktstelle für Banken und Nebensysteme bei ihrer nationalen Zentralbank. Der National Service Desk kümmert sich um die Belange der TARGET2-Nutzer im Hinblick auf die Nutzung der Gemeinschaftsplattform, der TIPS-Plattform und der lokalen Infrastrukturen.

Nebensystem (ancillary system – AS):
Ein der Aufsicht und/oder Überwachung durch eine zuständige Behörde unterliegendes, von einer Stelle mit Sitz im Europäischen Wirtschaftsraum (EWR) betriebenes und die Überwachungsanforderungen an den Standort der Infrastrukturen, die Dienstleistungen in Euro anbieten, in der jeweils geltenden und auf der Website der EZB veröffentlichten Fassung erfüllendes System, in dem Zahlungen und/oder Finanzinstrumente eingereicht und/oder ausgeführt oder erfasst werden, wobei gemäß der TARGET2-Leitlinie und einer bilateralen Vereinbarung zwischen dem Nebensystem und der betreffenden Zentralbank des Eurosystems a) die daraus resultierenden Zahlungsverpflichtungen über TARGET2 abgewickelt und/oder b) die Geldbeträge in TARGET2 gehalten werden.

Nebensysteme können sein:

- Massenzahlungsverkehrssysteme
- Großbetragszahlungssysteme
- Devisensysteme
- Geldmarktsysteme
- Clearinghäuser
- Wertpapierabwicklungssysteme

Nebensystemschnittstelle (ancillary system interface – ASI):
Die Nebensystemschnittstelle ist eine standardisierte Schnittstelle zum Zahlungsmodul, über die Nebensysteme einen Zahlungsausgleich ihrer Geschäfte herbeiführen können.

Netting:
Vereinbarte Aufrechnung gegenseitiger Positionen oder Verpflichtungen von direkten Teilnehmern eines Clearing- oder Abwicklungssystems. Das Netting verringert eine große Zahl von Einzelpositionen oder -verpflichtungen auf eine kleinere Zahl. Das Netting kann verschiedene Formen annehmen, deren rechtliche Durchsetzbarkeit bei Ausfall einer der Parteien unterschiedlich ist.

Notenbankfähige Sicherheiten (eligible assets):
Vermögenswerte, die als Sicherheiten für die Kreditaufnahme verwendet werden können.

NSG (national stakeholder groups):
Nationale Stakeholder-Gruppen

NSP (network service provider):
Netzwerkdienstleister

NZB (NCB):
Nationale Zentralbank

-P- *Glossar*

PAPSS (Payment and Accounting Processing Services Systems):
Zahlungsabwicklungs- und Kontoführungssystem

Eine der beiden technischen Konfigurationen der Gemeinschaftsplattform. Die andere ist das Kundenbetreuungssystem CRSS. Folgende Module der Gemeinschaftsplattform sind im PAPSS implementiert:

- Enhanced Contingency Solution (ECONS I)
- Heimatkontomodul (HAM)
- Informations- und Steuerungsmodul (ICM)
- Zahlungsmodul (PM) einschließlich der Schnittstelle für Nebensysteme (ASI)
- Modul für die Mindestreserveverwaltung (RM)
- Modul für die ständigen Fazilitäten (SF)
- Stammdatenmodul (SD)

Teile der folgenden Dienste sind ebenfalls im Zahlungsabwicklungs- und Kontoführungssystem enthalten:

- CRISP
- CRAKS3

Pfand (pledge):
Bereitstellung von Vermögenswerten, um die Erfüllung der Verpflichtung einer Partei (Schuldner) gegenüber einer anderen Partei (Sicherungsnehmer) zu gewährleisten. Ein Pfand räumt ein Sicherungsrecht an den übermittelten Vermögenswerten ein, wobei das Eigentum an diesen Aktiva beim Schuldner verbleibt.

PM-Konto (PM account):
Im Zahlungsmodul verwaltetes und von einem direkten Teilnehmer unterhaltenes Konto zur Abwicklung aller im Zahlungsmodul eingereichten und verarbeiteten Transaktionen (mit Ausnahme der Transaktionen im Rahmen des AS-Abwicklungsverfahrens 6, die über Unterkonten abgewickelt werden).

Prinzipien für Finanzmarktinfrastrukturen (Principles for Financial Market Infrastructures – PFMI):
Internationale Standards für Finanzmarktinfrastrukturen, die vom Ausschuss für Zahlungsverkehr und Marktinfrastrukturen (CPMI) und der Internationalen Organisation der Wertpapieraufsichtsbehörden (IOSCO) herausgegeben wurden.

Priorität (priority):
Im Allgemeinen werden Zahlungen sofort abgewickelt, sofern auf dem PM-Konto des Teilnehmers ausreichend Liquidität vorhanden ist. Je nach Dringlichkeit kann der Sender diesen Zahlungen verschiedene Prioritäten zuordnen:

- sehr dringender Zahlungsauftrag (Prioritätsstufe 0)
- dringender Zahlungsauftrag (Prioritätsstufe 1)
- normaler Zahlungsauftrag (Prioritätsstufe 2)

Zahlungen, die nicht sofort abgewickelt werden können, werden ihrer Dringlichkeit entsprechend in eine Warteschlange gestellt (je eine Warteschlange für sehr dringende, dringende und normale Zahlungsaufträge). Die Prioritätsstufe kann über das Informations- und Steuerungsmodul geändert werden.

Profilinformationen (profiling information):
Den nationalen Zentralbanken zur Verfügung stehende Informationen über das Verhalten eines direkten Teilnehmers oder einer Gruppe direkter Teilnehmer in einem bestimmten Zeitraum in der Vergangenheit. Die Angaben werden zum Abgleich mit den aktuellen Daten an einem beliebigen Geschäftstag herangezogen.

Proprietäres Heimatkonto (proprietary home account – PHA):
Ein proprietäres Heimatkonto ist ein von einigen nationalen Zentralbanken unterhaltenes Konto außerhalb der Gemeinschaftsplattform, z. B. für Einrichtungen, die nicht den Status eines direkten PM-Teilnehmers haben können, für Einrichtungen, die PM-Konten eröffnen dürfen und indirekte PM-Teilnehmer sind (oder die weder als direkte noch als indirekte Teilnehmer am Zahlungsmodul teilnehmen), oder für Inhaber eines PM-Kontos zum Zwecke der Abwicklung von Vorgängen, die nicht im Zahlungsmodul abgewickelt werden. Proprietäre Heimatkonten sind nicht auf der Gemeinschaftsplattform, sondern bei den nationalen Zentralbanken angesiedelt.

-R- *Glossar*

Raw Data File:
Die Raw Data File

- dient als Kontrolldatei zur Überprüfung der Positionen im Hauptbuch;
- kann für eigene Berichte der nationalen Zentralbanken verwendet werden.

Relationship Management Application (RMA):
Siehe *SWIFT Relationship Management Application (RMA)*.

Reserveguthaben (reserve holdings):
Innertages- und Übernachtliquidität, die bei Tagesschluss auf einem RTGS-Konto gehalten wird.

Reservierung (reservation):
Mit der Inanspruchnahme der Liquiditätsreservierung kann der Inhaber eines RTGS-Kontos Liquidität für spezielle Transaktionen mit einer bestimmten Prioritätsstufe reservieren. HAM-Kontoinhaber können diesen Service nutzen, um Liquidität für Barabhebungen zu reservieren. Reservierungen können über das Informations- und Steuerungsmodul vorgenommen und geändert werden.

Rolle (role):
Eine Gruppe von Berechtigungen (siehe auch *Berechtigung*).

RTGS (real-time gross settlement system):
Echtzeit-Bruttosystem

Rückkaufsvereinbarung (Repogeschäft) (repurchase agreement – Repo):
Vereinbarung über den Verkauf eines Vermögenswerts und dessen Rückkauf zu einem bestimmten Preis zu einem vorher festgelegten Zeitpunkt.

-S- *Glossar*

SCT^{Inst}:
SEPA Instant Credit Transfer

Sehr kritische Zahlung (very critical payment):
Siehe Kasten 4.

Selbstbesicherung (auto-collateralisation):
Die Selbstbesicherung ist ein spezieller Mechanismus, um zusätzliche Liquidität für das Wertpapierabwicklungsverfahren bereitzustellen. Dieser Mechanismus beruht auf der automatischen Interaktion zwischen dem Sicherheitenverwalter, dem Wertpapierabwicklungssystem und der Gemeinschaftsplattform, um Besicherungsfunktionen (z. B. Prüfung der Notenbankfähigkeit, Bewertung von Sicherheiten) und die damit verbundene Erhöhung der Liquidität durchzuführen.

Die Selbstbesicherung wird während des Wertpapierabwicklungsverfahrens aktiviert, um der Liquiditätsknappheit eines Teilnehmers zu begegnen: Die zu übertragende Sicherheit wird im Auftrag des Teilnehmers auf der Grundlage einer vorab erteilten Ermächtigung automatisch vom Wertpapierabwicklungssystem ausgewählt.

Die Wertpapierabwicklungssysteme verwenden derzeit zwei verschiedene Selbstbesicherungsverfahren:

- Selbstbesicherung aus Beständen: Die Teilnehmer wählen die verwendbaren notenbankfähigen Wertpapiere aus.
- Selbstbesicherung aus Strömen: Die Wertpapiere ergeben sich aus dem Abwicklungsverfahren selbst.

Settlement-Manager:
Jede Zentralbank hat einen Settlement-Manager, der für die Verwaltung und Überwachung sowie für die Kommunikation mit anderen Settlement-Managern innerhalb des Eurosystems verantwortlich ist.

Sicherheiten (collateral):
Sicherheiten sind Vermögenswerte oder die Verpflichtung eines Dritten, die vom Sicherungsnehmer zur Besicherung einer Verbindlichkeit des Sicherungsgebers gegenüber dem Sicherungsnehmer akzeptiert wird. Besicherungsvereinbarungen können verschiedene rechtliche Formen haben und als Übereignung oder Pfand auftreten.

Sicherheitenpool (collateral pool):
Vermögenswerte im Besitz der Teilnehmer eines Übertragungssystems, die diesen zu Besicherungszwecken gemeinschaftlich zur Verfügung stehen, damit sie sich nach genau festgelegten Regeln Liquidität beschaffen können.

SIRPS (systemically important retail payment systems):
Systemrelevante Massenzahlungsverkehrssysteme

Spiegelkonto (mirror account):
Spezielle PM-Konten, die den nationalen Zentralbanken eigens zur Nutzung von Nebensystemen zur Verfügung stehen. Spiegelkonten werden durch ein anderes im Wertpapierabwicklungssystem eröffnetes Konto gespiegelt. Im Fall einer Liquiditätsübertragung vom Konto eines direkten Teilnehmers im Zahlungsmodul auf sein Konto im Nebensystem wird der entsprechende Betrag dem Spiegelkonto belastet oder gutgeschrieben.

Spitzenrefinanzierungsfazilität (marginal lending facility):
Ständige Fazilität des Eurosystems, die die Geschäftspartner nutzen können, um sich von einer nationalen Zentralbank gegen notenbankfähige Sicherheiten Übernachtkredit zu einem im Voraus festgelegten Zinssatz zu beschaffen.

Im Allgemeinen stehen folgende Möglichkeiten zur Verfügung:

- Inanspruchnahme der Spitzenrefinanzierungsfazilität auf Antrag des direkten Teilnehmers, meist zur Erfüllung der Mindestreservepflicht.
- Automatisierte Inanspruchnahme der Spitzenrefinanzierungsfazilität (Übernachtkredit), wobei der Innertageskredit am Ende des Tages automatisch in Übernachtkredit umgewandelt wird.

Ständige Fazilität (standing facility):
Zentralbankfazilität, die die Geschäftspartner auf eigene Initiative in Anspruch nehmen können. Das Eurosystem bietet zwei ständige Übernachtfazilitäten an, und zwar die Spitzenrefinanzierungsfazilität und die Einlagefazilität.

Stammdatenmodul (static data module – SD):
Mithilfe des Stammdatenmoduls werden die Stammdaten durch Speicherung aller tatsächlich verwendeten statistischen Daten ordnungsgemäß und zuverlässig verwaltet. Es gewährleistet die Konsistenz der Daten in allen Modulen der Gemeinschaftsplattform. Das Stammdatenmodul wird unter anderem zur Erstellung des TARGET2-Directory genutzt.

SWIFT:
Society for Worldwide Interbank Financial Telecommunication

SWIFT Alliance Access (SAA):
SWIFT Alliance Access ist eine Nachrichtenschnittstelle, die es dem Anwender ermöglicht, eigene Anwendungen mit SWIFTNet FIN (MT) und MX-basierten SWIFT-Lösungen zu verbinden.

SWIFT Alliance Gateway (SAG):
SWIFT Alliance Gateway ist das einheitliche Fenster für jede Kommunikation über SWIFTNet. Alle SWIFTNet-Nachrichtenströme können über eine Schnittstelle zusammengeführt werden. Dies betrifft Anwendungen, die über WebSphere MQ angebunden sind, aber auch solche, die für eine Verbindung mit SWIFTNet Link bestimmt sind oder auf SWIFT Alliance WebStation basieren.

SWIFT-BIC (Business Identifier Code):
Identifikationscode von an das SWIFT-Netzwerk angeschlossenen Finanzinstituten und Unternehmen (ehemals „Bankidentifikationscode“ für Finanzinstitute).

SWIFTNet FileAct:
SWIFTNet FileAct ermöglicht die Übermittlung von Dateien und wird in der Regel zum stapelweisen Austausch strukturierter Finanznachrichten und umfangreicher Berichte verwendet. Auf der Gemeinschaftsplattform wird beispielweise das TARGET2-Directory mithilfe des FileAct-Service über das Secure IP Network (SIPN) von SWIFT transferiert.

SWIFTNet InterAct:
Ein interaktiver Nachrichtendienst von SWIFT, der den Austausch von Nachrichten zwischen zwei Parteien unterstützt. Auf der Gemeinschaftsplattform wird der InterAct Service verwendet, um XML-Anfragen über das Secure IP Network (SIPN) von SWIFT an das Informations- und Steuerungsmodul zu übermitteln.

SWIFT Relationship Management Application (RMA):
Von SWIFT angebotener Dienst zur Verwaltung der Geschäftsbeziehungen zwischen Finanzinstituten. Die RMA steuert, welche Nachrichtentypen zwischen den Anwendern eines SWIFT-Dienstes ausgetauscht werden dürfen.

SWIFT WebAccess
Ein bildschirmbasierter Kanal für den Zugriff auf Web-Anwendungen über SWIFT unter Verwendung der vorhandenen SWIFTNet-Infrastruktur des Kunden.

SWIFT-Zahlungsnachricht (SWIFT payment message):
Auftrag zur Überweisung eines Geldbetrags. Der Austausch von Mitteln (Abwicklung) erfolgt anschließend über ein Zahlungssystem oder über Korrespondenzbankbeziehungen. SWIFT-Zahlungsnachrichten werden für alle Zahlungen und die damit verbundenen Transaktionen auf der Gemeinschaftsplattform eingesetzt.

-T- *Glossar*

T2S-Abwicklungswährung (T2S settlement currency):
Währung, für die T2S die Abwicklung von Wertpapiertransaktionen in Zentralbankgeld auf T2S-Geldkonten anbietet.

T2S-Beteiligter (T2S actor):
Entweder ein vertragschließender/teilnehmender Zentralverwahrer, CSD-Teilnehmer (eine juristische oder gegebenenfalls natürliche Person), der für die Zwecke der Wertpapierabwicklung in T2S ein Vertragsverhältnis zum Zentralverwahrer unterhält, eine Zentralbank, deren Währung für die abwicklungsbezogenen Aktivitäten in T2S zur Verfügung steht, oder ein Kunde einer Zentralbank, der für die Zwecke der mit der Abwicklung verbundenen Geldverrechnung in T2S ein Vertragsverhältnis zur Zentralbank unterhält.

T2S-Betreiber (T2S operator):
Die rechtliche(n) und/oder organisatorische(n) Stelle(n), die die T2S-Plattform betreibt/betreiben. Im Rahmen der Aufgabenverteilung innerhalb des Eurosystems hat der EZB-Rat die 4ZB damit beauftragt, T2S im Namen des Eurosystems zu betreiben.

T2S-Geldkonto (T2S dedicated cash account – T2S DCA):
Ein in den Büchern einer Zentralbank geführtes T2S-Geldkonto.

T2S-Geldkontoinhaber (T2S DCA holder):
Eine Stelle, die bei einer Zentralbank mindestens ein T2S-Geldkonto in T2S eröffnet hat.

T2S-GUI-Nachricht (broadcast via T2S GUI):
Die Übermittlung einer Information, die einer bestimmten Gruppe von Teilnehmern zeitgleich auf der grafischen Benutzeroberfläche von T2S zur Verfügung gestellt wird.

T2SI (T2S Interface):
T2S-Schnittstelle in TARGET2

T2S-Partei (T2S party):
Eine juristische Person oder Organisation, die direkt oder indirekt (d. h. über einen Zentralverwahrer oder eine Zentralbank) in T2S aktiv ist.

T2SRC (TARGET2 security requirements and controls):
TARGET2-Sicherheitsanforderungen und -kontrollen

T2S Service Desk:
Zentraler Ansprechpartner für die Zentralverwahrer, die Zentralbanken, die nicht dem Euro-Währungsgebiet angehören und ihre Währung für die Abwicklungsaktivitäten in T2S bereitstellen, die Zentralbanken des Eurosystems, die direkt angeschlossenen Teilnehmer und die Netzwerkdienstleister bei allen Vorfällen, Anfragen und Anträgen, die sich auf den Betrieb, die Funktion oder technische Aspekte von T2S beziehen. Für alle geldbezogenen Fragen, mit Ausnahme von Konnektivitätsfragen, wird auf die TARGET2-Organisationsstruktur verwiesen.

T2S-System-Entität (T2S system entity):
Entweder der Betreiber von T2S, ein Zentralverwahrer oder eine nationale Zentralbank, bei denen Verarbeitungsfunktionen und Daten voneinander getrennt sein müssen.

T2S-Systemnutzer (T2S system user):
Eine natürliche Person oder ein technischer Prozess/eine technische Anwendung, die sich mit Nutzernamen und Passwort bei T2S anmelden können. Bei einem Nutzer kann es sich z. B. um eine natürliche Person handeln, die einen interaktiven Zugang zu T2S-Online-Funktionen hat, oder um eine Anwendungssoftware, die bei T2S Dienste anfordert.

Tagverarbeitung (day trade phase):
Als Tagverarbeitung bezeichnet man in TARGET2 die Zeit von 7.00 Uhr bis 18.00 Uhr.

TARGET:
Transeuropäisches automatisiertes Echtzeit-Brutto-Express-Zahlungssystem

TARGET2:
TARGET2 ist die zweite TARGET-Generation und ersetzt die ehemals dezentrale Infrastruktur durch eine gemeinsame technische Plattform.

TARGET2-Directory:
Von den TARGET2-Nutzern verwendetes Verzeichnis zur Adressierung von Zahlungen anhand des SWIFTNet Y-Copy Mode. Auf einzelstaatlicher Ebene kann mithilfe des Directory anhand der nationalen Bankleitzahl der zugehörige BIC ermittelt werden.

TARGET2-Geschäftstag (TARGET2 business day):
TARGET2-Geschäftstage sind Kalendertage, an denen das TARGET2-System in Betrieb ist.

TARGET2-Securities (T2S):
Die Gesamtheit der Hardware-, Software- und sonstigen technischen Infrastrukturkomponenten, durch die das Eurosystem Dienstleistungen für Zentralverwahrer und Zentralbanken erbringt, die es ermöglichen, grundlegende Abwicklungsdienste in Zentralbankgeld grenzüberschreitend und marktneutral auf Basis Lieferung gegen Zahlung anzubieten.

TARGET Instant Payment Settlement (TIPS):
Abwicklung von Instant-Zahlungsaufträgen in Zentralbankgeld über die TIPS-Plattform.

Technisches Konto (technical account):
Konto, das im Zusammenhang mit Nebensystem-Transaktionen als Zwischenkonto verwendet wird. Darauf werden Belastungen und Gutschriften verbucht, die sich aus einem Saldenausgleich oder Transaktionen auf Basis Lieferung gegen Zahlung ergeben. Der Saldo eines solchen Kontos ist immer null, da auf Belastungen (bzw. Gutschriften) stets Gutschriften (bzw. Belastungen) in insgesamt gleicher Höhe folgen.

Technisches Konto des Nebensystems (AS technical account):
In TARGET2 und TIPS angebotenes Konto zur spezifischen Nutzung von Nebensystemen.

Teilnehmer mit internetbasiertem Zugang (internet-based participant – IBP):
Teilnehmer, der über einen internetbasierten Zugang zu seinem PM- oder Heimatkonto verfügt.

TIPS-Geldkonto (TIPS dedicated cash account – TIPS DCA):
Ein in den Büchern einer Zentralbank geführtes Konto eines TIPS-Geldkontoinhabers, das zur Abwicklung von Instant-Zahlungen für die Kunden genutzt wird.

TIPS-Geldkontoinhaber (TIPS DCA holder):
Eine Stelle, die bei einer Zentralbank mindestens ein TIPS-Geldkonto in TIPS eröffnet hat.

TIPS-Netzwerkdienstleister (TIPS network service provider):
Ein Unternehmen, das a) eine technische Verbindung eingerichtet hat und alle erforderlichen Bedingungen erfüllt, um sich mit der TIPS-Plattform gemäß den maßgeblichen Bestimmungen und Verfahren zu verbinden, und b) die auf der Website der EZB abrufbaren TIPS-Connectivity-Hosting-Bedingungen unterzeichnet hat.

TIPS-Plattform (TIPS platform):
Gemeinsame technische Plattforminfrastruktur, die von den Anbieter-NZBen der TIPS-Plattform bereitgestellt wird.

Transaktionsreferenznummer (transaction reference number – TRN):
Alphanumerische Referenznummer mit bis zu 16 Stellen, die der Sender über das SWIFT-Netzwerk gesendeten Nachrichten zuordnet.

-U- *Glossar*

Übertragung (transfer):
Operational das Versenden (bzw. Bewegen) von Geldern oder Wertpapieren oder eines Rechts an Geldern oder Wertpapieren von einer Partei an eine andere durch: physische Übertragung von Wertpapieren/Geld, Verbuchung beim Finanzintermediär, Verbuchung in einem Überweisungs- und/oder Wertpapierübertragungssystem.

Der Akt der Übertragung wirkt sich hinsichtlich des übertragenen Geldbetrags, Wertpapiers oder Finanzinstruments auf die Rechte des Übertragenden, des Empfängers und möglicherweise auch Dritter aus.

Überweisung (credit transfer):
Geldtransfer auf Basis eines Zahlungsauftrags oder mitunter einer Reihe von Zahlungsaufträgen, um dem Empfänger finanzielle Mittel zur Verfügung zu stellen. Der Zahlungsauftrag kann über mehrere Intermediäre und/oder über ein oder mehrere Überweisungssysteme abgewickelt werden.

Unsecured Credit Limit:
Von der Payment Bank/Verrechnungsbank für ihren Kunden festgelegte Obergrenze für unbesicherte Kredite in T2S. Das External Guarantee Limit und das Unsecured Credit Limit sind aus der Sicht von T2S identisch. Sie unterscheiden sich nur hinsichtlich der Reihenfolge ihrer Inanspruchnahme, wobei das Unsecured Credit Limit genutzt wird, nachdem die Client Collateralisation ausgeschöpft wurde.

Unterkonto (sub-account):
Zu einem PM-Konto gehörendes spezielles Konto, auf dem dedizierte Liquidität gehalten wird, um den Ausgleich eines Nebensystems zu ermöglichen.

User Handbook (UHB):
Dokument, in dem beschrieben wird, wie T2S-Nutzer eine Reihe von T2S-Software-Funktionen nutzen können, die in einem (bildschirmbasierten) User-to-Application-Modus verfügbar sind.

User-to-Application (U2A):
Ziel ist die direkte Kommunikation zwischen den Anwendern eines Teilnehmers und dem ICM. Die Informationen werden in einem Browser angezeigt, der auf einem PC-System läuft. Kontrollen werden vom Anwender manuell vorgenommen.

-V- *Glossar*

VA-NSP (value-added network service provider):
Anbieter von Mehrwertnetzwerkdiensten für T2S

VAS (value-added services):

TARGET2-Zusatzleistungen für T2S

Verfügbare Liquidität (available liquidity):
Kontoguthaben zuzüglich der besicherten Überziehungskreditlinie (falls verfügbar).

Verlängerung des Annahmeschlusses (delayed closing):
Die Verlängerung der Annahmeschlusszeit ist eine Verlängerung der Tagverarbeitung in TARGET2.

Verschlüsselung (encryption):
Als Verschlüsselung bezeichnet man den Gebrauch kryptografischer Algorithmen zur Umwandlung eines lesbaren Textes (Klartext) in einen verschlüsselten Text, um ihn vor unbefugtem Zugriff zu schützen.

Verwahrstelle (depository):

Einrichtung mit der Hauptfunktion, Wertpapiere entweder effektiv oder elektronisch zu verwahren. Die Verwahrstelle kann auch über das Eigentum an diesen Wertpapieren Buch führen.

Virtuelles Konto (virtual account):
Methode zur Aggregation von Daten innerhalb einer Gruppe von Konten, die bei einer Zentralbank im Euro-Währungsgebiet gehalten werden. Zahlungen, die von Kontoinhabern im Rahmen eines virtuellen Kontos getätigt werden, werden im Hinblick auf die Gesamtliquidität des virtuellen Kontos überprüft. Diese entspricht der Summe der verfügbaren Liquidität aller Konten, aus denen sich das virtuelle Konto

zusammensetzt.

-W- *Glossar*

Warteschlangenverfahren (queuing):
Verfahren, mit dessen Hilfe Überweisungsaufträge vom sendenden direkten Teilnehmer oder vom System in einer Warteposition gehalten werden, bis sie entsprechend den Systemregeln verarbeitet werden können.

Wertpapierabwicklungssystem (securities settlement system – SSS):
Das Wertpapierabwicklungssystem umfasst die Gesamtheit aller institutionellen Regelungen für die Bestätigung, das Clearing, die Abwicklung sowie die Verwahrung und Registrierung von Wertpapieren.

-X- *Glossar*

XML:
Akronym für „Extensible Markup Language". Untereinheit der „Standard Generalized Markup Language" (SGML, ISO 8879), die speziell für die Verwendung im Internet sowie für webbasierte Anwendungen entwickelt wurde.

-Y- *Glossar*

Y-Copy:
Standard-Übertragungsart von SWIFT-Nachrichten an die Gemeinschaftsplattform. Sie wird bei über das Zahlungsmodul verarbeiteten Zahlungen verwendet.

-Z- *Glossar*

Zahlung (payment):
Die Gemeinschaftsplattform ermöglicht direkten Teilnehmern generell zwei Arten von Zahlungen:

- Kundenzahlungen (MT 103, MT 103 STP (vormals: MT 103+))
- Bank-an-Bank-Zahlungen (MT 202, MT 202 COV, MT 204).

Zahlungsblockade (gridlock):
Situation, die sich bei einem Geld- oder Wertpapierübertragungssystem ergeben kann, wenn einige Übertragungsaufträge nicht ausgeführt werden können (weil die nötigen Geld- oder Wertpapierguthaben nicht verfügbar sind) und dies dazu führt, dass eine beträchtliche Anzahl von Aufträgen anderer Teilnehmer ebenfalls nicht ausgeführt werden kann.

Zahlungsmodul (payments module – PM):
Das Zahlungsmodul ist ein obligatorisches Modul zur Abwicklung von Zahlungen in PM-Konten, die von allen direkten Teilnehmern unterhalten werden. Darüber hinaus bietet das Zahlungsmodul erweiterte Dienstleistungen zur Liquiditätssteuerung sowie zur Kommunikation mit direkten Teilnehmern und Nebensystemen.

Zahlungsnachricht/-auftrag (payment message/instruction):
Auftrag oder Nachricht zur Übertragung von Mitteln (in Form einer Geldforderung an eine Partei) an die Order des Zahlungsempfängers. In TARGET2 kann sich der Auftrag entweder auf eine Überweisung oder auf eine Lastschrift beziehen.

Zentralbank-Selbstbesicherung (Central Bank auto-collateralisation):
Von der Zentralbank bereitgestellter besicherter Innertageskredit. Die Selbstbesicherung bei einem T2S-Geldkontoinhaber wird als Client Collateralisation bezeichnet.

Zentraler Kontrahent (central counterparty – CCP):
Der zentrale Kontrahent agiert bei Handelsgeschäften an einem oder mehreren Finanzmärkten als Schaltstelle zwischen den Geschäftspartnern; dabei tritt er gegenüber jedem Verkäufer als Käufer und gegenüber jedem Käufer als Verkäufer auf.

Zentralverwahrer (central securities depository – CSD):
Eine zentrale Wertpapierverwahrstelle ist eine Einrichtung, die verbriefte und unverbriefte Wertpapiere hält, um die buchmäßige Übertragung von Wertpapieren zu ermöglichen. Neben der Verwahrung und Verwaltung von Wertpapieren kann ein Zentralverwahrer auch Clearing- und Abwicklungsfunktionen sowie Schuldendienstaufgaben wahrnehmen.