BESONDERE GESCHÄFTSBEDINGUNGEN FÜR DIE ERÖFFNUNG UND FÜHRUNG EINES PM-KONTOS IN TARGET2-BUNDESBANK (TARGET2-BBk) IM RAHMEN DES INTERNETBASIERTEN ZUGANGS

TITEL I

ALLGEMEINE BESTIMMUNGEN

Artikel 1 – Begriffsbestimmungen

In diesen Geschäftsbedingungen (nachfolgend „Bedingungen“) gelten die folgenden Begriffsbestimmungen:

- ‚Abbuchungsermächtigung‘ (‚direct debit authorisation‘): eine allgemeine Weisung/Anweisung eines Zahlers an seine Zentralbank, aufgrund derer die Zentralbank berechtigt und verpflichtet ist, das Konto des Zahlers bei Erhalt eines gültigen Lastschriftauftrags des Zahlungsempfängers zu belasten „AL-Gruppe“ (*AL group*): eine Gruppe, die aus AL-Gruppenmitgliedern besteht, die das AL-Verfahren nutzen;
- „AL-Gruppenmitglied“ (*AL group member*): ein TARGET2-Teilnehmer, der eine AL-Vereinbarung geschlossen hat;
- „AL-NZB“ (*AL NCB*): eine teilnehmende NZB, die Vertragspartei einer AL-Vereinbarung und Geschäftspartner der an ihrem TARGET2-Komponenten-System teilnehmenden AL-Gruppenmitglieder ist;
- „AL-Vereinbarung“ (*AL agreement*): multilaterale Vereinbarung über die Aggregierung von Deckungsmitteln (*aggregated liquidity* – AL) im AL-Verfahren, die zwischen den AL-Gruppenmitgliedern und ihren jeweiligen AL-NZBen (nationale Zentralbanken) geschlossen wurde;
- „AL-Verfahren“ (*AL mode*): die Aggregierung von Deckungsmitteln auf PM-Konten;
- „Anbieter-Zentralbanken“ (*SSP-providing CBs*): die Deutsche Bundesbank, die Banca d’Italia sowie die Banque de France in ihrer Eigenschaft als Anbieter und Betreiber der SSP für das Eurosystem;
- „Anbieter-NZBen der TIPS-Plattform“ (*TIPS Platform-providing NCBs*): die Deutsche Bundesbank, die Banco de España, die Banque de France sowie die Banca d’Italia in ihrer Eigenschaft als Anbieter und Betreiber der TIPS-Plattform für das Eurosystem;
- „angeschlossene Zentralbank“ (*connected CB*): eine NZB, die keine Zentralbank des Eurosystems ist und aufgrund einer besonderen Vereinbarung an TARGET2 angeschlossen ist;
- „Ausfallereignis“ (*event of default*): jedes bevorstehende oder bereits eingetretene Ereignis, durch welches ein Teilnehmer seine Verpflichtungen gemäß diesen Bedingungen oder sonstigen

Bestimmungen nicht erfüllen kann, die im Verhältnis zwischen ihm und der Deutschen Bundesbank oder anderen Zentralbanken gelten, zum Beispiel:

a) wenn ein Teilnehmer die in Artikel 4 festgelegten Zugangsvoraussetzungen oder die in Artikel 7 Absatz 1 Buchstabe a Ziffer i genannten Anforderungen nicht mehr erfüllt;

b) bei Eröffnung eines Insolvenzverfahrens über das Vermögen des Teilnehmers;

c) wenn ein Antrag auf Eröffnung des in Buchstabe b genannten Verfahrens gestellt wird;

d) wenn ein Teilnehmer schriftlich erklärt, dass er nicht mehr in der Lage ist, seine Verbindlichkeiten ganz oder teilweise zu erfüllen oder seinen Verpflichtungen aus der Inanspruchnahme von Innertageskredit nachzukommen;

e) wenn ein Teilnehmer eine umfassende außergerichtliche Schuldenregelung mit seinen Gläubigern trifft;

f) wenn ein Teilnehmer zahlungsunfähig ist oder seine Zentralbank ihn für zahlungsunfähig hält;

g) wenn über das Guthaben des Teilnehmers auf dem PM-Konto, das Vermögen des Teilnehmers oder wesentliche Teile davon Sicherungsmaßnahmen wie verfügungsbeschränkende Maßnahmen, Pfändungen oder Beschlagnahmen oder andere Maßnahmen im öffentlichen Interesse oder zum Schutz der Rechte der Gläubiger des Teilnehmers ergangen sind;

h) wenn ein Teilnehmer von der Teilnahme an einem anderen TARGET2-Komponenten-System und/oder einem Nebensystem suspendiert oder ausgeschlossen wurde;

i) wenn wesentliche Zusicherungen oder wesentliche vorvertragliche Erklärungen, die der Teilnehmer abgegeben hat oder die nach geltendem Recht als vom Teilnehmer abgegeben gelten, sich als unrichtig erweisen,

j) bei Abtretung des ganzen Vermögens des Teilnehmers oder wesentlicher Teile davon;

- „Business Identifier Code – BIC“: ein in der ISO-Norm 9362 festgelegter Code;
- „CAI-Verfahren“ (*CAI mode*): das Verfahren, in dem über das Informations- und Kontrollmodul (ICM) konsolidierte Konteninformationen (*Consolidated Account Information* – CAI) in Bezug auf PM-Konten zur Verfügung gestellt werden;
- „Eingangsdisposition“ (*entry disposition*): eine Phase der Zahlungsverarbeitung, während der TARGET2-BBk versucht, einen gemäß Artikel 13 angenommenen Zahlungsauftrag durch spezifische Verfahren gemäß Artikel 19 abzuwickeln;
- „Einlagefazilität“ (*deposit facility*): eine ständige Fazilität des Eurosystems, die den Geschäftspartnern die Möglichkeit bietet, täglich fällige Einlagen zu einem im Voraus festgelegten Einlagesatz bei einer NZB anzulegen“;
- „Einlagesatz“ (*deposit facility rate*): der Zinssatz für die Einlagefazilität;
- „einreichender Teilnehmer” (*instructing participant*): ein TARGET2-Teilnehmer, der einen Zahlungsauftrag eingereicht hat;

- „elektronische Zertifikate“ (*electronic certificates*) oder „Zertifikate“ (*certificates*): eine von den Zertifizierungsstellen ausgestellte elektronische Datei, die einen Public Key mit einer Identität verbindet und die für die folgenden Zwecke verwendet wird: zur Überprüfung, dass ein Public Key zu einer bestimmten Person gehört, zur Authentifizierung des Inhabers, zur Überprüfung einer Signatur dieser Person oder zur Verschlüsselung einer an diese Person gerichteten Nachricht. Die Zertifikate werden auf einem physischen Speichermedium wie einer Smart Card oder einem USB-Stick gespeichert. Verweise auf Zertifikate schließen diese physischen Speichermedien ein. Die Zertifikate werden im Authentifizierungsverfahren der Teilnehmer eingesetzt, die über das Internet auf TARGET2 zugreifen und Zahlungs- oder Kontrollnachrichten übermitteln;
- „erreichbare Partei“ (*reachable party*): eine Stelle, die a) Inhaberin eines Business Identifier Code (BIC) ist, b) von einem TIPS-Geldkontoinhaber oder durch ein Nebensystem als erreichbare Partei bestimmt wird, c) Korrespondent, Kunde oder Zweigstelle eines TIPS-Geldkontoinhabers, oder Teilnehmer eines Nebensystems, oder Korrespondent, Kunde oder Zweigstelle eines Teilnehmers eines Nebensystems ist und d) entweder über den TIPS-Geldkontoinhaber oder das Nebensystem Instant Payment-Aufträge oder, falls eine entsprechende Genehmigung des TIPS-Geldkontoinhabers oder des Nebensystems erteilt wurde, direkt Instant Payment-Aufträge bei der TIPS-Plattform einreichen und über diese Zahlungen empfangen kann;
- „erreichbarer BIC-Inhaber“ (*addressable BIC holder*): eine Stelle, die a) Inhaberin eines Business Identifier Code (BIC), b) nicht als indirekter Teilnehmer des PM anerkannt und c) Korrespondent oder Kunde eines PM-Kontoinhabers oder eine Zweigstelle eines direkten oder indirekten Teilnehmer des PM ist und die über den PM-Kontoinhaber Zahlungsaufträge bei einem TARGET2-Komponenten-System einreichen und über dieses Zahlungen empfangen kann;
- „Finalitätsrichtlinie“ (*Settlement Finality Directive*): die Richtlinie 98/26/EG des Europäischen Parlaments und des Rates vom 19. Mai 1998 über die Wirksamkeit von Abrechnungen in Zahlungs- sowie Wertpapierliefer- und -abrechnungssystemen[1];
- „Gemeinschaftsplattform“ (*Single Shared Platform* – SSP): die einheitliche technische Plattform, die von den Anbieter-Zentralbanken zur Verfügung gestellt wird;
- „Geschäftstag“ („business day“) oder „TARGET2-Geschäftstag“ („TARGET2 business day“): jeder Tag, an dem TARGET2 gemäß Anlage V zur Abwicklung von Zahlungsaufträgen geöffnet ist;
- „Gruppe“ (*group*):
  a) eine Gruppe von Kreditinstituten, deren Jahresabschlüsse in den konsolidierten Abschluss bei einem Mutterunternehmen eingehen, sofern das Mutterunternehmen den konsolidierten Abschluss gemäß der Verordnung (EG) Nr. 1126/2008 der Kommission[2] nach dem

[1] ABl. L 166 vom 11.6.1998, S. 45.

[2] Verordnung (EG) Nr. 1126/2008 der Kommission vom 3. November 2008 zur Übernahme bestimmter internationaler Rechnungslegungsstandards gemäß der Verordnung (EG) Nr. 1606/2002 des Europäischen Parlaments und des Rates (ABl. L 320 vom 29.11.2008, S. 1).

International Accounting Standard (IAS) 27 erstellt, wobei die Gruppe sich wie folgt zusammensetzen muss:

i) ein Mutterunternehmen und ein oder mehrere Tochterunternehmen oder

ii) zwei oder mehr Tochterunternehmen desselben Mutterunternehmens, oder

b) eine Gruppe von Kreditinstituten im Sinne von Buchstabe a Ziffer i oder ii, wobei das Mutterunternehmen zwar keinen konsolidierten Abschluss gemäß IAS 27 erstellt, jedoch die in IAS 27 festgelegten Kriterien für einen konsolidierten Abschluss erfüllt wären, vorbehaltlich der Bestätigung durch die Zentralbank des direkten Teilnehmers oder, im Falle einer AL-Gruppe, der Leit-NZB, oder

c) ein bilaterales oder multilaterales Netzwerk von Kreditinstituten,

i) bei dem die Zugehörigkeit von Kreditinstituten zum Netzwerk gesetzlich oder satzungsmäßig organisiert und geregelt ist; oder

ii) dessen Wesensmerkmal die selbst organisierte Zusammenarbeit (Förderung, Unterstützung und Vertretung der Geschäftsinteressen seiner Mitglieder) und/oder eine über die übliche Zusammenarbeit zwischen Kreditinstituten hinausgehende wirtschaftliche Solidarität ist, wobei die Zusammenarbeit bzw. Solidarität aufgrund der Satzung oder des Gründungsakts der betreffenden Kreditinstitute oder aufgrund von separaten Vereinbarungen ermöglicht wird.

In jedem in Buchstabe c genannten Fall ist erforderlich, dass der EZB-Rat das Netzwerk als Gruppe im Sinne dieser Definition anerkannt hat;

- „Heimatkonto“ (*Home Account*): ein Konto, das von einer NZB des Euro-Währungsgebiets für Kreditinstitute mit Sitz in der Union oder dem EWR außerhalb des PM eröffnet wird;
- „ICM-Nachricht“ (*ICM broadcast message*): Informationen, die allen oder bestimmten PM-Kontoinhabern über das ICM zeitgleich zur Verfügung gestellt werden;
- „indirekter Teilnehmer“ (*indirect participant*): ein Kreditinstitut mit Sitz oder Zweigstelle in der Union oder im EWR, das mit einem direkten Teilnehmer vereinbart hat, über das PM-Konto des direkten Teilnehmers Zahlungsaufträge einzureichen oder Zahlungen zu empfangen, wobei das Kreditinstitut von einem TARGET2-Komponenten-System als indirekter Teilnehmer erkannt wird;
- „Informations- und Kontrollmodul“ (‚Information and Control Module‘ – ICM): das SSP-Modul, das es PM-Kontoinhabern ermöglicht, online Informationen zu erhalten, Liquiditätsüberträge in Auftrag zu geben, Liquidität zu steuern und gegebenenfalls in Notfällen Ersatzzahlungen oder Zahlungen in der Notfalllösung zu veranlassen;
- „Innertageskredit“ (*intraday credit*): die Kreditgewährung mit einer Laufzeit von weniger als einem Geschäftstag;
- „Insolvenzverfahren“ (*insolvency proceedings*): Insolvenzverfahren im Sinne von Artikel 2 Buchstabe j der Finalitätsrichtlinie;
- „internetbasierter Zugang“ (*internet based access*): auf Antrag des Teilnehmers kann für sein PM-

Konto ein ausschließlicher Zugang über das Internet eingerichtet werden; in diesem Fall übermittelt der Teilnehmer Zahlungs- oder Kontrollnachrichten an TARGET2 über das Internet;

- „Internetdienstleister“ (*internet service provider*): das Unternehmen oder die Institution, das bzw. die vom TARGET2-Teilnehmer genutzt wird, um im Rahmen des internetbasierten Zugangs auf sein TARGET2-Konto zuzugreifen;
- „Kreditinstitut“ (*credit institution*): entweder a) ein Kreditinstitut im Sinne von Artikel 4 Absatz 1 Nummer 1 der Verordnung (EU) Nr. 575/2013 des Europäischen Parlaments und des Rates, das von einer zuständigen Behörde beaufsichtigt wird; oder b) ein sonstiges Institut im Sinne von Artikel 123 Absatz 2 des Vertrags über die Arbeitsweise der Europäischen Union (AEUV), das einer Überprüfung unterliegt, die einen der Aufsicht durch eine zuständige Behörde vergleichbaren Standard aufweist;
- „Lastschriftauftrag“ oder „Lastschrift“ (*direct debit instruction*): eine Weisung/Anweisung des Zahlungsempfängers an seine Zentralbank, aufgrund derer die Zentralbank des Zahlers den Lastschriftbetrag dem Konto des Zahlers auf der Grundlage einer Abbuchungsermächtigung belastet;
- „Liquiditätsübertrag“ (*liquidity transfer order*): ein Zahlungsauftrag zur Übertragung von Liquidität zwischen verschiedenen Konten desselben Teilnehmers oder innerhalb einer CAI-Gruppe oder einer AL-Gruppe;
- „Multi-Adressaten-Zugang“ (*multi-addressee access*): die Art des Zugangs zu einem TARGET2-Komponenten-System, über die in der Union oder im EWR ansässige Zweigstellen oder Kreditinstitute Zahlungsaufträge unmittelbar über das TARGET2-Komponenten-System einreichen und/oder Zahlungen empfangen können; Zahlungsaufträge vorgenannter Stellen werden direkt über das PM-Konto des direkten Teilnehmers verrechnet, ohne dass dessen Mitwirkung erforderlich wäre;
- „Nebensystem“ oder „Ancillary System (AS)“: ein der Aufsicht und/oder Überwachung durch eine zuständige Behörde unterliegendes, von einer Stelle mit Sitz in der Europäischen Union oder 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[3] erfüllendes System, in dem Zahlungen und/oder Finanzinstrumente eingereicht und/oder ausgeführt oder erfasst werden, wobei gemäß der Leitlinie EZB/2012/27 der Europäischen Zentralbank[4] und einer bilateralen Vereinbarung

---

3 Die derzeitige Politik des Eurosystems in Bezug auf den Standort von Infrastrukturen ist in den folgenden Erklärungen festgelegt, die auf der Website der EZB unter www.ecb.europa.eu abrufbar sind: a) das ‚Policy statement on euro payment and settlement systems located outside the euro area‘ vom 3. November 1998, b) ‚The Eurosystem's policy line with regard to consolidation in central counterparty clearing‘ vom 27. September 2001, c) ‚The Eurosystem policy principles on the location and operation of infrastructures settling euro-denominated payment transactions‘ vom 19. Juli 2007, d) ‚The Eurosystem policy principles on the location and operation of infrastructures settling euro-denominated payment transactions: specification of ‘legally and operationally located in the euro area’‘ vom 20. November 2008 und e) ‚The Eurosystem oversight policy framework‘ in der geänderten Fassung von Juli 2016.

4 Leitlinie EZB/2012/27 der Europäischen Zentralbank vom 5. Dezember 2012 über ein transeuropäisches

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;

- „Netzwerkdienstleister“ (*network service provider*): das vom EZB-Rat bestimmte Unternehmen, welches IT-gestützte Netzwerkanschlüsse bereitstellt, über die Zahlungsnachrichten in TARGET2 übermittelt werden;
- „nicht abgewickelter Zahlungsauftrag“ (*non-settled payment order*): ein Zahlungsauftrag, der nicht an demselben Geschäftstag abgewickelt wird, an dem er angenommen wurde;
- „Notfalllösung“ (*Contingency Solution*): die SSP-Funktionalität, die sehr kritische und kritische Zahlungen in einem Notfall verarbeitet
- „öffentliche Stelle“ (*public sector body*): eine Stelle des öffentlichen Sektors im Sinne des Artikels 3 der Verordnung (EG) Nr. 3603/93 des Rates vom 13. Dezember 1993 zur Festlegung der Begriffsbestimmungen für die Anwendung der in Artikel 104 und Artikel 104b Absatz 1 des Vertrages vorgesehenen Verbote[5] (jetzt Artikel 123 bzw. Artikel 125 Absatz 1 AEUV);
- „PM-Konto“ (*PM account*): ein Konto eines TARGET2-Teilnehmers innerhalb des PM, das dieser bei einer Zentralbank hat, um:
  a) über TARGET2 Zahlungsaufträge einzureichen oder Zahlungen zu empfangen; und
  b) solche Zahlungen bei der betreffenden Zentralbank zu verrechnen;
- „Rechtsfähigkeitsgutachten“ (*capacity opinion)*: ein Rechtsgutachten zur Prüfung, ob ein bestimmter Teilnehmer die in diesen Bedingungen festgelegten Verpflichtungen wirksam eingehen und erfüllen kann;
- „SEPA Instant Credit Transfer (SCT Inst) Scheme des European Payments Council“ oder „SCT Inst Scheme“ (*European Payments Council's SEPA Instant Credit Transfer (SCT Inst) scheme or SCT Inst scheme*): ein automatisiertes Verfahren mit offenen Standards, das ein Regelwerk für den Interbankenverkehr vorsieht, das von den SCT-Inst-Teilnehmern einzuhalten ist und es den im SEPA tätigen Zahlungsdienstleistern ermöglicht, ein automatisiertes, SEPA-weites Produkt für Euro-Echtzeitüberweisungen anzubieten;
- „Spitzenrefinanzierungsfazilität“ (*marginal lending facility*): eine ständige Fazilität des Eurosystems, die Geschäftspartner in Anspruch nehmen können, um von einer Zentralbank des Eurosystems Übernachtkredit zum festgelegten Spitzenrefinanzierungssatz zu erhalten;
- „Spitzenrefinanzierungssatz“ (*marginal lending rate*): der aktuelle Zinssatz für die Spitzenrefinanzierungsfazilität des Eurosystems;

---

automatisiertes Echtzeit-Brutto-Express-Zahlungsverkehrssystem (TARGET2) (ABl. L 30 vom 30.1.2013, S. 1).

[5] ABl. L 332 vom 31.12.1993, S. 1.

- „Stammdatenformular“ (*static data collection form*): ein Formular der Deutschen Bundesbank, mit dem Kundenstammdaten bei der Anmeldung zu TARGET2-BBk-Diensten und Änderungen bezüglich der Bereitstellung dieser Dienste erhoben werden;
- „Suspendierung“ (*suspension*): die vorübergehende Aufhebung der Rechte und Pflichten eines Teilnehmers während eines von der Deutschen Bundesbank festzulegenden Zeitraums;
- „TARGET Instant Payment Settlement (TIPS)-Dienst“ (*TARGET Instant Payment Settlement (TIPS) service*): Abwicklung von Instant Payment-Aufträgen in Zentralbankgeld über die TIPS-Plattform;
- „TARGET2-BBk“: das TARGET2-Komponenten-System der Deutschen Bundesbank;
- „TARGET2“: die Gesamtheit aller TARGET2-Komponenten-Systeme der Zentralbanken;
- „TARGET2-Komponenten-System“ (*TARGET2 component system*): ein Echtzeit-Brutto-Zahlungsverkehrssystem (RTGS-System) einer Zentralbank, das Bestandteil von TARGET2 ist;
- „TARGET2-CUG“ (*TARGET2 CUG*): eine spezielle Kundengruppe des Netzwerkdienstleisters für den Zugang zum PM, zur Nutzung der betreffenden Dienste und Produkte des Netzwerkdienstleisters;
- „Teilnehmer“ (oder „direkter Teilnehmer“) (*participant or direct participant*): eine Stelle, die mindestens ein PM-Konto (PM-Kontoinhaber) bei einer Zentralbank des Eurosystems hat;
- „technische Störung von TARGET2“ (*technical malfunction of TARGET2*): alle Probleme, Mängel oder Ausfälle der von TARGET2-BBk verwendeten technischen Infrastruktur und/oder IT-Systeme oder alle sonstigen Ereignisse, die eine taggleiche Ausführung von Zahlungen am betreffenden Geschäftstag in TARGET2-BBk unmöglich machen;
- „Teilnehmer“ (oder „direkter Teilnehmer“) (*participant (or 'direct participant')*): eine Stelle, die mindestens ein PM-Konto bei der Deutschen Bundesbank hat;
- „TIPS-Geldkonto“ (*TIPS Dedicated Cash Account (TIPS DCA)*): ein von einem TIPS-Geldkontoinhaber unterhaltenes, in TARGET2-BBk eröffnetes Konto, das für die Abwicklung von Instant Payments für die Kunden verwendet wird;
- „TIPS-Plattform“ (*TIPS Platform*): die einheitliche technische Plattform, die von den Anbieter-NZBen der TIPS-Plattform zur Verfügung gestellt wird;
- „Überweisungsauftrag“ (*credit transfer order*): eine Weisung/Anweisung eines Zahlers, einem Zahlungsempfänger Geld durch Gutschrift auf einem PM-Konto zur Verfügung zu stellen;
- „User Detailed Functional Specifications“ (UDFS): die aktuellste Version der UDFS (der technischen Dokumentation für die Interaktion eines Teilnehmers mit TARGET2);
- „verfügbare Liquidität“ oder „Liquidität“ (*available liquidity or liquidity*): ein Guthaben auf einem PM-Konto eines Teilnehmers und gegebenenfalls eine Innertageskreditlinie, die von der betreffenden NZB des Euro-Währungsgebiets für dieses Konto gewährt wird, aber noch nicht in Anspruch genommen wurde, gegebenenfalls vermindert um den Betrag etwaiger verarbeiteter Liquiditätsreservierungen auf dem PM-Konto;

- „Wertpapierfirma“ (*investment firm*): eine Wertpapierfirma im Sinne von § 2 Abs. 10 WpHG oder vergleichbarer Vorschriften eines EWR-Mitgliedstaates, mit Ausnahme der in § 3 WpHG genannten Einrichtungen, sofern die betreffende Wertpapierfirma,
  a) von einer gemäß der Richtlinie 2014/65/EU anerkannten, zuständigen Behörde zugelassen und beaufsichtigt wird und
  b) berechtigt ist, die in § 2 Abs. 8 Satz 1 Nr. 2, 3, 5 und 6 sowie Satz 6 WpHG oder vergleichbaren Vorschriften eines EWR-Mitgliedstaates genannten Tätigkeiten auszuüben;
- „Zahler“ (*payer*): mit Ausnahme der Verwendung in Artikel 34 dieser Bedingungen ein TARGET2-Teilnehmer, dessen PM-Konto aufgrund der Abwicklung eines Zahlungsauftrags belastet wird;
- „Zahlungsauftrag“ (*payment order*): ein Überweisungsauftrag, ein Liquiditätsübertragungsauftrag oder ein Lastschriftauftrag;
- „Zahlungsempfänger“ (*payee*): mit Ausnahme der Verwendung in Artikel 34 dieser Bedingungen ein TARGET2-Teilnehmer, auf dessen PM-Konto zur Abwicklung eines Zahlungsauftrags eine Gutschrift erfolgt;
- „Zahlungsmodul (*Payments Module* – PM)“: ein Modul der SSP zur Verrechnung von Zahlungen von TARGET2-Teilnehmern über PM-Konten;
- „Zentralbank des Eurosystems“ (*Eurosystem CB*): die EZB oder die NZB eines Mitgliedstaats, der den Euro eingeführt hat;
- „Zentralbanken“ (*central banks*): die Zentralbanken des Eurosystems und die angeschlossenen Zentralbanken;
- „Zertifikatsinhaber” (*certificate holder*): eine namentlich benannte Einzelperson, die von einem TARGET2-Teilnehmer als berechtigt identifiziert und bestimmt wurde, internetbasierten Zugang zum TARGET2-Konto des Teilnehmers zu haben. Der Antrag auf Zertifikate wird von der kontoführenden Zentralbank des Teilnehmers geprüft und den Zertifizierungsstellen übermittelt, die ihrerseits Zertifikate liefern, die den Public Key mit den Referenzen verbinden, die den Teilnehmer identifizieren;
- „Zertifizierungsstellen“ (*certification authorities*): eine oder mehrere NZBen, die vom EZB-Rat dazu bestimmt wurden, bei der Ausstellung, der Verwaltung, dem Widerruf und der Erneuerung elektronischer Zertifikate für das Eurosystem tätig zu werden;
- „Zweigstelle“ (*branch*): eine Zweigniederlassung im Sinne von Artikel 4 Absatz 1 Nummer 17 der Verordnung (EU) Nr. 575/2013 des Europäischen Parlaments und des Rates[6].

Artikel 1a – Anwendungsbereich

[6] Verordnung (EU) Nr. 575/2013 des Europäischen Parlaments und des Rates vom 26. Juni 2013 über Aufsichtsanforderungen an Kreditinstitute und Wertpapierfirmen und zur Änderung der Verordnung (EU) Nr. 648/2012 (ABl. L 176 vom 27.6.2013, S. 1).

Die vorliegenden Bedingungen gelten für das Verhältnis zwischen der Deutschen Bundesbank (im Folgenden: Bank) und ihrem PM-Kontoinhaber bei der Eröffnung und Führung des PM-Kontos im Rahmen des internetbasierten Zugangs.

Artikel 2 – Anlagen

1. Folgende Anlagen sind Bestandteil dieser Bedingungen:

   Anlage I: Technische Spezifikationen für die Verarbeitung von Zahlungsaufträgen im Rahmen des internetbasierten Zugangs

   Anlage II: TARGET2-Ausgleichsregelung

   Anlage III: Muster für Rechtsfähigkeitsgutachten (*capacity opinion*) und Ländergutachten (*country opinion*)

   Anlage IV: Aufrechterhaltung des Geschäftsbetriebs (*Business Continuity*) und Notfallverfahren

   Anlage V: Öffnungszeiten und Tagesablauf

   Anlage VI: Gebührenverzeichnis und Rechnungsstellung im Rahmen des internetbasierten Zugangs

   Anlage VII: Anforderungen an das Informationssicherheitsmanagement und das Business-Continuity-Management

2. Bei Widersprüchen zwischen einer Anlage zu diesen Bedingungen und diesen Bedingungen sind Letztere maßgebend.

Artikel 3 – Allgemeine Beschreibung von TARGET2

1. TARGET2 bietet Echtzeit-Brutto-Abwicklung (RTGS) von Euro-Zahlungen in Zentralbankgeld über PM-Konten an.

2. TARGET2-BBk dient der Abwicklung folgender Transaktionen:

   a) Transaktionen, die unmittelbar aus geldpolitischen Operationen des Eurosystems folgen oder unmittelbar mit diesen in Zusammenhang stehen;

   b) Verrechnung der Euro-Seite von Devisengeschäften des Eurosystems;

   c) Eurozahlungen, die sich aus Geschäften in grenzüberschreitenden Großbetrags-Verrechnungssystemen ergeben;

   d) Eurozahlungen, die sich aus Geschäften in Euro-Massenzahlungsverkehrssystemen mit systemischer Bedeutung ergeben;

   e) alle sonstigen, an TARGET2-Teilnehmer adressierten Transaktionen in Euro.

3. TARGET2 ist ein Echtzeit-Brutto-Zahlungsverkehrssystem in Euro, über das Zahlungen von und auf PM-Konten in Zentralbankgeld abgewickelt werden. TARGET2 wird auf der Grundlage der SSP betrieben, über die — technisch in gleicher Weise — Zahlungsaufträge eingereicht und verarbeitet sowie schließlich Zahlungen empfangen werden.

4. Die Bank ist Erbringer der Dienstleistungen nach Maßgabe dieser Bedingungen. Handlungen und Unterlassungen der SSP-Anbieter-NZBen gelten als Handlungen und Unterlassungen der Bank, die für solche Handlungen und Unterlassungen gemäß Artikel 26 haftet. Die Teilnahme gemäß diesen

Bedingungen begründet keine vertragliche Beziehung zwischen den PM-Kontoinhabern und den SSP-Anbieter-NZBen, wenn einer der Letztgenannten in dieser Eigenschaft handelt. Weisungen/Anweisungen, Nachrichten oder Informationen, die ein PM-Kontoinhaber im Rahmen der gemäß diesen Bedingungen erbrachten Diensten von der SSP erhält oder an diese sendet, gelten als von der Bank erhalten oder an diese gesendet.

5. TARGET2 besteht in rechtlicher Sicht aus einer Vielzahl von Zahlungsverkehrssystemen (TARGET2-Komponenten-Systeme), die gemäß den nationalen Rechtsvorschriften zur Umsetzung der Finalitätsrichtlinie als „Systeme“ angesehen werden. TARGET2-BBk ist ein „System“ im Sinne von § 1 Abs. 16 KWG.

6. Die Teilnahme an TARGET2 erfolgt durch die Teilnahme an einem TARGET2-Komponenten-System. Die gegenseitigen Rechte und Pflichten der PM-Kontoinhaber an TARGET2-BBk einerseits und der Bank andererseits sind in den vorliegenden Bedingungen festgelegt. Die Regeln für die Verarbeitung von Zahlungsaufträgen gemäß diesen Bedingungen (Titel IV und Anlage I) gelten für alle eingereichten Zahlungsaufträge und empfangenen Zahlungen aller PM-Kontoinhaber.

TITEL II

TEILNAHME

Artikel 4 – Zugangsvoraussetzungen

1. Für die internetbasierte direkte Teilnahme an TARGET2-BBk sind zugelassen:

   a) Kreditinstitute, die ihren Sitz in der Union oder im EWR haben, auch wenn sie über eine in der Union oder im EWR ansässige Zweigstelle handeln;

   b) Kreditinstitute mit Sitz außerhalb des EWR, sofern sie über eine in der Union oder im EWR ansässige Zweigstelle handeln;

   unter der Voraussetzung, dass die in den Buchstaben a und b genannten Stellen keinen vom Rat der Europäischen Union oder von Mitgliedstaaten verabschiedeten restriktiven Maßnahmen gemäß Artikel 65 Absatz 1 Buchstabe b, Artikel 75 oder Artikel 215 AEUV unterliegen, deren Umsetzung nach Ansicht der Bank – nachdem sie dies der EZB angezeigt hat – mit dem reibungslosen Funktionieren von TARGET2 unvereinbar ist.

2. Die Bank kann nach ihrem Ermessen darüber hinaus als direkte Teilnehmer zulassen:

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

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

   c) i) Wertpapierfirmen mit Sitz in der Union oder im EWR, auch wenn sie über eine in der Union oder im EWR ansässige Zweigstelle handeln; und

   ii) Wertpapierfirmen mit Sitz außerhalb des EWR, sofern sie über eine in der Union oder im EWR ansässige Zweigstelle handeln; und

d) Kreditinstitute oder Stellen der in den Buchstaben a bis c aufgeführten Art, sofern diese ihren Sitz oder eine ihrer Zweigstellen in einem 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 dem einschlägigen Unionsrecht entsprechen.

3. E-Geld-Institute im Sinne von § 1 Abs. 2 Satz 1 Nr. 1 ZAG sind zur Teilnahme an TARGET2-BBk nicht berechtigt.

Artikel 5 – Direkte Teilnehmer

1. Direkte Teilnehmer an TARGET2-BBk, die den internetbasierten Zugang nutzen, müssen die in Artikel 7 Absätze 1 und 2 festgelegten Anforderungen erfüllen. Sie müssen über mindestens ein PM-Konto bei der Bank verfügen. PM-Kontoinhaber, die durch Zeichnung des SEPA Instant Credit Transfer Adherence Agreements dem SEPA Instant Credit Transfer Scheme beigetreten sind, sind verpflichtet, jederzeit auf der TIPS-Plattform erreichbar zu sein und zu bleiben, sei es als TIPS-Geldkontoinhaber oder als erreichbare Partei über einen TIPS-Geldkontoinhaber.
2. Direkte Teilnehmer , die den internetbasierten Zugang nutzen, können keine indirekten Teilnehmer oder erreichbare BIC-Inhaber benennen; die Nutzung des Multi-Adressaten-Zugangs, des AL-Verfahrens sowie des CAI-Verfahrens ist ebenfalls nicht möglich.

Artikel 6 – Verantwortung des direkten Teilnehmers

1. Direkte Teilnehmer , die den Zugang über den Netzwerkdienstleister nutzen, können indirekte Teilnehmer oder erreichbare BIC-Inhaber benennen sowie den Multi-Adressaten-Zugang nutzen. Es wird klargestellt, dass Zahlungsaufträge oder Zahlungen, die von indirekten Teilnehmern und von Zweigstellen mit Multi-Adressaten-Zugang eingereicht oder empfangen wurden, in diesem Fall als vom direkten Teilnehmer selbst eingereichte Zahlungsaufträge oder empfangene Zahlungen gelten.
2. Der direkte Teilnehmer ist an diese Zahlungsaufträge gebunden, ungeachtet der vertraglichen oder sonstigen Vereinbarungen zwischen ihm und einer der in Absatz 1 genannten Stellen und deren Einhaltung.

Artikel 7 - Antragsverfahren

1. Für die Eröffnung eines PM-Kontos in TARGET2-BBk, auf das über das Internet zugegriffen werden kann, bzw. die Einrichtung eines Internet Zugangs für ein bestehendes PM-Konto, sind die Antragsteller verpflichtet,
   a) die folgenden technischen Anforderungen zu erfüllen:
      i) die für den Anschluss und zur Übermittlung von Zahlungsaufträgen an die SSP notwendige IT-Infrastruktur gemäß den technischen Spezifikationen in Anlage I zu installieren, zu verwalten, zu betreiben und zu überwachen sowie deren Sicherheit zu

gewährleisten. Dabei können die Antragsteller zwar Dritte mit einbeziehen, bleiben aber für deren Tun oder Unterlassen allein verantwortlich, und

ii) die von der Bank vorgeschriebenen Tests bestanden zu haben; und

b) die folgenden rechtlichen Anforderungen zu erfüllen:

i) ein Rechtsfähigkeitsgutachten (*capacity opinion*) im Sinne von Anlage III vorzulegen, sofern die Bank die im Rahmen dieses Rechtsfähigkeitsgutachtens einzureichenden Informationen und Erklärungen nicht bereits in einem anderen Zusammenhang erhalten hat; und

ii) (gilt nur für Institute im Sinne von Artikel 4 Absatz 1 Buchstabe b und Artikel 4 Absatz 2 Buchstabe c Ziffer ii): ein Ländergutachten im Sinne von Anlage III vorzulegen, sofern die Bank die im Rahmen dieses Ländergutachtens einzureichenden Informationen und Erklärungen nicht bereits in einem anderen Zusammenhang erhalten hat und

c) anzugeben, dass sie wünschen, auf ihr PM-Konto über das Internet zuzugreifen, und ein gesondertes PM-Konto in TARGET2 zu beantragen, falls sie darüber hinaus wünschen, über den Netzwerkdienstleister auf TARGET2 zugreifen zu können. Die Antragsteller übermitteln ein ordnungsgemäß ausgefülltes Antragsformular für die Ausstellung der elektronischen Zertifikate, die für den Zugriff auf TARGET2 im Wege des internetbasierten Zugangs erforderlich sind.

2. Der Antrag ist schriftlich an die Bank zu richten und muss mindestens folgende Unterlagen/Informationen enthalten:

a) vollständig ausgefüllte, von der Bank bereitgestellte Stammdatenformulare;

b) das Rechtsfähigkeitsgutachten (*capacity opinion*), sofern von der Bank verlangt, und

c) das Ländergutachten, sofern von der Bank verlangt.

3. Die Bank kann zusätzliche Informationen anfordern, die sie für die Entscheidung über den Antrag auf Teilnahme für notwendig hält.

4. Die Bank lehnt den Antrag auf Teilnahme ab, wenn

a) die Zugangsvoraussetzungen nach Artikel 4 nicht erfüllt sind,

b) eine oder mehrere Teilnahmevoraussetzungen nach Absatz 1 nicht erfüllt sind und/oder

c) nach Einschätzung der Bank eine Teilnahme die Gesamtstabilität, Solidität und Sicherheit von TARGET2-BBk oder eines anderen TARGET2-Komponenten-Systems oder die Erfüllung der in § 3 BBankG und in der Satzung des Europäischen Systems der Zentralbanken und der Europäischen Zentralbank genannten Aufgaben der Deutschen Bundesbank gefährden würde oder unter Risikoerwägungen eine Gefahr darstellt.

5. Die Bank teilt dem Antragsteller ihre Entscheidung über den Antrag auf Teilnahme innerhalb eines Monats nach Eingang des Antrags bei der Bank mit. Verlangt die Bank nach Absatz 3 zusätzliche

Angaben, teilt sie die Entscheidung innerhalb eines Monats nach Eingang dieser Angaben mit. Jeder abschlägige Bescheid enthält eine Begründung für die Ablehnung.

Artikel 8 - TARGET2-Directory

1. Das TARGET2-Directory ist die maßgebliche Datenbank, der die BICs für das Routing von Zahlungsaufträgen entnommen werden können, die an folgende Stellen gerichtet sind:
   a) TARGET2-Teilnehmer und ihre Zweigstellen mit Multi-Adressaten-Zugang,
   b) indirekte TARGET2-Teilnehmer, einschließlich solcher mit Multi-Adressaten-Zugang, und
   c) erreichbare BIC-Inhaber von TARGET2.

   Das TARGET2-Directory wird wöchentlich aktualisiert.
2. Sofern vom Teilnehmer nicht anders gewünscht, wird/werden sein(e) BIC(s) im TARGET2-Directory veröffentlicht.
3. Die Teilnehmer, die den internetbasierten Zugang nutzen, dürfen das TARGET2-Verzeichnis lediglich online einsehen und dürfen es weder intern noch extern weitergeben.
4. Die Stellen im Sinne von Absatz 1 Buchstaben b und c dürfen ihren BIC lediglich in Bezug auf einen direkten Teilnehmer verwenden.
5. Die Teilnehmer willigen ein, dass die Bank und andere Zentralbanken die Namen und BICs der Teilnehmer veröffentlichen dürfen.

TITEL III

PFLICHTEN DER PARTEIEN

Artikel 9 – Pflichten der Bank und der Teilnehmer

1. Die Bank bietet die in Titel IV beschriebenen Dienste im Rahmen eines internetbasierten Zugangs an. Soweit nicht in diesen Bedingungen oder gesetzlich anders vorgeschrieben, unternimmt die Bank alle zumutbaren Anstrengungen, um ihre Verpflichtungen gemäß diesen Bedingungen zu erfüllen, ohne dabei ein bestimmtes Ergebnis zu garantieren.
2. Die Teilnehmer zahlen der Bank die in Anlage VI festgelegten Gebühren.
3. Die Teilnehmer stellen sicher, dass sie an Geschäftstagen während den in Anlage V genannten Öffnungszeiten an TARGET2-BBk angeschlossen sind.
4. Der Teilnehmer sichert der Bank zu, dass die Erfüllung seiner Verpflichtungen gemäß diesen Bedingungen gegen keine für ihn geltenden Gesetze, Bestimmungen oder Verordnungen und Vereinbarungen verstößt, an die er gebunden ist.
5. Die Teilnehmer sind verpflichtet,
   a) während jedes Geschäftstages in regelmäßigen Abständen alle Informationen, die ihnen auf dem ICM zur Verfügung gestellt werden, aktiv zu überprüfen, insbesondere Informationen über wichtige Systemereignisse (z.B. Nachrichten, die den Zahlungsausgleich von Nebensystemen betreffen) und Fälle des vorläufigen oder endgültigen Ausschlusses eines

Teilnehmers. Die Bank haftet nicht für direkte oder indirekte Schäden, die entstehen, weil der Teilnehmer diese Überprüfungen nicht vornimmt, und

b) zu jeder Zeit die Einhaltung der in Anlage I festgelegten Sicherheitsanforderungen – insbesondere im Hinblick auf die sichere Verwahrung der Zertifikate – zu gewährleisten und über Regelungen und Verfahren zu verfügen, die gewährleisten, dass sich die Zertifikatsinhaber ihrer Pflichten zur Sicherung der Zertifikate bewusst sind.

Artikel 10 – Zusammenarbeit und Informationsaustausch

1. Bei der Erfüllung ihrer Verpflichtungen und der Ausübung ihrer Rechte nach diesen Bedingungen arbeiten die Bank und die Teilnehmer eng zusammen, um die Stabilität, Solidität und Sicherheit von TARGET2-BBk zu gewährleisten. Vorbehaltlich ihrer Verpflichtung zur Wahrung des Bankgeheimnisses stellen sie einander alle Informationen oder Unterlagen zur Verfügung, die für die Erfüllung bzw. Ausübung ihrer jeweiligen Verpflichtungen und Rechte nach diesen Bedingungen von Bedeutung sind.
2. Zur Unterstützung von Teilnehmern bei Problemen, die sich im Zusammenhang mit dem Betrieb des Systems ergeben, richtet die Bank eine System-Unterstützungsstelle (*System Support Desk*) ein.
3. Aktuelle Informationen über den Betriebsstatus der SSP stehen über das TARGET2-Informationssystem (T2IS) auf einer gesonderten Internetseite der EZB-Website zur Verfügung. Das T2IS kann genutzt werden, um Informationen über alle Ereignisse zu erhalten, die Auswirkungen auf den Normalbetrieb von TARGET2 haben.
4. Die Bank kann Nachrichten an die Teilnehmer über das Informations- und Kontrollmodul (ICM) oder andere Kommunikationswege übermitteln.
5. Die Teilnehmer sind für die rechtzeitige Aktualisierung vorhandener und Vorlage neuer Kundenstammdaten auf den Stammdatenformularen bei der Bank verantwortlich. Die Teilnehmer überprüfen die Richtigkeit der sie betreffenden Daten, die von der Bank in TARGET2-BBk erfasst wurden.
6. Die Teilnehmer, die den internetbasierten Zugang nutzen, sind für die rechtzeitige Aktualisierung der Formulare für die Ausstellung elektronischer Zertifikate, die für den Zugriff auf TARGET2 im Rahmen des internetbasierten Zugangs erforderlich sind, und für die Übermittlung neuer Formulare für die Ausstellung dieser elektronischen Zertifikate an die Bank verantwortlich. Die Teilnehmer überprüfen die Richtigkeit der sie betreffenden Daten, die von der Bank in TARGET2-BBk erfasst werden.
7. Die Bank ist befugt, Daten über die Teilnehmer, die den internetbasierten Zugang nutzen, an die Zertifizierungsstellen weiterzuleiten, die diese benötigen.
8. Die Teilnehmer informieren die Bank über Veränderungen ihrer rechtlichen Befähigung (*capacity*) und über relevante Rechtsänderungen, die sich auf das sie betreffende Ländergutachten auswirken.
9. Die Teilnehmer informieren die Bank umgehend, wenn ein sie betreffendes Ausfallereignis eintritt oder wenn sie von Krisenpräventions- oder Krisenmanagementmaßnahmen im Sinne der Richtlinie

2014/59/EU des Europäischen Parlaments und des Rates[7] oder jeglicher sonstiger vergleichbarer geltender Rechtsvorschriften betroffen sind.

TITEL IV

PM-KONTOFÜHRUNG UND VERARBEITUNG VON ZAHLUNGSAUFTRÄGEN

Artikel 11 – Eröffnung und Führung von PM-Konten

1. Die Bank eröffnet und führt für jeden Teilnehmer mindestens ein PM-Konto. Auf Antrag eines Teilnehmers, der auch Verrechnungsinstitut ist, eröffnet die Bank ein oder mehrere Unterkonten in TARGET2-BBk, um Liquidität zu dedizieren.

2. PM-Konten und deren Unterkonten werden entweder mit null Prozent oder zum Einlagesatz, je nachdem, welcher dieser Zinssätze niedriger ist, verzinst, sofern diese Konten nicht zur Haltung von Mindestreserven oder von Überschussreserven genutzt werden.

   Im Falle von Mindestreserven werden die Berechnung und Zahlung der anfallenden Zinsen durch die Verordnung (EG) Nr. 2531/98 des Rates[8] und die Verordnung (EU) 2021/378 der Europäischen Zentralbank (EZB/2021/1)[9] geregelt.

   Im Falle von Überschussreserven werden die Berechnung und Zahlung der anfallenden Zinsen durch den Beschluss (EU) 2019/1743 (EZB/2019/31)[10] geregelt.

3. Zusätzlich zur Abwicklung von Zahlungsaufträgen im Zahlungsmodul kann ein PM-Konto zu Abwicklung von Zahlungsaufträgen von und auf HAM-Konten gemäß den von der Bank festgelegten Regelungen genutzt werden.

4. Die Bank stellt auf Wunsch des Teilnehmers täglich einen Kontoauszug bereit.

Artikel 12 – Arten von Zahlungsaufträgen

Im Rahmen von TARGET2 gelten als Zahlungsaufträge:

a) Überweisungsaufträge

b) Lastschriftaufträge, die auf der Basis einer Abbuchungsermächtigung empfangen wurden. Die Teilnehmer, die den internetbasierten Zugang nutzen, können von ihrem PM-Konto keine Lastschriftaufträge senden;

---

[7] Richtlinie 2014/59/EU des Europäischen Parlaments und des Rates vom 15. Mai 2014 zur Festlegung eines Rahmens für die Sanierung und Abwicklung von Kreditinstituten und Wertpapierfirmen und zur Änderung der Richtlinie 82/891/EWG des Rates, der Richtlinien 2001/24/EG, 2002/47/EG, 2004/25/EG, 2005/56/EG, 2007/36/EG, 2011/35/EU, 2012/30/EU und 2013/36/EU sowie der Verordnungen (EU) Nr. 1093/2010 und (EU) Nr. 648/2012 des Europäischen Parlaments und des Rates (ABl. L 173 vom 12.6.2014, S. 190).

[8] Verordnung (EG) Nr. 2531/98 des Rates vom 23. November 1998 über die Auferlegung einer Mindestreservepflicht durch die Europäische Zentralbank (ABl. L 318 vom 27.11.1998, S. 1).

[9] Verordnung (EU) 2021/378 der Europäischen Zentralbank vom 22. Januar 2021 über die Auferlegung einer Mindestreservepflicht (EZB/2021/1) (ABl. L 73 vom 3.3.2021, S. 1).

[10] Beschluss (EU) 2019/1743 der Europäischen Zentralbank vom 15. Oktober 2019 über die Verzinsung von Überschussreserven und bestimmten Einlagen (EZB/2019/31) (ABl. L 267 vom 21.10.2019, S. 12).

c) Liquiditätsübertragungsaufträge.

Artikel 13 – Annahme und Zurückweisung von Zahlungsaufträgen

1. Vom Teilnehmer eingereichte Zahlungsaufträge gelten als von der Bank angenommen, wenn
   a) die Zahlungsnachricht den Formatierungsregeln und -bedingungen von TARGET2-BBk entspricht und die in Anlage I beschriebene Doppeleinreichungskontrolle erfolgreich durchlaufen hat und
   b) im Fall der Suspendierung des Zahlers oder Zahlungsempfängers die Zentralbank des suspendierten Teilnehmers der Zahlung ausdrücklich zugestimmt hat.
2. Die Bank weist umgehend einen Zahlungsauftrag zurück, der die in Absatz 1 aufgeführten Bedingungen nicht erfüllt. Die Bank informiert den Teilnehmer über eine Zurückweisung eines Zahlungsauftrags gemäß Anlage I.
3. Die SSP bringt den Zeitstempel für die Verarbeitung von Zahlungsaufträgen in der Reihenfolge ihres Eingangs an.

Artikel 14 – Prioritätsregeln

1. Die einreichenden Teilnehmer kennzeichnen den jeweiligen Zahlungsauftrag als
   a) normalen Zahlungsauftrag (Prioritätsstufe 2),
   b) dringenden („urgent“) Zahlungsauftrag (Prioritätsstufe 1) oder
   c) sehr dringenden („highly urgent“) Zahlungsauftrag (Prioritätsstufe 0).

   Wenn bei einem Zahlungsauftrag keine Priorität angegeben ist, wird dieser als normaler Zahlungsauftrag behandelt.
2. Sehr dringende Zahlungsaufträge dürfen nur eingereicht werden von
   a) Zentralbanken und
   b) Teilnehmern, sofern es sich um Zahlungen an die bzw. von der CLS Bank International – mit Ausnahme von Zahlungen in Verbindung mit dem CCP-Dienst der CLS und dem CLSNow-Dienst – oder um Liquiditätsüberträge im Zusammenhang mit dem Zahlungsausgleich von Nebensystemen mittels der Nebensystemschnittstelle (ASI) handelt.

   Alle Zahlungsaufträge, die von einem Nebensystem über die ASI zur Belastung von oder Gutschrift auf PM-Konten der Teilnehmer eingereicht werden gelten als sehr dringende Zahlungsaufträge.
3. Über das ICM beauftragte Liquiditätsüberträge sind dringende Zahlungsaufträge.
4. Bei dringenden und normalen Zahlungsaufträgen kann der Zahler die Priorität über das ICM mit sofortiger Wirkung ändern. Die Priorität eines sehr dringenden Zahlungsauftrags kann nicht geändert werden.

Artikel 15 – Liquiditätslimite

1. Ein Teilnehmer kann gegenüber anderen TARGET2-Teilnehmern, mit Ausnahme der Zentralbanken, die Nutzung seiner verfügbaren Liquidität für Zahlungsaufträge durch bilaterale oder multilaterale Limite begrenzen. Solche Limite können lediglich für normale Zahlungsaufträge festgelegt werden.
2. Die Teilnehmer dürfen die AL-Gruppen-Funktionalität nicht für ein PM-Konto mit internetbasiertem Zugang nutzen oder dieses PM-Konto mit einem anderen von ihnen geführten TARGET2-Konto verbinden.

   Limite können nur gegenüber einer gesamten AL-Gruppe festgesetzt werden. Limite können nicht gegenüber einem einzelnen PM-Konto eines AL-Gruppenmitglieds festgelegt werden.
3. Durch Setzen eines bilateralen Limits weist ein Teilnehmer die Bank an, einen angenommenen Zahlungsauftrag nicht abzuwickeln, wenn der Gesamtbetrag seiner ausgehenden normalen Zahlungsaufträge an das betreffende PM-Konto eines anderen TARGET2-Teilnehmers abzüglich des Gesamtbetrags aller eingehenden dringenden und normalen Zahlungen von diesem PM-Konto das bilaterale Limit übersteigen würde.
4. Ein Teilnehmer kann ein multilaterales Limit nur gegenüber jenen PM-Konten festlegen, für die kein bilaterales Limit festgelegt wurde. Ein multilaterales Limit kann nur festgelegt werden, wenn der Teilnehmer mindestens ein bilaterales Limit gesetzt hat. Indem ein Teilnehmer ein multilaterales Limit setzt, weist er die Bank an, einen angenommenen Zahlungsauftrag nicht abzuwickeln, wenn der Gesamtbetrag seiner ausgehenden normalen Zahlungsaufträge an alle PM-Konten von TARGET2-Teilnehmern, für die kein bilaterales Limit festgelegt wurde, abzüglich des Gesamtbetrags aller eingehenden dringenden und normalen Zahlungen von diesen PM-Konten das multilaterale Limit übersteigen würde.
5. Der Mindestbetrag für jedes dieser Limite liegt bei 1 Mio €. Ein bilaterales bzw. multilaterales Liquiditätslimit mit einem Betrag in Höhe von null wird so behandelt, als ob kein Limit festgelegt worden wäre. Limite zwischen null und 1 Mio € sind nicht möglich.
6. Die Liquiditätslimite können jederzeit mit sofortiger Wirkung oder mit Wirkung für den nächsten Geschäftstag über das ICM geändert werden. Wenn ein Limit auf null geändert wird, kann es am gleichen Geschäftstag nicht erneut geändert werden. Ein erstmalig gesetztes bilaterales oder multilaterales Limit wird erst am nächsten Geschäftstag wirksam.

Artikel 16 – Liquiditätsreservierungen

1. Die Teilnehmer können über das ICM Liquidität für sehr dringende oder dringende Zahlungsaufträge reservieren.
2. Durch die Reservierung eines bestimmten Liquiditätsbetrags für sehr dringende Zahlungsaufträge weist ein Teilnehmer die Bank an, dringende und normale Zahlungsaufträge nur abzuwickeln, wenn nach Abzug des für sehr dringende Zahlungen reservierten Betrags noch ausreichend Liquidität zur Verfügung steht.
3. Durch die Reservierung eines bestimmten Liquiditätsbetrags für dringende Zahlungsaufträge weist der Teilnehmer die Bank an, normale Zahlungsaufträge nur abzuwickeln, wenn nach Abzug des für

dringende und sehr dringende Zahlungen reservierten Betrags noch ausreichend Liquidität zur Verfügung steht.

4. Nach Eingang des Reservierungsauftrags überprüft die Bank, ob auf dem PM-Konto des Teilnehmers ausreichend Liquidität für die Reservierung vorhanden ist. Wenn dies nicht der Fall ist, wird nur die auf dem PM-Konto vorhandene Liquidität reserviert. Der Rest der beantragten Liquidität wird reserviert, wenn zusätzliche Liquidität zur Verfügung steht.

5. Die Höhe der zu reservierenden Liquidität kann geändert werden. Die Teilnehmer können mit sofortiger Wirkung oder mit Wirkung für den nächsten Geschäftstag über das ICM die Reservierung eines neuen Betrags beauftragen.

Artikel 16a - Daueraufträge für Liquiditätsreservierung und Liquiditätszuordnung

1. Die Teilnehmer können über das ICM den reservierten Liquiditätsbetrag für sehr dringende oder dringende Zahlungsaufträge im Voraus festlegen. Dieser Dauerauftrag oder eine Änderung dieses Dauerauftrags wird ab dem nächsten Geschäftstag wirksam.

2. Die Teilnehmer können über das ICM den für den Zahlungsausgleich von Nebensystemen reservierten Liquiditätsbetrag im Voraus festlegen. Dieser Dauerauftrag oder eine Änderung dieses Dauerauftrags wird ab dem nächsten Geschäftstag wirksam. Die Bank gilt als von den Teilnehmern beauftragt, Liquidität zu dedizieren (d.h. auf das Unterkonto des jeweiligen Teilnehmers zu übertragen), wenn das betreffende Nebensystem dies beantragt.

Artikel 17 – Zeitvorgaben für die Abwicklung

1. Einreichende Teilnehmer können die innertäglichen Ausführungszeiten für Zahlungsaufträge mit Hilfe des Earliest Debit Time Indicator (Indikator für den frühesten Belastungszeitpunkt) oder des Latest Debit Time Indicator (Indikator für den spätesten Belastungszeitpunkt) vorgeben.

2. Bei Verwendung des Earliest Debit Time Indicator wird der angenommene Zahlungsauftrag gespeichert und erst zum angegebenen Zeitpunkt in die Eingangsdisposition gestellt.

3. Bei Verwendung des Latest Debit Time Indicator wird der angenommene Zahlungsauftrag als nicht ausgeführt zurückgegeben, wenn er nicht bis zum angegebenen Belastungszeitpunkt abgewickelt werden konnte. 15 Minuten vor dem festgelegten Belastungszeitpunkt wird der einreichende Teilnehmer über das ICM informiert, erhält aber keine automatisierte Benachrichtigung. Der einreichende Teilnehmer kann den Latest Debit Time Indicator auch lediglich als Warnindikator nutzen. In solchen Fällen wird der betreffende Zahlungsauftrag nicht zurückgegeben.

4. Einreichende Teilnehmer können den Earliest Debit Time Indicator und den Latest Debit Time Indicator über das ICM ändern.

5. Weitere technische Einzelheiten sind in Anlage I dargelegt.

Artikel 18 – Im Voraus eingereichte Zahlungsaufträge

1. Zahlungsaufträge können bis zu fünf Geschäftstage vor dem festgelegten Abwicklungstag eingereicht werden (gespeicherte (*warehoused*) Zahlungsaufträge).

2. Gespeicherte Zahlungsaufträge werden an dem vom einreichenden Teilnehmer bestimmten Geschäftstag zu Beginn der Tagesbetrieb-Phase gemäß Anlage V angenommen und in die Eingangsdisposition eingestellt. Sie haben Vorrang vor Zahlungsaufträgen derselben Priorität.

3. Für gespeicherte Zahlungsaufträge gelten die Artikel 14 Absatz 3, Artikel 21 Absatz 2 und Artikel 24 Absatz 1 Buchstabe a entsprechend.

Artikel 19 – Abwicklung von Zahlungsaufträgen in der Eingangsdisposition

1. Sofern einreichende Teilnehmer keinen Ausführungszeitpunkt nach Artikel 17 angegeben haben, werden angenommene Zahlungsaufträge umgehend, spätestens jedoch bis zum Ablauf des Geschäftstages, an dem sie angenommen wurden, ausgeführt. Dies gilt unter der Voraussetzung, dass der Zahler über ein ausreichendes Guthaben auf seinem PM-Konto verfügt und erfolgt unter Berücksichtigung etwaiger Liquiditätslimite sowie Liquiditätsreservierungen im Sinne der Artikel 15 und 16.

2. Die Deckung erfolgt durch

   a) die verfügbare Liquidität auf dem PM-Konto; oder

   b) eingehende Zahlungen von anderen TARGET2-Teilnehmern gemäß den anwendbaren Optimierungsverfahren.

3. Für sehr dringende Zahlungsaufträge gilt das FIFO (*First In, First Out*)-Prinzip. Dieses Prinzip bedeutet, dass sehr dringende Zahlungsaufträge in chronologischer Reihenfolge abgewickelt werden. Solange sich sehr dringende Zahlungsaufträge in der Warteschlange befinden, werden keine dringenden und normalen Zahlungsaufträge ausgeführt.

4. Das FIFO-Prinzip ist auch bei dringenden Zahlungsaufträgen anwendbar. Solange sich dringende und sehr dringende Zahlungsaufträge in der Warteschlange befinden, werden keine normalen Zahlungsaufträge ausgeführt.

5. Abweichend von den Absätzen 3 und 4 können Zahlungsaufträge mit geringerer Priorität (einschließlich solcher derselben Priorität, die jedoch später angenommen wurden) *vor* Zahlungsaufträgen mit höherer Priorität (einschließlich solcher derselben Priorität, die jedoch früher angenommen wurden) abgewickelt werden, sofern sich die Zahlungsaufträge mit geringerer Priorität mit eingehenden Zahlungen ausgleichen und dies per saldo zu einem Liquiditätszufluss für den Zahler führt.

6. Normale Zahlungsaufträge werden nach dem „FIFO-Überhol-Prinzip“ *(FIFO bypass)* abgewickelt. Das bedeutet, dass diese Zahlungsaufträge außerhalb des FIFO-Prinzips umgehend (unabhängig davon, ob sich in der Warteschlange zu einem früheren Zeitpunkt angenommene normale Zahlungen befinden) ausgeführt werden können, sofern ausreichend Liquidität vorhanden ist.

7. Weitere Einzelheiten zur Abwicklung von Zahlungsaufträgen in der Eingangsdisposition sind in Anlage I dargelegt.

Artikel 20 – Abwicklung und Rückgabe von Zahlungsaufträgen in der Warteschlange

1. Zahlungsaufträge, die nicht umgehend in der Eingangsdisposition abgewickelt werden können, werden gemäß Artikel 14 mit der vom betreffenden Teilnehmer angegebenen Priorität in die Warteschlangen eingestellt.
2. Die Bank kann zur besseren Abwicklung von Zahlungsaufträgen in der Warteschlange die in Anlage I aufgeführten Optimierungsverfahren anwenden.
3. Außer bei sehr dringenden Zahlungsaufträgen kann der Zahler die Position von Zahlungsaufträgen in der Warteschlange über das ICM verändern (d. h. eine neue Reihenfolge festlegen). Zahlungsaufträge können während der Tagverarbeitung (siehe Anlage V) jederzeit mit sofortiger Wirkung entweder an den Anfang oder das Ende der jeweiligen Warteschlange verschoben werden.
4. Auf Antrag eines Zahlers kann die Bank entscheiden, die Position eines sehr dringenden Zahlungsauftrags in der Warteschlange (außer sehr dringenden Zahlungsaufträgen im Rahmen der Abwicklungsverfahren 5 und 6) zu ändern, wenn diese Änderung weder den reibungslosen Zahlungsausgleich durch Nebensysteme in TARGET2 beeinträchtigen noch anderweitig zu Systemrisiken führen würde.
5. Über das ICM beauftragte Liquiditätsüberträge werden bei unzureichender Liquidität umgehend als nicht ausgeführt zurückgegeben. Sonstige Zahlungsaufträge werden als nicht ausgeführt zurückgegeben, wenn sie bis zum Annahmeschluss für den entsprechenden Nachrichtentyp (siehe Anlage V) nicht ausgeführt werden konnten.

Artikel 21 – Einbringung von Zahlungsaufträgen in das System und ihre Unwiderruflichkeit

1. Im Sinne von Artikel 3 Absatz 1 Satz 1 der Finalitätsrichtlinie und der deutschen Regelungen zur Umsetzung dieses Artikels der Finalitätsrichtlinie gelten Zahlungsaufträge in TARGET2-BBk zu dem Zeitpunkt als eingebracht, zu dem das PM-Konto des betreffenden Teilnehmers belastet wird.
2. Zahlungsaufträge können bis zu dem in Absatz 1 genannten Zeitpunkt widerrufen werden. Zahlungsaufträge, die von einem Algorithmus im Sinne von Anlage I erfasst sind, können während des Laufs des Algorithmus nicht widerrufen werden.

TITEL V

SICHERHEITSANFORDERUNGEN UND NOTFALLVERFAHREN

Artikel 22 – Aufrechterhaltung des Geschäftsbetriebs („*Business Continuity*“) und Notfallverfahren

1) Im Falle eines außergewöhnlichen externen Ereignisses oder eines anderen Ereignisses, das den Betrieb der SSP beeinträchtigt, finden die in Anlage IV beschriebenen Business-Continuity- und Notfallverfahren Anwendung.

(2) Das Eurosystem sieht eine Notfalllösung für den Fall vor, dass die in Absatz 1 genannten Ereignisse eintreten. Die Anbindung an die Notfalllösung und die Nutzung der Notfalllösung sind

obligatorisch für Teilnehmer, die die Bank als kritisch einstuft. Andere Teilnehmer, die nicht den internetbasierten Zugang nutzen, können sich auf Antrag an die Notfalllösung anbinden.

Artikel 23 – Sicherheitsanforderungen und Kontrollverfahren

1. Die Teilnehmer, die den internetbasierten Zugang nutzen, führen zum Schutz ihrer Systeme vor unberechtigtem Zugriff und unbefugter Nutzung angemessene Sicherheitskontrollen, insbesondere die in Anlage I genannten, durch. Der angemessene Schutz der Vertraulichkeit, Integrität und Verfügbarkeit ihrer Systeme obliegt der ausschließlichen Verantwortung der Teilnehmer.
2. Die Teilnehmer informieren die Bank über alle sicherheitsrelevanten Vorfälle in ihrer technischen Infrastruktur und, sofern dies angemessen erscheint, über sicherheitsrelevante Vorfälle in der technischen Infrastruktur von Drittanbietern. Die Bank kann weitere Informationen über den Vorfall anfordern und erforderlichenfalls verlangen, dass der Teilnehmer angemessene Maßnahmen ergreift, um solche Ereignisse zukünftig zu vermeiden.
3. Die Bank kann für alle Teilnehmer und/oder Teilnehmer, die von der Bank als systemkritisch angesehen werden, zusätzliche Sicherheitsanforderungen verlangen, insbesondere im Hinblick auf Cybersicherheit oder Betrugsbekämpfung.
4. Teilnehmer, die den internetbasierten Zugang nutzen, übermitteln der Bank jährlich die auf der Website der Bank und der Website der EZB in englischer Sprache veröffentlichte TARGET2-Selbstzertifizierungserklärung.

(4a) Die Bank beurteilt anhand der Selbstzertifizierungserklärung(en) des Teilnehmers den Grad der Einhaltung jeder der in den TARGET2-Selbstzertifizierungsanforderungen festgelegten Anforderungen durch den Teilnehmer. Diese Anforderungen sind in Anlage VII aufgeführt, die neben den in Artikel 2 Absatz 1 genannten Anlagen Bestandteil dieser Bedingungen sind.

(4b) Der Grad der Einhaltung der Anforderungen der TARGET2-Selbstzertifizierung durch den Teilnehmer wird, geordnet nach zunehmendem Schweregrad der Nichteinhaltung, wie folgt eingestuft: ‚vollständige Einhaltung', ‚geringfügige Nichteinhaltung', ‚gravierende Nichteinhaltung'. Die folgenden Kriterien finden Anwendung: Vollständige Einhaltung ist erreicht, wenn ein Teilnehmer 100 % der Anforderungen erfüllt; eine geringfügige Nichteinhaltung liegt vor, wenn ein Teilnehmer weniger als 100 %, aber mindestens 66 % der Anforderungen erfüllt, und eine gravierende Nichteinhaltung liegt vor, wenn ein Teilnehmer weniger als 66 % der Anforderungen erfüllt. Weist ein Teilnehmer nach, dass eine bestimmte Anforderung auf ihn nicht anwendbar ist, so wird für die Zwecke der Einstufung davon ausgegangen, dass er die Anforderungen erfüllt. Ein Teilnehmer, der die ‚vollständige Einhaltung' nicht erreicht, legt einen Maßnahmenplan vor, aus dem hervorgeht, wie er die vollständige Einhaltung zu erreichen beabsichtigt. Die Bank unterrichtet die betreffenden Aufsichtsbehörden über den Stand der Einhaltung durch den jeweiligen Teilnehmer.

(4c) Übermittelt der Teilnehmer die TARGET2-Selbstzertifizierung nicht, so wird der Grad der Einhaltung der Anforderungen durch den Teilnehmer als ‚gravierende Nichteinhaltung' eingestuft.

(4d) Die Bank beurteilt jährlich erneut die Einhaltung der Anforderungen durch die Teilnehmer.

(4e) Die Bank kann Teilnehmern, deren Grad der Einhaltung der Anforderungen als geringfügige oder gravierende Nichteinhaltung eingestuft wurde, mit zunehmendem Schweregrad folgende Abhilfemaßnahmen auferlegen:

i) verstärkte Überwachung: Der Teilnehmer legt der Bank monatlich einen von einem leitenden Angestellten unterzeichneten Bericht über seine Fortschritte bei der Behebung der Nichteinhaltung vor. Darüber hinaus zahlt der Teilnehmer für jedes betroffene Konto ein monatliches Strafentgelt in Höhe seiner monatlichen Gebühr gemäß Anlage VI Nummer 1 ohne Transaktionsgebühren. Diese Abhilfemaßnahme kann auferlegt werden, wenn bei der Beurteilung der Einhaltung der Anforderungen durch den Teilnehmer zweimal in Folge eine geringfügige Nichteinhaltung oder eine gravierende Nichteinhaltung festgestellt wird;

ii) Suspendierung: Die Teilnahme an TARGET2-BBk kann bei Vorliegen der in Artikel 34 Absatz 2 Buchstaben b und c dieses Anhangs beschriebenen Umstände suspendiert werden. Abweichend von Artikel 29(2)(b) und (c) dieser Bedingungen erfolgt die Suspendierung der Teilnahme mit einer Ankündigungsfrist von drei Monaten. Der Teilnehmer zahlt für jedes suspendierte Konto ein monatliches Strafentgelt in Höhe seiner doppelten monatlichen Gebühr gemäß Anlage VI Nummer 1 ohne Transaktionsgebühren. Diese Abhilfemaßnahme kann auferlegt werden, wenn bei der Beurteilung der Einhaltung der Anforderungen durch den Teilnehmer zweimal in Folge eine gravierende Nichteinhaltung festgestellt wird;

iii) Beendigung: Die Teilnahme an TARGET2-BBk kann bei Vorliegen der in Artikel 29 (2)(b) und (c) dieser Bedingungen beschriebenen Umstände beendet werden. Abweichend von Artikel 29 dieser Bedingungen erfolgt die Beendigung der Teilnahme mit einer Ankündigungsfrist von drei Monaten. Der Teilnehmer zahlt für jedes im Rahmen der Beendigung der Teilnahme geschlossene Konto ein zusätzliches Strafentgelt in Höhe von 1 000 EUR. Diese Abhilfemaßnahme kann auferlegt werden, wenn der Teilnehmer die gravierende Nichteinhaltung nicht innerhalb von drei Monaten nach der Suspendierung zur Zufriedenheit der Bank behoben hat.

5. Die Teilnehmer, die den internetbasierten Zugang nutzen, informieren die Bank unverzüglich über jedes Ereignis, das die Gültigkeit der Zertifikate beeinträchtigen kann, insbesondere über die in Anlage I genannten Ereignisse wie zum Beispiel den Verlust oder die missbräuchliche Verwendung der Zertifikate.

TITEL VI

DAS INFORMATIONS- UND KONTROLLMODUL (ICM)

Artikel 24 – Nutzung des ICM

1. Das ICM ermöglicht den Teilnehmern,

   a) Zahlungen einzugeben,

   b) Informationen über ihre Konten abzurufen und ihre Liquidität zu steuern,

c) Liquiditätsüberträge zu beauftragen und

d) auf System-Nachrichten zuzugreifen.

2. Weitere technische Einzelheiten in Bezug auf die Nutzung des ICM in Verbindung mit dem internetbasierten Zugang sind in Anlage I enthalten.

TITEL VII

AUSGLEICH, HAFTUNGSREGELUNG UND NACHWEISE

Artikel 25 - Ausgleichsregelung

Wenn ein Zahlungsauftrag aufgrund einer technischen Störung von TARGET2 nicht am Geschäftstag seiner Annahme abgewickelt werden kann, bietet die Bank den betreffenden direkten Teilnehmern Ausgleichszahlungen gemäß dem in Anlage II dargelegten besonderen Verfahren an.

Artikel 26 – Haftungsregelung

1. Bei der Erfüllung ihrer Verpflichtungen gemäß diesen Bedingungen lassen die Bank und die Teilnehmer gegenseitig die verkehrsübliche Sorgfalt walten.

2. Die Bank haftet bei Vorsatz oder grober Fahrlässigkeit gegenüber den Teilnehmern für Schäden aus dem Betrieb von TARGET2-BBk. Bei einfacher/leichter Fahrlässigkeit ist die Haftung der Bank auf unmittelbare Schäden des Teilnehmers, d. h. auf den Betrag des betreffenden Zahlungsauftrags und/oder den hierauf entfallenen Zinsschaden, ausgenommen etwaige Folgeschäden, begrenzt.

3. Die Bank haftet nicht für etwaige Verluste durch Störungen oder Ausfälle der technischen Infrastruktur (insbesondere ihrer EDV-Systeme, Programme, Daten, Anwendungen oder Netzwerke), sofern diese Störungen oder Ausfälle eintreten, obwohl die Bank notwendige und zumutbare Maßnahmen zum Schutz dieser Infrastruktur gegen Störungen oder Ausfälle und zur Behebung der Folgen dieser Störungen oder Ausfälle (insbesondere durch Einleitung und Durchführung der in Anlage IV beschriebenen Business-Continuity- und Notfallverfahren) getroffen hat.

4. Die Bank übernimmt keine Haftung

   a) soweit der Schaden von einem Teilnehmer verursacht wurde oder

   b) wenn der Schaden durch äußere Ereignisse verursacht wurde, die außerhalb der Einflussnahmemöglichkeit der Bank liegen (höhere Gewalt).

5. Als zwischengeschaltete Stelle haftet die Bank im Rahmen der gesetzlichen Regressansprüche des § 676a BGB nur soweit der Zahlungsdienstleister gegenüber dem Zahlungsdienstnutzer seine Haftung nach den gesetzlichen Bestimmungen nicht hätte ausschließen oder begrenzen können.

6. Die Bank und die Teilnehmer unternehmen alle zumutbaren Maßnahmen zur Minderung etwaiger Schäden oder Verluste im Sinne dieses Artikels.

7. Bei der Erfüllung ihrer Verpflichtungen gemäß diesen Bedingungen kann die Bank im eigenen Namen Dritte, insbesondere Telekommunikations- oder sonstige Netzwerkanbieter oder andere Stellen beauftragen, sofern dies für die Einhaltung der Verpflichtungen der Bank erforderlich oder marktüblich ist. Die Verpflichtung der Bank einschließlich ihrer Haftung beschränkt sich auf die sorgfältige Auswahl und Beauftragung dieser Dritten. Die Anbieter-Zentralbanken gelten nicht als Dritte im Sinne dieses Absatzes.

Artikel 27 – Nachweise

1. Sofern in diesen Bedingungen nicht anders vorgesehen, werden dem Teilnehmer, der den internetbasierten Zugang nutzt, alle zahlungs- und abwicklungsbezogenen Nachrichten in Bezug auf TARGET2 (z. B. Belastungs- und Gutschriftbestätigungen oder Kontoauszüge) zwischen der Bank und den Teilnehmern auf dem ICM zur Verfügung gestellt.
2. Von der Bank oder vom Netzwerkdienstleister aufbewahrte, elektronisch gespeicherte oder schriftliche Aufzeichnungen von Nachrichten können zum Nachweis von Zahlungen verwendet werden, die von der Bank verarbeitet wurden. Die gespeicherte oder gedruckte Fassung der Originalnachricht des Netzwerkdienstleisters kann – ungeachtet des Formats der Originalnachricht – als Nachweis verwendet werden.
3. Wenn die Verbindung eines Teilnehmers ausfällt, ist der Teilnehmer verpflichtet, die in Anlage I beschriebenen alternativen Übertragungswege für Nachrichten zu nutzen. In diesen Fällen wird die gespeicherte oder gedruckte Fassung der von der Bank erstellten Nachricht als Nachweis akzeptiert.
4. Die Bank bewahrt Aufzeichnungen über eingereichte Zahlungsaufträge und empfangene Zahlungen von Teilnehmern über einen Zeitraum von zehn Jahren ab dem Zeitpunkt der Einreichung der Zahlungsaufträge bzw. des Empfangs der Zahlungen auf.
5. Eigene Kontounterlagen und Aufzeichnungen der Bank (auf Papier, als Mikrofilm, Mikrofiche, elektronische oder magnetische Aufzeichnung, in anderer mechanisch reproduzierbarer oder sonstiger Form) können ebenfalls als Nachweis etwaiger Verpflichtungen von Teilnehmern sowie über Sachverhalte und Ereignisse, auf die sich die Parteien berufen, verwendet werden.

TITEL VIII

BEENDIGUNG DER TEILNAHME UND KONTOSCHLIESSUNG

Artikel 28 – Dauer und ordentliche Kündigung der Teilnahme

1. Unbeschadet des Artikels 29 erfolgt die Teilnahme an TARGET2-BBk auf unbestimmte Zeit.
2. Ein Teilnehmer kann seine Teilnahme an TARGET2-BBk jederzeit unter Einhaltung einer Frist von 14 Geschäftstagen kündigen, sofern er mit der Bank keine kürzere Kündigungsfrist vereinbart.
3. Die Bank kann die Teilnahme eines Teilnehmers an TARGET2-BBk jederzeit unter Einhaltung einer Frist von drei Monaten kündigen, sofern sie mit diesem Teilnehmer keine andere Kündigungsfrist vereinbart.

4. Auch nach Beendigung der Teilnahme gelten die in Artikel 33 dargelegten Geheimhaltungspflichten für einen Zeitraum von fünf Jahren ab dem Zeitpunkt der Beendigung weiter.

5. Bei Beendigung der Teilnahme werden die PM-Konten des betreffenden Teilnehmers gemäß Artikel 30 geschlossen.

Artikel 29 – Suspendierung und außerordentliche Beendigung der Teilnahme

1. Die Teilnahme eines Teilnehmers an TARGET2-BBk endet fristlos und mit sofortiger Wirkung, oder ist in gleicher Weise suspendiert wenn eines der folgenden Ausfallereignisse eintritt:

   a) die Eröffnung eines Insolvenzverfahrens und/oder

   b) der Teilnehmer erfüllt die in Artikel 4 festgelegten Zugangsvoraussetzungen nicht mehr.

   Für die Zwecke dieses Absatzes gelten gegen einen PM-Kontoinhaber gerichtete Krisenpräventionsmaßnahmen oder Krisenmanagementmaßnahmen im Sinne der Richtlinie 2014/59/EU des Europäischen Parlaments und des Rates[11] nicht automatisch als Eröffnung eines Insolvenzverfahrens.2. Die Bank kann einem Teilnehmer fristlos kündigen oder ihn fristlos suspendieren, wenn

   a) ein oder mehrere Ausfallereignisse (außer den in Absatz 1 genannten) eintreten,

   b) der Teilnehmer erheblich gegen diese Bedingungen verstößt,

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

   d) der Teilnehmer aus einer TARGET2-CUG ausgeschlossen wird oder dieser aus anderen Gründen nicht mehr angehört,

   e) ein anderes Ereignis in Bezug auf den Teilnehmer eintritt, das nach Einschätzung der Bank ein besonderes Risiko für die Gesamtstabilität, Solidität und Sicherheit von TARGET2-BBk oder eines anderen TARGET2-Komponenten-Systems begründet, oder die Erfüllung der in § 3 BBankG und in der Satzung des Europäischen Systems der Zentralbanken und der Europäischen Zentralbank beschriebenen Aufgaben durch die Bank gefährden würde oder unter Risikoerwägungen eine Gefahr darstellt, und/oder

   f) eine NZB einen Teilnehmer vom Zugang zum Innertageskredit vorläufig oder endgültig ausschließt.

3. In der Ausübung ihres Ermessens im Rahmen von Absatz 2 berücksichtigt die Bank unter anderem die Schwere der in den Buchstaben a bis c genannten Ausfallereignisse bzw. Ereignisse.

4. a) Wenn die Bank die Teilnahme eines PM-Kontoinhabers an TARGET2-BBk gemäß Absatz 1 oder 2 beendet, kündigt oder suspendiert, setzt sie diesen PM-Kontoinhaber, andere Zentralbanken und andere PM-Kontoinhaber in allen TARGET2-Komponenten-Systemen

[11] Richtlinie 2014/59/EU des Europäischen Parlaments und des Rates vom 15. Mai 2014 zur Festlegung eines Rahmens für die Sanierung und Abwicklung von Kreditinstituten und Wertpapierfirmen und zur Änderung der Richtlinie 82/891/EWG des Rates und der Richtlinien 2001/24/EG, 2002/47/EG, 2004/25/EG, 2005/56/EG, 2007/36/EG, 2011/35/EU, 2012/30/EU und 2013/36/EU sowie der Verordnungen (EU) Nr. 1093/2010 und (EU) Nr. 648/2012 des Europäischen Parlaments und des Rates (ABl. L 173 vom 12.6.2014, S. 190).

hierüber unverzüglich mittels einer ICM-Nachricht in Kenntnis. Diese Nachricht gilt als von der kontoführenden NZB des die Nachricht empfangenden PM-Kontoinhabers erteilt.

b) Sobald eine solche ICM-Nachricht den Teilnehmern, die den internetbasierten Zugang nutzen, zur Verfügung gestellt wurde, gelten diese Teilnehmer als über die Beendigung/Kündigung oder Suspendierung der Teilnahme eines Teilnehmers an TARGET2-BBk oder eines anderen TARGET2-Komponenten-Systems in Kenntnis gesetzt. Die Teilnehmer tragen den Schaden, der aus der Einreichung von Zahlungsaufträgen an Teilnehmer resultiert, deren Teilnahme suspendiert oder beendet wurde, wenn solche Zahlungsaufträge in TARGET2-BBk eingereicht wurden, nachdem die ICM-Nachricht zur Verfügung gestellt wurde.

5. Nach Beendigung der Teilnahme eines Teilnehmers nimmt TARGET2-BBk keine weiteren Zahlungsaufträge von diesem Teilnehmer mehr an. Zahlungsaufträge in der Warteschlange, gespeicherte Zahlungsaufträge oder neue Zahlungsaufträge zugunsten dieses Teilnehmers werden zurückgegeben.

6. Im Fall der Suspendierung eines PM-Kontoinhabers von TARGET2-BBk aus anderen als den in Absatz 1 Buchstabe a genannten Gründen werden alle seine eingehenden und ausgehenden Zahlungsaufträge gesammelt und erst nach ausdrücklicher Annahme durch die Zentralbank des suspendierten PM-Kontoinhabers in die Eingangsdisposition eingestellt.

7. Im Fall der Suspendierung eines PM-Kontoinhabers von TARGET2-BBk aus den in Absatz 1 Buchstabe a genannten Gründen werden alle ausgehenden Zahlungsaufträge dieses PM-Kontoinhabers nur verarbeitet auf Weisung seiner vertretungsberechtigten Personen einschließlich behördlich oder gerichtlich bestellter Vertreter, unter anderem der Insolvenzverwalter des PM-Kontoinhabers, oder auf der Grundlage einer vollziehbaren behördlichen Entscheidung oder nach Maßgabe einer gerichtlichen Anordnung zur Zahlungsverarbeitung. Alle eingehenden Zahlungen werden gemäß Absatz 6 verarbeitet.

Artikel 30 – Schließung von PM-Konten

1. Die Teilnehmer können ihre PM-Konten jederzeit unter Einhaltung einer Kündigungsfrist von 14 Geschäftstagen schließen.

2. Im Falle einer Beendigung der Teilnahme entweder gemäß Artikel 28 oder gemäß Artikel 29 schließt die Bank die PM-Konten des betreffenden Teilnehmers, nachdem sie

a) die in der Warteschlange befindlichen Zahlungsaufträge abgewickelt oder zurückgegeben hat und

b) ihre Pfand- und Aufrechnungsrechte nach Artikel 31 ausgeübt hat.

TITEL IX

SCHLUSSBESTIMMUNGEN

Artikel 31 – Pfand- und Aufrechnungsrechte der Bank

1. Zur Besicherung aller gegenwärtigen und künftigen Ansprüche aus dem Vertragsverhältnis zwischen den Parteien hat die Bank ein Pfandrecht an allen bestehenden und künftigen Guthaben auf den PM-Konten des Teilnehmers.
2. Ungeachtet der Einleitung eines Insolvenzverfahrens gegen einen Teilnehmer, einer gerichtlichen oder sonstigen Pfändung, einer Abtretung oder einer sonstigen Verfügung über Rechte des Teilnehmers werden in folgenden Fällen alle Verbindlichkeiten des Teilnehmers automatisch und mit sofortiger Wirkung fällig gestellt: bei Eintritt
   (a) eines Ausfallsereignisses gem. Artikel 29 Absatz 1 oder
   (b) eines anderen Ausfallsereignisses oder eines in Art. 29 Absatz 2 genannten Falles, wenn dieses Ausfallereignis bzw. dieser Fall zu einer Beendigung oder Suspendierung eines Teilnehmers in TARGET2-BBk geführt hat.

   Die Fälligstellung tritt ohne Vorankündigung oder behördliche Genehmigung ein. Ferner werden die beiderseitigen Verbindlichkeiten des Teilnehmers und der Bank automatisch gegeneinander aufgerechnet. Die Vertragspartei, die den höheren Betrag schuldet, hat der anderen die Differenz zu zahlen.
3. Die Bank informiert den Teilnehmer unverzüglich über gemäß Absatz 2 erfolgte Aufrechnungen.
4. Die Bank ist jederzeit und ohne Vorankündigung berechtigt, das PM-Konto eines Teilnehmers mit Beträgen zu belasten, die der betreffende Teilnehmer der Bank aus der Geschäftsbeziehung zwischen dem Teilnehmer und der Bank schuldet.

Artikel 32 – Sicherungsrechte an Guthaben auf Unterkonten

1. Der Bank steht ein Pfandrecht über die Guthaben auf Teilnehmer-Unterkonten zu, die eröffnet wurden, um die Abwicklung nebensystembezogener Zahlungsaufträge gemäß den Vereinbarungen zwischen dem betreffenden Nebensystem und dessen Zentralbank zu ermöglichen. Das Guthaben dient der Sicherung der in Absatz 7 genannten Verpflichtung des Teilnehmers gegenüber der Bank, die aus jener Abwicklung resultiert.
2. Auf Anforderung durch das Nebensystem (mittels der Nachricht „Beginn des Zyklus“ (*start of cycle*)) sperrt die Bank das Guthaben auf dem Unterkonto des Teilnehmers. Gegebenenfalls erhöht oder reduziert die Bank danach den eingefrorenen Betrag durch Gutschrift oder Belastung des Unterkontos von bzw. mit Zahlungen im Wege der systemübergreifenden Abwicklung oder durch Gutschrift von Liquiditätsübertragungen auf dem Unterkonto. Auf Mitteilung des Nebensystems (mittels der Nachricht „Ende des Zyklus“ (*end of cycle)*) wird das Guthaben wieder freigegeben.
3. Durch die Bestätigung, dass das Guthaben auf dem Unterkonto des Teilnehmers gesperrt wurde, übernimmt die Bank gegenüber dem Nebensystem eine Zahlungsgarantie bis zum Betrag dieses Guthabens. Durch die gegebenenfalls abzugebende Bestätigung der Erhöhung oder Reduzierung des eingefrorenen Betrags durch Gutschrift oder Belastung des Unterkontos von bzw. mit

Zahlungen im Wege der systemübergreifenden Abwicklung oder durch Gutschrift von Liquiditätsübertragungen auf dem Unterkonto wird die Garantie automatisch um den Betrag der Zahlung erhöht oder reduziert. Unbeschadet der vorgenannten Erhöhung oder Reduzierung ist die Garantie unwiderruflich, unbedingt und zahlbar auf erstes Anfordern. Ist die Bank nicht die Zentralbank des Nebensystems, gilt die Bank als angewiesen, gegenüber der Zentralbank des Nebensystems die vorgenannte Garantie zu übernehmen.

4. Unter normalen Umständen (d.h. soweit kein Insolvenzverfahren in Bezug auf den Teilnehmer eingeleitet wurde) werden die nebensystembezogenen Zahlungsaufträge für den Ausgleich der Abrechnungsverbindlichkeit des Teilnehmers ohne Rückgriff auf die Garantie oder das Sicherungsrecht über das Guthaben auf dem Teilnehmer-Unterkonto abgewickelt.

5. Im Falle eines Insolvenzverfahrens in Bezug auf einen Teilnehmer umfasst der nebensystembezogene Zahlungsauftrag zum Ausgleich der Abrechnungsverbindlichkeit des Teilnehmers gleichzeitig eine Aufforderung zur Zahlung aus der Garantie; die Belastung des angewiesenen Betrags vom Teilnehmer-Unterkonto (sowie die Gutschrift auf dem technischen Konto des Nebensystems) beinhalten daher sowohl die Erfüllung der Verpflichtung der Bank aus der Garantie als auch die Ausübung ihres Sicherungsrechts über das Guthaben auf dem Teilnehmer-Unterkonto.

6. Die Garantie erlischt nach der Mitteilung (mittels der Nachricht „Ende des Zyklus“ (*end of cycle*)) durch das Nebensystem, dass die Abwicklung abgeschlossen ist.

7. Der Teilnehmer ist verpflichtet, der Bank alle Zahlungen zu erstatten, die Letztere aufgrund der Inanspruchnahme aus der Garantie erbracht hat.

Artikel 33 – Vertraulichkeit

1. Die Bank behandelt alle sicherheitsrelevanten oder geheimhaltungsbedürftigen Informationen vertraulich. Dies gilt auch, wenn es sich hierbei um zahlungsbezogene, technische oder organisatorische Informationen des Teilnehmers, der Teilnehmer derselben Gruppe oder seiner Kunden handelt, es sei denn, der Teilnehmer oder seine Kunden haben der Offenlegung schriftlich zugestimmt oder diese Offenlegung ist nach deutschem Recht erlaubt oder erforderlich.

1a. Abweichend von Absatz 1 erklärt der Teilnehmer, dass die in Artikel 29 behandelten Informationen oder Handlungen nicht als vertraulich gelten.

2. Abweichend von Absatz 1 erklärt der Teilnehmer hiermit seine Zustimmung zur Weiterleitung von zahlungsbezogenen, technischen oder organisatorischen Informationen, die ihn, seine Kunden oder Teilnehmer aus derselben Gruppe betreffen und die die Bank im Rahmen des Betriebs von TARGET2-BBk erhalten hat, sofern die Weitergabe nicht dem anwendbaren Recht widerspricht. Die Weiterleitung kann erfolgen: a) an andere Zentralbanken oder am Betrieb von TARGET2-BBk beteiligte Dritte, soweit dies für das effiziente Funktionieren von TARGET2 oder die Überwachung der Risiken des Teilnehmers oder der Risiken seiner Gruppe erforderlich ist, b) an andere Zentralbanken, die diese für erforderliche Analysen zum Zwecke der Marktoperationen, Geldpolitik, Finanzstabilität oder Finanzmarktintegration benötigen, oder c) an Aufsichts-,

Abwicklungs- oder Überwachungsbehörden der Mitgliedstaaten und der Union einschließlich Zentralbanken, soweit dies für die Erfüllung ihrer öffentlichen Aufgaben erforderlich ist. Die Bank haftet nicht für die finanziellen und wirtschaftlichen Konsequenzen dieser Offenlegung.

3. Abweichend von Absatz 1 und vorausgesetzt, dass dabei die Identität des Teilnehmers oder seiner Kunden weder direkt noch indirekt ermittelt werden kann, ist die Bank berechtigt, Zahlungsinformationen über den Teilnehmer oder dessen Kunden zu verwenden, offenzulegen oder zu veröffentlichen, und zwar für statistische, historische, wissenschaftliche oder sonstige Zwecke im Rahmen der Erfüllung ihrer öffentlichen Aufgaben oder der Aufgaben anderer öffentlichen Stellen, an welche die Informationen weitergegeben werden können.

4. Teilnehmer dürfen Informationen im Zusammenhang mit dem Betrieb von TARGET2-BBk, auf die sie Zugriff hatten, ausschließlich für die in diesen Bedingungen genannten Zwecke verwenden. Die Teilnehmer behandeln diese Informationen vertraulich, es sei denn, die Bank hat ihre ausdrückliche schriftliche Zustimmung zur Offenlegung erteilt. Die Teilnehmer stellen sicher, dass Dritte, an die sie Aufgaben auslagern, übertragen oder weitervergeben, welche Auswirkungen auf die Ausübung ihrer Verpflichtungen gemäß diesen Bedingungen haben oder haben können, an die Vertraulichkeitsanforderungen dieses Artikels gebunden sind.

5. Zur Abwicklung von Zahlungsaufträgen ist die Bank befugt, die erforderlichen Daten zu verarbeiten und an den Netzwerkdienstleister zu übertragen.

Artikel 34 – Datenschutz, Geldwäschebekämpfung, Verwaltungsmaßnahmen oder restriktive Maßnahmen und damit zusammenhängende Aspekte

1. Es wird davon ausgegangen, dass sich die Teilnehmer ihrer gesetzlichen Pflichten zum Datenschutz bewusst sind, diese einhalten und in der Lage sind, die Einhaltung gegenüber den betreffenden zuständigen Behörden nachzuweisen. Sie sind sich ihrer gesetzlichen Pflichten zur Bekämpfung der Geldwäsche, der Terrorismusfinanzierung, proliferationsrelevanter nuklearer Tätigkeiten und der Entwicklung von Trägersystemen für Kernwaffen bewusst und halten diese ein; insbesondere treffen sie danach angemessene Vorkehrungen bei den Zahlungen, die auf ihren PM-Konten verbucht werden. Die Teilnehmer stellen vor Abschluss des Vertrags mit dem Internetdienstleister sicher, dass sie mit den Regelungen des Internetdienstleisters zur Wiederherstellung verloren gegangener Daten vertraut sind.

2. Die Bank gilt als vom Teilnehmer ermächtigt, von nationalen oder ausländischen Finanz- oder Aufsichtsbehörden oder Industrieverbänden Informationen über ihn einzuholen, falls diese für seine Teilnahme an TARGET2-BBk erforderlich sind.

3. Wenn Teilnehmer als Zahlungsdienstleister eines Zahlers oder Zahlungsempfängers handeln, müssen sie alle für sie geltenden Anforderungen erfüllen, die sich aus Verwaltungsmaßnahmen oder restriktiven Maßnahmen gemäß Artikel 75 bzw. Artikel 215 des Vertrags über die Arbeitsweise der Europäischen Union ergeben, einschließlich im Hinblick auf die Benachrichtigung und/oder Einholung der Zustimmung einer zuständigen Behörde im Zusammenhang mit der Bearbeitung von Transaktionen. Darüber hinaus gilt Folgendes:

a) Ist die Bank der Zahlungsdienstleister eines Teilnehmers, der Zahler ist,

i) muss der Teilnehmer im Namen der Zentralbank, die vorrangig zur Vornahme der Benachrichtigung oder Einholung der Zustimmung verpflichtet ist, die erforderliche Benachrichtigung vornehmen oder Zustimmung einholen und der Bank nachweisen, dass er die Benachrichtigung vorgenommen oder die Zustimmung eingeholt hat;

ii) darf der Teilnehmer einen Zahlungsauftrag für die Überweisung von Geldern auf ein von einer anderen Einheit als dem Teilnehmer gehaltenes Konto erst dann in TARGET2 einstellen, wenn er von der Bank die Bestätigung erhalten hat, dass die erforderliche Benachrichtigung oder Zustimmung vom Zahlungsdienstleister des Zahlungsempfängers oder im Namen des Zahlungsdienstleisters des Zahlungsempfängers vorgenommen bzw. erhalten wurde.

b) Ist die Bank der Zahlungsdienstleister eines Teilnehmers, der Zahlungsempfänger ist, muss der Teilnehmer im Namen der Zentralbank, die vorrangig zur Vornahme der Benachrichtigung oder Einholung der Zustimmung verpflichtet ist, die erforderliche Benachrichtigung vornehmen oder Zustimmung einholen und der Bank nachweisen, dass er die Benachrichtigung vorgenommen oder die Zustimmung eingeholt hat.

Im Sinne dieses Absatzes haben die Begriffe ‚Zahlungsdienstleister', ‚Zahler' und ‚Zahlungsempfänger' die Bedeutungen, die ihnen in den einschlägigen Verwaltungs- oder restriktiven Maßnahmen zukommen.

Artikel 35 – Mitteilungen

1. Soweit in diesen Bedingungen nicht anders vorgesehen, werden alle gemäß diesen Bestimmungen erlaubten oder erforderlichen Mitteilungen per Einschreiben, Fax oder sonst schriftlich übermittelt. Mitteilungen an die Bank sind an den TARGET2-BBk National Service Desk bei der Deutschen Bundesbank, Wilhelm-Epstein-Straße 14, 60431 Frankfurt oder an den BIC der Deutschen Bundesbank, MARKDEFF, zu richten. Mitteilungen an den Teilnehmer sind an die von ihm mitgeteilte Adresse, Faxnummer oder an seinen BIC zu richten.
2. Als Nachweis für die Übermittlung einer Mitteilung reicht es aus, wenn die Auslieferung der Mitteilung an die entsprechende Adresse oder die Aufgabe zur Post des ordnungsgemäß adressierten Briefs mit jener Mitteilung nachgewiesen wird.
3. Alle Mitteilungen werden in Deutsch und/oder Englisch verfasst.
4. Die Teilnehmer sind an alle Formulare und Dokumente der Bank gebunden, die sie ausgefüllt und/oder unterzeichnet haben. Hierzu zählen unter anderem die Stammdatenformulare im Sinne von Artikel 7 Absatz 2 Buchstabe a und die gemäß Artikel 10 Absatz 5 zur Verfügung gestellten Daten, die gemäß Absatz 1 und 2 übermittelt wurden und von denen die Bank annehmen kann, dass sie von den Teilnehmern (einschließlich ihrer Angestellten oder Beauftragten) übermittelt wurden.

Artikel 36 – Änderungen

Die Bank kann diese Bedingungen, einschließlich der Anlagen, jederzeit ändern. Änderungen dieser Bedingungen, einschließlich der Anlagen, werden schriftlich oder auf elektronischem Wege bekannt gegeben. Die Änderungen gelten als angenommen, wenn der Teilnehmer nicht innerhalb von 14 Tagen, nachdem er über diese Änderungen informiert wurde, ausdrücklich widerspricht. Wenn ein Teilnehmer der Änderung widerspricht, ist die Bank berechtigt, die Teilnahme dieses Teilnehmers an TARGET2-BBk umgehend zu beenden und seine PM-Konten zu schließen.

Artikel 37 – Rechte Dritter

1. Rechte und Pflichten aus diesen Bedingungen dürfen ohne schriftliche Zustimmung der Bank nicht an Dritte übertragen oder verpfändet werden.
2. Diese Bedingungen begründen ausschließlich Rechte und Pflichten zwischen der Bank und den TARGET2-BBk-Teilnehmern.

Artikel 38 – Anwendbares Recht, Gerichtsstand und Erfüllungsort

1. Für die Geschäftsbeziehung zwischen der Bank und den TARGET2-BBk-Teilnehmern gilt deutsches Recht.
2. Unbeschadet der Zuständigkeit des Europäischen Gerichtshofes (EuGH) ist Frankfurt am Main der ausschließliche Gerichtsstand für alle Streitigkeiten aus der in Absatz 1 genannten Geschäftsbeziehung.
3. Der Erfüllungsort für das Rechtsverhältnis zwischen der Bank und den Teilnehmern ist Frankfurt am Main.

Artikel 39 – Salvatorische Klausel

Sollte eine Bestimmung dieser Bedingungen ungültig sein oder werden, bleiben alle übrigen Bedingungen hiervon unberührt.

Artikel 39a – Übergangsbestimmungen

1. Sobald das TARGET-System den Betrieb aufnimmt und der Betrieb von TARGET2 eingestellt wurde, werden PM-Kontosalden auf die entsprechenden Nachfolgekonten des Kontoinhabers im TARGET-System übertragen. Die PM-Konten werden zur Betriebsaufnahme von TARGET geschlossen und diese Bedingungen gegenstandslos.
2. Die Anforderung, dass PM-Kontoinhaber, die dem SEPA Instant Credit Transfer Scheme beigetreten sind, gemäß Artikel 5 auf der TIPS-Plattform erreichbar sein müssen, gilt ab dem 25. Februar 2022.

Artikel 40 – Inkrafttreten und Verbindlichkeit

1. Diese Bedingungen gelten ab dem 21. November 2021.
2. Mit der Beantragung eines PM-Kontos in TARGET2-BBk stimmen die Antragsteller, die den internetbasierten Zugang nutzen, diesen Bedingungen, sowohl im Verhältnis zu anderen Teilnehmern als auch gegenüber der Bank, automatisch zu.

TECHNISCHE SPEZIFIKATIONEN FÜR DIE VERARBEITUNG VON ZAHLUNGSAUFTRÄGEN IM RAHMEN DES INTERNETBASIERTEN ZUGANGS

Zusätzlich zu den Bedingungen gelten für die Abwicklung von Zahlungsaufträgen im Rahmen des internetbasierten Zugangs die folgenden Regelungen:

1. Technische Anforderungen für die Teilnahme an TARGET2-BBk bezüglich Infrastruktur, Netzwerk und Formaten

1) Jeder Teilnehmer, der den internetbasierten Zugang nutzt, muss sich mit dem ICM von TARGET2 verbinden, indem er einen Local Client, ein Betriebssystem und einen Internetbrowser gemäß dem Anhang „Internetbasierte Teilnahme - Systemanforderungen für den Internetzugang“ zu den User Detailed Functional Specifications (UDFS) mit bestimmten Einstellungen verwendet. Alle PM-Konten der Teilnehmer erhalten einen acht- bzw. elfstelligen BIC als Kennung. Darüber hinaus muss jeder Teilnehmer vor seiner Aufnahme in TARGET2-BBk eine Reihe von Tests bestehen, um seine technische und operationale Eignung unter Beweis zu stellen.

2) Für die Übermittlung von Zahlungsaufträgen und Zahlungsnachrichten im PM wird die TARGET2-Plattform BIC, TRGTXEPMLVP, als Sender und Empfänger von Nachrichten genutzt. Zahlungsaufträge, die an einen Teilnehmer gesendet werden, der den internetbasierten Zugang nutzt, sollten diesen Teilnehmer als Empfänger in dem Feld für den Begünstigten benennen. Zahlungsaufträge, die von einem Teilnehmer eingegeben wurden, der den internetbasierten Zugang nutzt, werden diesen Teilnehmer als den Auftraggeber identifizieren.

3) Die Teilnehmer, die den internetbasierten Zugang nutzen, verwenden die Public Key Infrastructure (PKI) gemäß dem „Benutzerhandbuch Internetzugang für den Public-Key-Zertifizierungsdienst“.

2. Typen von Zahlungsnachrichten

1) Die Teilnehmer, die den internetbasierten Zugang nutzen, können folgende Zahlungsarten nutzen:

   a) Kundenzahlungen, d.h. Überweisungen, bei denen der beauftragende und/oder begünstigte Kunde kein Finanzinstitut ist,

   b) STP-Kundenzahlungen, d.h. Überweisungen, bei denen der beauftragende und/oder begünstigte Kunde kein Finanzinstitut ist und die im Modus ‚durchgängig automatisierte Abwicklung’ (‚Straight Through Processing‘ – STP) ausgeführt werden,

   c) Bank-an-Bank-Überweisungen zur Anforderung von Geldtransfers zwischen Finanzinstituten,

d) Deckungszahlungen zur Anforderung von Geldtransfers zwischen Finanzinstituten im Zusammenhang mit einer zugrunde liegende Kundenüberweisung.

Darüber hinaus können die Teilnehmer, die den internetbasierten Zugang zu einem PM-Konto nutzen, Lastschriftaufträge empfangen.

2) Die Teilnehmer müssen die Feldbelegungsregeln, die in Kapitel 9.1.2.2 der UDFS, Buch 1, definiert sind, beachten.

3) Die Feldbelegung wird auf der Ebene von TARGET2-BBk gemäß den UDFS-Anforderungen geprüft. Die Teilnehmer können untereinander besondere Regeln für die Feldbelegung vereinbaren. Ob die Teilnehmer diese besonderen Regeln einhalten, wird innerhalb von TARGET2-BBk jedoch nicht geprüft.

4) Die Teilnehmer, die den internetbasierten Zugang nutzen, können über TARGET2 Deckungszahlungen vornehmen, d.h. Zahlungen durch Korrespondenzbanken zur Abwicklung (Deckung) von Überweisungsnachrichten, die auf andere, direktere Weise an die Bank eines Kunden übermittelt werden. Die in diesen Deckungszahlungen enthaltenen Kundendaten werden nicht im ICM angezeigt.

3. Überprüfung auf doppelte Auftragserteilung

1) Alle Zahlungsaufträge werden einer Überprüfung auf doppelte Auftragserteilung unterzogen, damit Zahlungsaufträge, die versehentlich mehr als einmal eingereicht wurden, zurückgewiesen werden können.

2) Folgende Felder von Nachrichtentypen werden überprüft:

Angaben	**Teil der Nachricht**	**Feld**
Absender	Basis-Header	BIC-Adresse
Nachrichtentyp	Anwendungsheader (Application Header)	Nachrichtentyp
Empfänger	Anwendungsheader (Application Header)	Zieladresse
Transaktionsreferenznummer (TRN)	Textblock	:20
Zugehörige Referenz (Related Reference)	Textblock	:21
Wertstellungsdatum/Valutadatum (Value Date)	Textblock	:32
Betrag	Textblock	:32

3) Stimmen alle in Absatz 2 beschriebenen Felder bezüglich eines neu eingereichten Zahlungsauftrags mit denen eines bereits angenommenen Zahlungsauftrags überein, wird der neu eingereichte Zahlungsauftrag zurückgegeben.

4. Fehlercodes

Wird ein Zahlungsauftrag zurückgewiesen, wird eine Abbruchmitteilung über das ICM zur Verfügung gestellt, in der mittels Fehlercodes der Grund für die Zurückweisung angegeben wird. Die Fehlercodes sind in Kapitel 9.4.2 der UDFS definiert.

5. Zeitvorgaben für die Abwicklung

1) Bei Zahlungsaufträgen mit Earliest Debit Time Indicator ist das Codewort „/FROTIME/“ zu verwenden.

2) Bei Zahlungsaufträgen mit Latest Debit Time Indicator stehen zwei Optionen zur Verfügung.

   a) Codewort „/REJTIME/“: Zahlungsaufträge, die nicht bis zum angegebenen Belastungszeitpunkt abgewickelt werden konnten, werden zurückgegeben.

   b) Codewort „/TILTIME/“: Zahlungsaufträge, die nicht bis zum angegebenen Belastungszeitpunkt abgewickelt werden konnten, werden nicht zurückgegeben, sondern bleiben in der entsprechenden Warteschlange.

   Für beide Optionen gilt: Wurden Zahlungsaufträge mit einem Latest Debit Time Indicator 15 Minuten vor der angegebenen Zeit noch nicht abgewickelt, wird der einreichende Teilnehmer über das ICM informiert.

3) Wenn das Codewort „/CLSTIME/“ verwendet wird, wird mit dem Zahlungsauftrag in gleicher Weise verfahren wie in Absatz 2 Buchstabe b.

6. Abwicklung von Zahlungsaufträgen in der Eingangsdisposition

1) Im Rahmen der Eingangsdisposition werden Zahlungsaufträge in eine einfache und, soweit zweckdienlich, in eine erweiterte Gegenläufigkeitsprüfung (jeweils im Sinne der Absätze 2 und 3) einbezogen, um eine rasche und liquiditätssparende Bruttoabwicklung zu gewährleisten.

2) Bei einer einfachen Gegenläufigkeitsprüfung wird zunächst festgestellt, ob an der Spitze der Warteschlange eines Zahlungsempfängers sehr dringende oder – falls es eine solche nicht gibt – dringende Aufträge stehen, die zur Verrechnung mit dem Zahlungsauftrag des Zahlers herangezogen werden können (nachfolgend „verrechenbare Zahlungsaufträge“). Wenn solche verrechenbaren Zahlungsaufträge nicht ausreichend Liquidität für die in der Eingangsposition befindlichen Zahlungsaufträge des Zahlers verschaffen, wird geprüft, ob auf seinem PM-Konto genügend Liquidität verfügbar ist.

3) Wenn die einfache Gegenläufigkeitsprüfung erfolglos bleibt, kann die Bank eine erweiterte Gegenläufigkeitsprüfung durchführen. Hierbei wird geprüft, ob in der Warteschlange eines

Zahlungsempfängers verrechenbare Zahlungsaufträge stehen, und zwar unabhängig davon, wann sie in die Warteschlange eingestellt wurden. Wenn sich allerdings in der Warteschlange des Zahlungsempfängers an andere TARGET2-Teilnehmer adressierte Zahlungsaufträge mit höherer Priorität befinden, kann vom FIFO-Prinzip nur abgewichen werden, wenn die Einbeziehung eines solchen verrechenbaren Zahlungsauftrags zu einem Liquiditätszufluss für den Zahlungsempfänger führen würde.

7. Abwicklung von Zahlungsaufträgen in der Warteschlange

1) Die Behandlung von Zahlungsaufträgen in Warteschlangen richtet sich nach der vom einreichenden Teilnehmer festgelegten Prioritätsstufe.

2) Zahlungsaufträge in der sehr dringenden und der dringenden Warteschlange werden bei Liquiditätszuflüssen oder bei Veränderungen innerhalb der Warteschlange (Veränderung der Position, der vorgegebenen Ausführungszeit, der Priorität oder Widerruf eines Zahlungsauftrags) unter Anwendung der in Abschnitt 6 beschriebenen Gegenläufigkeitsprüfungen abgewickelt, beginnend mit den Zahlungsaufträgen an der Spitze der Warteschlange.

3) Zahlungsaufträge in der normalen Warteschlange werden – unter Einbeziehung aller noch nicht abgewickelten sehr dringenden und dringenden Zahlungsaufträge – fortlaufend bearbeitet. Dabei kommen verschiedene Optimierungsverfahren (Algorithmen) zur Anwendung. Ist ein Algorithmus erfolgreich, werden die darin enthaltenen Zahlungsaufträge ausgeführt; wenn er nicht erfolgreich ist, verbleiben die betreffenden Zahlungsaufträge in der Warteschlange. Drei Algorithmen (1 bis 3) werden zur Verrechnung von Zahlungsströmen angewendet. Algorithmus 4 wird zur Abwicklung von Zahlungsaufträgen aus Nebensystemen im Abwicklungsverfahren 5 (wie in Kapitel 2.8.1 der UDFS beschrieben) eingesetzt. Ein besonderer Algorithmus (Algorithmus 5) wird zur Optimierung der Abwicklung von sehr dringenden Nebensystem-Zahlungsaufträgen über Unterkonten von Teilnehmern genutzt.

   a) Bei Algorithmus 1 („all-or-nothing“) wird die Bank sowohl für Beziehungen, für die ein bilaterales Limit festgesetzt wurde, als auch für die Gesamtheit der Beziehungen, für die ein multilaterales Limit festgesetzt wurde,

      i) die Gesamtliquiditätsposition jedes PM-Kontos der TARGET2-Teilnehmer berechnen, indem sie ermittelt, ob der (rechnerische) Saldo aus den in der Warteschlange befindlichen ein- und ausgehenden Zahlungsaufträgen positiv oder negativ ist. Wenn der (rechnerische) Saldo negativ ist, prüft die Bank, ob er die verfügbare Liquidität des Teilnehmers übersteigt (die so errechnete gesamte Liquidität bildet die „Gesamtliquiditätsposition“);

      ii) prüfen, ob die von den TARGET2-Teilnehmern festgelegten Limite und Reservierungen hinsichtlich jedes relevanten PM-Kontos eingehalten werden.

Wenn das Ergebnis dieser Berechnungen und Prüfungen für jedes betroffene PM-Konto positiv ausfällt, wickeln die Bank und sonstigen beteiligten Zentralbanken alle Zahlungen zeitgleich auf den PM-Konten der betreffenden TARGET2-Teilnehmer ab.

b) Bei Algorithmus 2 („partial“) wird die Bank

   i) wie bei Algorithmus 1 die Liquiditätspositionen, Limite und Reservierungen jedes betreffenden PM-Kontos ermitteln und überprüfen;

   ii) bei negativer Gesamtliquiditätsposition eines oder mehrerer betreffender PM-Konten einzelne Zahlungsaufträge herausnehmen, bis die Gesamtliquiditätsposition aller betreffenden PM-Konten positiv ist.

   Im Anschluss daran wickeln die Bank und die sonstigen beteiligten Zentralbanken alle verbleibenden Zahlungen (mit Ausnahme der herausgenommenen Zahlungsaufträge) zeitgleich auf den PM-Konten der betreffenden TARGET2-Teilnehmer ab, sofern ausreichend Deckung verfügbar ist.

   Bei der Herausnahme von Zahlungsaufträgen beginnt die Bank bei dem PM-Konto des TARGET2-Teilnehmers mit der höchsten negativen Gesamtliquiditätsposition und bei dem am Ende der Warteschlange befindlichen Zahlungsauftrag mit der niedrigsten Priorität. Das Auswahlverfahren läuft nur über einen kurzen Zeitraum, dessen Dauer im Ermessen der Bank steht.

c) Bei Algorithmus 3 („multiple“) wird die Bank

   i) PM-Konten von TARGET2-Teilnehmern paarweise gegenüberstellen, um zu errechnen, ob Zahlungsaufträge in der Warteschlange im Rahmen der verfügbaren Liquidität der betreffenden PM-Konten der beiden TARGET2-Teilnehmer und etwaiger gesetzter Limite abgewickelt werden können (ausgehend von den beiden PM-Konten, bei denen die Differenz zwischen den bilateral erteilten Zahlungsaufträgen am geringsten ist). Die beteiligte(n) Zentralbank(en) verbucht/en diese Zahlungen zeitgleich auf den PM-Konten der beiden TARGET2-Teilnehmer;

   ii) ferner, wenn bei einem PM-Kontenpaar im Sinne von Ziffer i die Liquidität zum Ausgleich der bilateralen Position nicht ausreicht, einzelne Zahlungsaufträge herausnehmen, bis ausreichend Liquidität verfügbar ist. In diesem Fall wickelt/n die beteiligte(n) Zentralbank(en) die verbleibenden Zahlungsaufträge (mit Ausnahme der herausgenommenen) zeitgleich auf den PM-Konten der beiden TARGET2-Teilnehmer ab.

   Nach Durchführung der in den Ziffern i und ii beschriebenen Prüfung ermittelt die Bank die multilaterale Position (zwischen dem PM-Konto eines Teilnehmers und den PM-Konten anderer TARGET2-Teilnehmer, für die ein multilaterales Limit gesetzt wurde). Zu diesem Zweck gilt das in den Ziffern i und ii beschriebene Verfahren entsprechend.

d) Bei Algorithmus 4 („partial plus ancillary system settlement“) verfährt die Bank ebenso wie bei Algorithmus 2, jedoch ohne Herausnahme von Zahlungsaufträgen, die dem Zahlungsausgleich eines Nebensystems (das die Abwicklung auf simultan-multilateraler Basis durchführt) dienen.

e) Bei Algorithmus 5 („ancillary system settlement via sub-accounts“) verfährt die Bank ebenso wie bei Algorithmus 1, wobei sie jedoch Algorithmus 5 über die Nebensystem-Schnittstelle („Ancillary System Interface – ASI“) startet. Dabei überprüft die Bank lediglich, ob auf den Unterkonten der Teilnehmer ausreichend Deckung verfügbar ist. Zudem werden keine Limite und Reservierungen berücksichtigt. Algorithmus 5 läuft auch während der Nachtverarbeitung.

4) Trotz des Starts eines der Algorithmen 1 bis 4 können in die Eingangsdisposition eingestellte Zahlungsaufträge dort umgehend abgewickelt werden, wenn die Positionen und Limite der betreffenden PM-Konten der TARGET2-Teilnehmer mit der Abwicklung dieser Zahlungsaufträge und der Abwicklung von Zahlungsaufträgen im Rahmen des laufenden Optimierungsverfahrens im Einklang stehen. Zwei Algorithmen laufen jedoch nie gleichzeitig.

5) Während der Tagverarbeitung laufen die Algorithmen nacheinander. Solange keine simultan-multilaterale Abwicklung eines Nebensystems ansteht, lautet die Reihenfolge wie folgt:

a) Algorithmus 1;

b) wenn Algorithmus 1 erfolglos ist, folgt Algorithmus 2;

c) wenn Algorithmus 2 erfolglos ist, folgt Algorithmus 3; ist Algorithmus 2 erfolgreich, wird Algorithmus 1 wiederholt.

Wenn eine simultan-multilaterale Abwicklung (Abwicklungsverfahren 5) bei einem Nebensystem ansteht, läuft Algorithmus 4.

6) Die verschiedenen Algorithmen laufen flexibel und mit bestimmtem zeitlichem Versatz ab, um einen zeitlichen Mindestabstand zwischen dem Ablauf von zwei Algorithmen sicherzustellen. Die zeitliche Abfolge wird automatisch gesteuert. Ein manuelles Eingreifen ist jedoch möglich.

7) Während ein Zahlungsauftrag einen Algorithmus durchläuft, kann weder seine Position in der Warteschlange geändert noch kann er widerrufen werden. Bis zum Abschluss eines laufenden Algorithmus werden Anträge auf Änderung der Position oder Widerruf eines Zahlungsauftrags in eine Warteschlange gestellt. Wurde ein Zahlungsauftrag während des laufenden Algorithmus abgewickelt, werden Anträge auf Änderung der Position oder Widerruf zurückgewiesen. Wurde er dagegen nicht abgewickelt, wird der Antrag des Teilnehmers umgehend berücksichtigt.

8. Nutzung des Informations- und Kontrollmoduls (ICM)

1) Das ICM kann für die Eingabe von Zahlungsaufträgen genutzt werden.

2) Das ICM kann für den Informationsaustausch und die Liquiditätssteuerung genutzt werden.

3) Mit Ausnahme von gespeicherten Zahlungsaufträgen und Kundenstammdaten sind über das ICM lediglich Daten, die sich auf den laufenden Geschäftstag beziehen, abrufbar. Die Bildschirmmasken werden nur in englischer Sprache angeboten.

4) Informationen werden im Anfragemodus (pull) bereitgestellt; das bedeutet, dass jeder Teilnehmer um Bereitstellung von Informationen ersuchen muss. Die Teilnehmer überprüfen das ICM während des Geschäftstages regelmäßig auf wichtige Nachrichten.

5) Für die Teilnehmer, die den internetbasierten Zugang nutzen, steht nur der User-to-Application-Modus (U2A) zur Verfügung. Der U2A ermöglicht die direkte Kommunikation zwischen dem Teilnehmer und dem ICM. Die Informationen werden in einem Browser angezeigt, der auf einem PC läuft. Weitere Einzelheiten sind im ICM-Benutzerhandbuch aufgeführt.

6) Jeder Teilnehmer verfügt über mindestens einen Computerarbeitsplatz mit Internetzugang, um über U2A Zugriff auf das ICM zu erhalten.

7) Die Zugriffsrechte für das ICM werden mittels Zertifikaten gewährt, deren Nutzung in den Absätzen 10 bis 13 ausführlicher beschrieben wird.

8) Die Teilnehmer können das ICM auch nutzen, um Liquidität

   a) von ihrem PM-Konto auf ein HAM-Konto,

   b) zwischen dem PM-Konto und den Unterkonten des betreffenden Teilnehmers sowie

   c) vom PM-Konto im Rahmen des Abwicklungsverfahrens 6 , (‚Echtzeit') auf das technische Konto eines Nebensystems zu übertragen.

9. Die UDFS, das ICM-Benutzerhandbuch und das „Benutzerhandbuch: Internetzugang für den Public-Key-Zertifizierungsdienst"

Weitere Einzelheiten und Beispiele zur Erläuterung der oben aufgeführten Regeln sind in den UDFS und im ICM-Benutzerhandbuch, die von Zeit zu Zeit geändert und auf der Website der Bank sowie der TARGET2-Website (in englischer Sprache) veröffentlicht werden, sowie im „Benutzerhandbuch: Internetzugang für den Public-Key-Zertifizierungsdienst" aufgeführt.

10. Ausstellung, Suspendierung, Reaktivierung, Widerruf und Erneuerung von Zertifikaten

1) Der Teilnehmer beantragt bei der Bank die Ausstellung von Zertifikaten, die den Zugang zu TARGET2-Bank im Rahmen des internetbasierten Zugangs ermöglichen.

2) Der Teilnehmer beantragt bei der Bank die Suspendierung und die Reaktivierung sowie den Widerruf und die Erneuerung von Zertifikaten, wenn ein Zertifikatsinhaber nicht länger

wünscht, Zugang zu TARGET2 zu haben, oder wenn der Teilnehmer seine Aktivitäten in TARGET2-BBk (z.B. infolge einer Fusion oder Übernahme) einstellt.

3) Der Teilnehmer trifft alle Vorsichtsmaßnahmen und organisatorische Vorkehrungen um sicherzustellen, dass die Zertifikate ausschließlich im Einklang mit den Harmonisierten Bedingungen verwendet werden.

4) Der Teilnehmer informiert die Bank unverzüglich über wesentliche Änderungen der Informationen, die in den an die Bank in Verbindung mit der Ausstellung von Zertifikaten übermittelten Formulare enthalten sind.

5) Ein Teilnehmer kann höchstens fünf aktive Zertifikate für jedes PM-Konto haben. Auf Anfrage kann die Bank nach ihrem Ermessen die Ausstellung weiterer Zertifikate von den Zertifizierungsstellen beantragen.

11. Umgang mit Zertifikaten durch den Teilnehmer

1) Der Teilnehmer stellt die sichere Verwahrung aller Zertifikate sicher und ergreift wirksame organisatorische und technische Maßnahmen, um Schäden für Dritte zu vermeiden und zu gewährleisten, dass jedes Zertifikat ausschließlich von dem spezifischen Zertifikatsinhaber verwendet wird, an den es ausgestellt wurde.

2) Der Teilnehmer stellt unverzüglich alle Informationen zur Verfügung, die von der Bank angefordert werden und gewährleistet die Zuverlässigkeit dieser Informationen. Die Teilnehmer tragen zu jeder Zeit die volle Verantwortung für die kontinuierliche Richtigkeit aller der Bank zur Verfügung gestellten Informationen. im Zusammenhang mit der Ausstellung von Zertifikaten.

3) Der Teilnehmer übernimmt die volle Verantwortung für die Gewährleistung, dass alle seine Zertifikatsinhaber die ihnen zugewiesenen Zertifikate getrennt von den geheimen PIN- und PUK-Codes aufbewahren.

4) Der Teilnehmer übernimmt die volle Verantwortung für die Gewährleistung, dass keiner seiner Zertifikatsinhaber die Zertifikate für andere Funktionen oder Zwecke verwendet als die, für welche die Zertifikate ausgestellt wurden.

5) Der Teilnehmer informiert die Bank unverzüglich über jeden Antrag und die Gründe für die Suspendierung, die Reaktivierung, den Widerruf oder die Erneuerung von Zertifikaten.

6) Der Teilnehmer beantragt bei der Bank unverzüglich die Suspendierung von Zertifikaten, oder der darin enthaltenen Schlüssel, die fehlerhaft sind oder die sich nicht mehr im Besitz ihres Zertifikatsinhabers befinden.

7) Der Teilnehmer informiert die Bank unverzüglich über jeden Verlust oder Diebstahl der Zertifikate.

12. Sicherheitsanforderungen

1) Das Computersystem, das ein Teilnehmer für den Zugang zu TARGET2 im Rahmen des internetbasierten Zugangs nutzt, befindet sich in Räumlichkeiten, die im Eigentum des Teilnehmers stehen oder von diesem gemietet werden. Der Zugang zu TARGET2-BBk ist nur von diesen Räumlichkeiten aus gestattet und es wird klargestellt, dass ein Fernzugang nicht gestattet ist.

2) Der Teilnehmer verwendet auf Computersystemen Software, die gemäß aktuellen internationalen IT-Sicherheitsstandards installiert und eingerichtet wird, wobei die genannten Sicherheitsstandards mindestens die in den Abschnitten 12 Absatz 3 und 13 Absatz 4 beschriebenen Anforderungen enthalten müssen. Der Teilnehmer führt angemessene Maßnahmen ein, wozu insbesondere Viren- und Malware-Schutz, Anti-Phishing-Maßnahmen, Maßnahmen zur Erhöhung des Sicherheitsgrads (sog. „Hardening“) und Verfahren zur Verwaltung von Korrekturauslieferungen („Patch Management Procedures“) gehören. Alle diese Maßnahmen und Verfahren werden regelmäßig vom Teilnehmer aktualisiert.

3) Der Teilnehmer führt eine verschlüsselte Kommunikationsverbindung zu TARGET2-BBk für den Internetzugang ein.

4) Benutzerkonten auf den Computerarbeitsplätzen des Teilnehmers werden keine Systemverwaltungsrechte zugewiesen. Rechte werden gemäß dem „Least Privilege“-Prinzip (Prinzip, nach dem den Nutzern nur die Rechte zugewiesen werden, die sie benötigen) zugewiesen.

5) Der Teilnehmer schützt die für den Internetzugang für TARGET2-BBk verwendeten Computersysteme zu jeder Zeit wie folgt:

   a) Sie schützen die Computersysteme und Computerarbeitsplätze vor unberechtigtem physischen Zugriff und Zugriff über das Netzwerk – wobei zu jeder Zeit eine Firewall zur Abschirmung der Computersysteme und Computerarbeitsplätze vor eingehendem Internetdatenverkehr einzusetzen ist – und die Computerarbeitsplätze vor unberechtigtem Zugriff über das interne Netzwerk. Sie setzen eine Firewall ein, die vor eingehendem Datenverkehr schützt, sowie eine Firewall auf den Computerarbeitsplätzen, die sicherstellt, dass ausschließlich zugelassene Programme nach außen kommunizieren.

   b) Die Teilnehmern dürfen nur Software auf den Computerarbeitsplätzen installieren, die für den Zugang zu TARGET2 erforderlich und gemäß den internen Sicherheitsvorgaben des Teilnehmers zugelassen ist.

   c) Die Teilnehmer stellen zu jeder Zeit sicher, dass alle Softwareanwendungen, die auf den Computerarbeitsplätzen laufen, regelmäßig aktualisiert und mit den neuesten Korrekturauslieferungen ausgestattet („gepatcht“) werden. Dies gilt insbesondere im Hinblick auf das Betriebssystem, den Internetbrowser und Plug-Ins.

d) Die Teilnehmer beschränken den von den Computerarbeitsplätzen hinausgehenden Datenverkehr zu jeder Zeit auf geschäftsrelevante Seiten sowie auf Seiten, die für berechtigte und angemessene Softwareaktualisierungen erforderlich sind.

e) Die Teilnehmer gewährleisten, dass alle Ströme sensibler interner Informationen an oder von den Computerarbeitsplätzen gegen Offenlegung und bösartige Änderungen geschützt werden, insbesondere, wenn Dateien durch ein Netzwerk übertragen werden.

6) Der Teilnehmer gewährleistet, dass seine Zertifikatsinhaber zu jeder Zeit Praktiken für sicheres Browsen anwenden, zum Beispiel

a) bestimmte Computerarbeitsplätze für den Zugriff auf Seiten mit demselben Gefährlichkeitsgrad zu reservieren und auf diese Seiten nur von diesen Computerarbeitsplätzen zuzugreifen,

b) die Browser-Sitzung vor und nach dem Zugriff auf TARGET2-BBk immer neu zu starten,

c) die Authentizität des SSL-Zertifikats jedes Servers bei jeder Anmeldung zum Internetzugang für TARGET2-BBk zu überprüfen,

d) bei E-Mails, die von TARGET2-BBk zu kommen scheinen, misstrauisch zu sein und das Passwort für ein Zertifikat nicht herauszugeben, wenn nach diesem Passwort gefragt wird, da TARGET2-BBk weder in einer E-Mail noch auf anderem Wege nach einem Passwort für ein Zertifikat fragen wird.

7) Der Teilnehmer befolgt die folgenden Systemverwaltungsgrundsätze zu jeder Zeit, um die Risiken für sein System zu verringern:

a) Einführung von Nutzerverwaltungspraktiken, die sicherstellen, dass nur berechtigte Nutzer eingerichtet werden und im System verbleiben, und Unterhaltung einer genauen und aktuellen Liste befugter Nutzer;

b) Überprüfung des täglichen Zahlungsverkehrs, um Abweichungen zwischen dem zugelassenen und dem tatsächlichen täglichen Zahlungsverkehr (sowohl im Hinblick auf Sendung als auch auf Empfang) aufzudecken;

c) Gewährleistung, dass ein Zertifikatsinhaber nicht – während er auf TARGET2-BBk zugreift – gleichzeitig eine andere Internetseite aufruft.

13. Zusätzliche Sicherheitsanforderungen

1) Der Teilnehmer gewährleistet zu jeder Zeit durch angemessene organisatorische und/oder technische Maßnahmen, dass Nutzeridentitäten, die zum Zwecke der Überprüfung von Zugriffsrechten („Access Right Review“) offengelegt werden, nicht missbraucht werden und insbesondere, dass keine unbefugten Personen Kenntnis von ihnen erlangen.

2) Der Teilnehmer muss über ein Verfahren zur Nutzerverwaltung verfügen, in dem für den Fall, dass ein Arbeitnehmer oder ein anderer Nutzer eines Systems am Standort eines

Teilnehmers die Organisation dieses Teilnehmers verlässt, die sofortige und dauerhafte Löschung der jeweiligen Nutzeridentität sichergestellt werden kann.

3) Der Teilnehmer muss über ein Verfahren zur Nutzerverwaltung verfügen, in dem Nutzeridentitäten, die auf irgendeine Weise manipuliert wurden, sofort und dauerhaft blockiert werden, einschließlich in Fällen, in denen die Zertifikate verloren gegangen sind oder gestohlen wurden oder in denen ein Passwort im Wege des Phishing aufgedeckt wurde.

4) Ist ein Teilnehmer nicht in der Lage, sicherheitsbezogene Mängel oder Konfigurationsfehler (die z.B. dadurch verursacht werden, dass Systeme mit Malware infiziert sind) nach drei Vorfällen zu beheben, können die Anbieter-Zentralbanken alle Nutzeridentitäten des Teilnehmers dauerhaft blockieren.

TARGET2-AUSGLEICHSREGELUNG

1. Allgemeine Grundsätze

a) Wenn in TARGET2 eine technische Störung auftritt, können die direkten Teilnehmer gemäß der in dieser Anlage festgelegten TARGET2-Ausgleichsregelung Ausgleichsforderungen geltend machen.

b) Vorbehaltlich einer anders lautenden Entscheidung des EZB-Rates 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.

c) Ausgleichszahlungen gemäß der TARGET2-Ausgleichsregelung stellen den einzigen Ausgleichsmechanismus dar, der im Falle einer technischen Störung von TARGET2 angeboten wird. Die Teilnehmer können jedoch auf anderem rechtlichen Wege Ausgleichsforderungen geltend machen. Mit Annahme eines Ausgleichsangebots im Rahmen der TARGET2-Ausgleichsregelung verzichtet der 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.

d) Ein Ausgleichsangebot stellt kein Haftungszugeständnis der Bank oder einer anderen Zentralbank in Bezug auf eine technische Störung von TARGET2 dar.

2. Bedingungen für Ausgleichsangebote

a) Ein Zahler kann eine Aufwandspauschale und eine Zinsausgleichszahlung geltend machen, wenn aufgrund einer technischen Störung von TARGET2 ein Zahlungsauftrag nicht am Geschäftstag seiner Annahme abgewickelt wurde.

b) Ein Zahlungsempfänger kann eine Aufwandspauschale geltend machen, wenn er aufgrund einer technischen Störung von TARGET2 eine an einem bestimmten Geschäftstag erwartete Zahlung nicht empfangen hat. Der Zahlungsempfänger kann ferner eine Zinsausgleichszahlung geltend machen, wenn eine oder mehrere der folgenden Bedingungen erfüllt sind:

i) bei Teilnehmern, die Zugang zur Spitzenrefinanzierungsfazilität haben: wenn ein Zahlungsempfänger aufgrund einer technischen Störung von TARGET2 die Spitzenrefinanzierungsfazilität in Anspruch genommen hat und/oder

ii) bei allen Teilnehmern: wenn es technisch unmöglich war, sich über den Geldmarkt zu refinanzieren, oder eine solche Refinanzierung aus anderen, objektiv nachvollziehbaren Gründen unmöglich war.

3. Berechnung des Ausgleichs

a) Bei einem Ausgleichsangebot für einen Zahler gilt Folgendes:

i) Die Aufwandspauschale beträgt in Bezug auf jeden einzelnen Zahlungsempfänger für den ersten nicht ausgeführten Zahlungsauftrag 50 €, für die nächsten vier nicht ausgeführten Zahlungsaufträge jeweils 25 € und für jeden weiteren nicht ausgeführten Zahlungsauftrag 12,50 €.

ii) Die Zinsausgleichszahlung erfolgt auf der Basis des täglich neu festzulegenden Referenzzinssatzes. Dies ist entweder der EONIA (Euro Overnight Index Average) oder der Spitzenrefinanzierungssatz, je nachdem, welcher der beiden niedriger ist. Der Referenzzinssatz wird auf den Betrag des Zahlungsauftrags angewandt, der aufgrund der technischen Störung von TARGET2 nicht ausgeführt wurde, und zwar für jeden Tag zwischen dem Datum der tatsächlichen oder — bei Zahlungsaufträgen im Sinne von Abschnitt 2 Buchstabe b Ziffer ii — der beabsichtigten Einreichung des Zahlungsauftrags und dem Datum, an dem der Zahlungsauftrag erfolgreich abgewickelt wurde oder hätte abgewickelt werden können. Zinsen oder Gebühren, die sich aus nicht ausgeführten Zahlungsaufträgen in der Einlagefazilität des Eurosystems ergeben, werden vom Ausgleichsbetrag abgezogen bzw. diesem in Rechnung gestellt.

iii) Eine Zinsausgleichszahlung erfolgt nicht, wenn und soweit Mittel aus nicht ausgeführten Zahlungsaufträgen am Geldmarkt angelegt oder zur Erfüllung des Mindestreserve-Solls verwendet wurden.

b) Bei einem Ausgleichsangebot für einen Zahlungsempfänger gilt Folgendes:

i) Die Aufwandspauschale beträgt in Bezug auf jeden einzelnen Zahler für den ersten nicht ausgeführten Zahlungsauftrag 50 €, für die nächsten vier nicht ausgeführten Zahlungsaufträge jeweils 25 € und für jeden weiteren nicht ausgeführten Zahlungsauftrag 12,50 €.

ii) Die in Buchstabe a Ziffer ii dargelegte Methode zur Berechnung der Zinsausgleichszahlung findet mit der Maßgabe Anwendung, dass die Zinsausgleichszahlung auf der Differenz zwischen dem Spitzenrefinanzierungssatz und dem Referenzzinssatz beruht und anhand des Betrags berechnet wird, der sich aus der Inanspruchnahme der Spitzenrefinanzierungsfazilität aufgrund der technischen Störung von TARGET2 ergibt.

4. Verfahrensvorschriften

a) Ausgleichsforderungen sind auf dem Antragsformular geltend zu machen, das auf der Website der Bank in englischer Sprache zur Verfügung steht (siehe www.bundesbank.de). 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.

b) Teilnehmer müssen ihre Anträge innerhalb von vier Wochen nach einer technischen Störung von TARGET2 bei der Bank einreichen. Weitere Informationen oder Belege, die die Bank anfordert, sind innerhalb von zwei Wochen nach Anforderung einzureichen.

c) Die Bank prüft die Anträge und leitet sie an die EZB weiter. Vorbehaltlich eines anders lautenden, den Teilnehmern mitzuteilenden Beschlusses des EZB-Rates werden alle eingegangenen Anträge spätestens innerhalb von vierzehn Wochen nach Auftreten der technischen Störung beurteilt.

d) Die Bank teilt den jeweiligen Teilnehmern das Ergebnis der in Buchstabe c genannten 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 dessen Übermittlung entweder durch Unterzeichnung eines Standard-Annahmeschreibens, dessen jeweils aktuelle Fassung auf der Website der Bank abrufbar ist (siehe www.bundesbank.de), annehmen oder ablehnen. Geht der Bank innerhalb von vier Wochen kein Annahmeschreiben zu, so gilt dies als Ablehnung des Ausgleichsangebots durch die betreffenden Teilnehmer.

e) Die Bank leistet die Ausgleichszahlungen nach Erhalt des Annahmeschreibens des Teilnehmers. Auf Ausgleichszahlungen werden keine Zinsen erstattet.

MUSTER FÜR RECHTSFÄHIGKEITSGUTACHTEN (*CAPACITY OPINION*) UND LÄNDERGUTACHTEN (*COUNTRY OPINION*)

Muster für Rechtsgutachten über die rechtliche Befähigung zur TARGET2-Teilnahme

An die
Deutsche Bundesbank
Wilhelm-Epstein-Straße 14
60431 Frankfurt am Main
Deutschland

Teilnahme an TARGET2-BBk

[Ort], [Datum]

Sehr geehrte Damen und Herren,

als [interne oder externe] Rechtsberater von [genaue Bezeichnung des Teilnehmers oder der Zweigstelle des Teilnehmers] (nachfolgend der „Teilnehmer“) wurden wir beauftragt, dieses Rechtsgutachten im Hinblick auf die gemäß [Adjektiv, das den Staat bezeichnet, in dem der Teilnehmer seinen Sitz hat (nachfolgend „Adjektiv, das den Staat bezeichnet“)] Recht im Zusammenhang mit der Teilnahme des Teilnehmers an TARGET2-BBk (nachfolgend das „System“) auftretenden Fragen zu erstellen.

Dieses Gutachten beschränkt sich auf das zu diesem Zeitpunkt geltende [Adjektiv, das den Staat bezeichnet] Recht. Wir haben als Grundlage für dieses Rechtsgutachten keine anderen Rechtsordnungen untersucht und geben keine implizite oder ausdrückliche Stellungnahme dazu ab. Alle im Folgenden angeführten Aussagen und Stellungnahmen sind nach [Adjektiv, das den Staat bezeichnet] Recht gleichermaßen richtig und gültig, unabhängig davon, ob die Einreichung oder der Empfang von Zahlungsaufträgen über den Firmensitz des Teilnehmers oder über eine oder mehrere innerhalb oder außerhalb von [Staat, in dem der Teilnehmer seinen Sitz hat (nachfolgend der „Staat“)] belegene Zweigstelle(n) erfolgt.

I. GEPRÜFTE UNTERLAGEN

Für den Zweck dieses Gutachtens haben wir folgende Unterlagen geprüft:

(1) eine beglaubigte Abschrift der [Angabe der entsprechenden Gründungsurkunde(n)] des Teilnehmers, die zum gegenwärtigen Zeitpunkt gültig ist/sind;

(2) [falls zutreffend] ein Auszug aus [genaue Bezeichnung des relevanten Gesellschaftsregisters] und [falls zutreffend] aus [Verzeichnis der Kreditinstitute oder entsprechendes Register];

(3) [falls zutreffend] eine Abschrift der Lizenz des Teilnehmers oder eines anderen Nachweises der Zulassung zur Erbringung von Bank-, Wertpapier-, Überweisungs- oder sonstigen Finanzdienstleistungen in [Staat];

(4) [falls zutreffend] eine Kopie des vom Vorstand (Geschäftsführungsorgan) des Teilnehmers gefassten Beschlusses vom [Datum einfügen], aus dem die Zustimmung des Teilnehmers zur Anerkennung der nachstehend genannten Systembedingungen hervorgeht;

(5) [Angabe aller Vollmachten und anderer Unterlagen, aus denen die erforderlichen Befugnisse der Person(en), welche im Namen des Teilnehmers die (nachstehend genannten) Systembedingungen anerkennen, hervorgehen]

sowie weitere Unterlagen zur Gründung sowie zu den Befugnissen und Genehmigungen des Teilnehmers, die für die Erstellung dieses Gutachtens erforderlich oder zweckdienlich sind (nachfolgend die „Unterlagen des Teilnehmers").

Für den Zweck dieses Rechtsgutachtens haben wir ferner folgende Unterlagen geprüft:

(1) Die „Besonderen Geschäftsbedingungen für die Eröffnung und Führung eines PM-Kontos in TARGET2-Bundesbank (TARGET2-BBk) im Rahmen des internetbasierten Zugangs" vom [Datum einfügen] (nachfolgend die „Bedingungen") und

(2) […].

Die [Bedingungen] und […] werden im Folgenden als die „Systembedingungen" und zusammen mit den Unterlagen des Teilnehmers als die „Unterlagen" bezeichnet.

II. RECHTLICHE ANNAHMEN

Für den Zweck dieses Rechtsgutachtens sind wir in Bezug auf die Unterlagen von folgenden Annahmen ausgegangen:

(1) Bei den uns vorgelegten Systembedingungen handelt es sich um Originale oder Kopien, die mit dem Original übereinstimmen.

(2) Die Systembedingungen sowie die dadurch begründeten Rechte und Pflichten sind nach deutschem Recht, dem sie nach eigener Aussage unterliegen, gültig und rechtsverbindlich. Die Wahl deutschen Rechts, dem die Systembedingungen unterliegen sollen, wird vom deutschen Recht anerkannt.

(3) Die Unterlagen des Teilnehmers zur Teilnahme am System entsprechen den satzungsmäßigen Befugnissen der betreffenden Vertragsparteien und sind von diesen in gültiger Weise genehmigt, beschlossen oder ausgefertigt und erforderlichenfalls zugestellt worden.

(4) Die Unterlagen des Teilnehmers sind für die Vertragsparteien rechtsverbindlich, und es liegt kein Verstoß gegen eine der darin festgelegten Bestimmungen vor.

III. STELLUNGNAHMEN BEZÜGLICH DES TEILNEHMERS

A. Der Teilnehmer ist eine nach [Adjektiv, das den Staat bezeichnet] Recht ordnungsgemäß gegründete und eingetragene oder auf andere Weise ordnungsgemäß eingetragene oder organisierte Gesellschaft.

B. Der Teilnehmer verfügt über die erforderlichen gesellschaftsrechtlichen Befugnisse zur Erfüllung der Rechte und Pflichten im Rahmen der Systembedingungen.

C. Die Teilnahmeerklärung sowie die Erfüllung von Rechten und Pflichten des Teilnehmers im Rahmen der Systembedingungen führen zu keinem Verstoß gegen [Adjektiv, das den Staat bezeichnet] Recht, das auf den Teilnehmer oder die Unterlagen des Teilnehmers anwendbar ist.

D. Der Teilnehmer benötigt zum Zwecke der Wirksamkeit seiner Teilnahmeerklärung und der Wahrnehmung der Rechte und Pflichten im Rahmen der Systembedingungen keine zusätzlichen Ermächtigungen, Genehmigungen, Zustimmungen, Eintragungen, Zulassungen, notariellen Beglaubigungen oder sonstigen Bescheinigungen eines Gerichts oder einer Regierungs-, Justiz- oder sonstigen öffentlichen in [Staat] zuständigen Behörde.

E. Der Teilnehmer hat alle notwendigen gesellschaftsrechtlichen Handlungen und sonstigen Schritte unternommen, die gemäß [Adjektiv, das den Staat bezeichnet] Recht erforderlich sind, um sicherzustellen, dass seine Pflichten gemäß den Systembedingungen rechtmäßig, gültig und rechtsverbindlich sind.

Dieses Rechtsgutachten gilt mit dem angegebenen Datum und richtet sich, zum gegebenen Zeitpunkt, ausschließlich an die Deutsche Bundesbank und den [Teilnehmer]. Keine anderen Personen können sich auf dieses Gutachten berufen, noch darf der Inhalt dieses Gutachtens ohne unsere vorherige schriftliche Zustimmung anderen Personen als den vorgesehenen Empfängern und deren Rechtsberatern zugänglich gemacht werden, mit Ausnahme der Europäischen Zentralbank und der nationalen Zentralbanken des Europäischen Systems der Zentralbanken [sowie der [nationalen Zentralbank/zuständigen Aufsichtsbehörde] von [Staat]].

Mit freundlichen Grüßen

[Unterschrift]

Muster für Ländergutachten (*country opinion*) für TARGET2-Teilnehmerländer, die nicht dem EWR angehören

An die
Deutsche Bundesbank
Wilhelm-Epstein-Straße 14
60431 Frankfurt am Main
Deutschland

TARGET2-BBk

[Ort], [Datum]

Sehr geehrte Damen und Herren,

als [externe] Rechtsberater von [genaue Bezeichnung des Teilnehmers oder der Zweigstelle des Teilnehmers] (nachfolgend der „Teilnehmer“) wurden wir beauftragt, dieses Rechtsgutachten im Hinblick auf die gemäß [Adjektiv, das den Staat, bezeichnet, in dem der Teilnehmer seinen Sitz hat (nachfolgend „Adjektiv, das den Staat, bezeichnet“)] im Zusammenhang mit der Teilnahme des Teilnehmers an einem System, bei dem es sich um ein TARGET2-Komponenten-System (nachfolgend das „System“) handelt, auftretenden Fragen zu erstellen. Verweise auf die [Adjektiv, das den Staat bezeichnet] Rechtsordnung umfassen alle anwendbaren Bestimmungen der [Adjektiv, das den Staat bezeichnet] Rechtsordnung. Unser Gutachten erfolgt gemäß [Adjektiv, das den Staat bezeichnet] Recht unter besonderer Berücksichtigung des Teilnehmers mit Sitz außerhalb der Bundesrepublik Deutschland bezüglich der durch die Teilnahme am System entstehenden Rechte und Pflichten, die in den nachstehend genannten Systembedingungen dargelegt sind.

Dieses Gutachten beschränkt sich auf das zu diesem Zeitpunkt geltende [Adjektiv, das den Staat bezeichnet] Recht. Wir haben als Grundlage für dieses Rechtsgutachten keine anderen Rechtsordnungen untersucht und geben keine implizite oder ausdrückliche Stellungnahme dazu ab. Wir sind davon ausgegangen, dass keine andere Rechtsordnung Auswirkungen auf dieses Gutachten hat.

1. GEPRÜFTE UNTERLAGEN

Für den Zweck dieses Rechtsgutachtens haben wir die nachstehend aufgeführten Unterlagen und sonstige für erforderlich und zweckdienlich erachtete Dokumente geprüft:

(1) die „Besonderen Geschäftsbedingungen für die Eröffnung und Führung eines PM-Kontos in TARGET2-Bundesbank (TARGET2-BBk) im Rahmen des internetbasierten Zugangs“ vom [Datum einfügen] (nachfolgend die „Bedingungen“) und

(2) sonstige für das System und/oder das Verhältnis zwischen dem Teilnehmer und anderen Teilnehmern des Systems sowie zwischen den Teilnehmern des Systems und der Deutschen Bundesbank maßgebliche Dokumente.

Die Bedingungen und […] werden nachfolgend als die „Systembedingungen“ bezeichnet.

2. RECHTLICHE ANNAHMEN

Für den Zweck dieses Rechtsgutachtens sind wir in Bezug auf die Systembedingungen von folgenden Annahmen ausgegangen:

(1) Die Systembedingungen entsprechen den satzungsmäßigen Befugnissen der betreffenden Vertragsparteien und sind von diesen in gültiger Weise genehmigt, beschlossen und ausgefertigt sowie erforderlichenfalls zugestellt worden.

(2) Die Systembedingungen sowie die dadurch begründeten Rechte und Pflichten sind nach deutschem Recht, dem sie nach eigener Aussage unterliegen, gültig und rechtsverbindlich. Die Wahl deutschen Rechts, dem die Systembedingungen unterliegen sollen, wird von deutschem Recht anerkannt.

(3) Die Teilnehmer des Systems, über das Zahlungsaufträge versendet oder Zahlungen empfangen werden oder über das Rechte und Pflichten gemäß den Systembedingungen ausgeübt oder erfüllt werden, sind berechtigt, in allen einschlägigen Rechtsordnungen Überweisungsdienstleistungen zu erbringen.

(4) Die bei uns in Kopie oder als Muster eingegangenen Unterlagen entsprechen den Originalen.

3. RECHTSGUTACHTEN

Nach Maßgabe und vorbehaltlich des Obenstehenden sowie jeweils vorbehaltlich der unten aufgeführten Punkte erstellen wir folgendes Rechtsgutachten:

3.1 Länderspezifische rechtliche Aspekte [falls zutreffend]

Folgende Aspekte des [Adjektiv, das den Staat bezeichnet] Rechts stehen den aus den Systembedingungen für den Teilnehmer erwachsenden Verpflichtungen nicht entgegen: [Auflistung der länderspezifischen rechtlichen Aspekte].

3.2 Allgemeine Insolvenz- und Krisenmanagementaspekte

3.2.a Arten von Insolvenz- und Krisenmanagementverfahren

Die einzigen Arten von Insolvenzverfahren (einschließlich eines Vergleichs oder einer Sanierung) – welche für die Zwecke dieses Rechtsgutachtens alle Verfahren hinsichtlich der Vermögenswerte oder etwaiger Zweigstellen des Teilnehmers in [Staat] umfassen –, denen der Teilnehmer in [Staat] unterliegen könnte, sind die Folgenden: [Verfahren in Originalsprache und englischer Übersetzung auflisten] (zusammengefasst als ‚Insolvenzverfahren' bezeichnet).

Zusätzlich zu den Insolvenzverfahren können der Teilnehmer, seine Vermögenswerte oder Zweigstellen, die innerhalb von [Staat] ansässig sind, nach [Adjektiv, das den Staat bezeichnet] Recht folgenden Verfahren unterliegen: [Moratorien, Zwangsverwaltungen oder sonstige Verfahren, durch die Zahlungen vom und/oder an den Teilnehmer ausgesetzt oder beschränkt werden können, einschließlich Krisenpräventions- und Krisenmanagementmaßnahmen, die den in der Richtlinie 2014/59/EU definierten Maßnahmen entsprechen – bitte in Originalsprache und

englischer Übersetzung aufzählen] (zusammengefasst als ‚sonstige Verfahren' bezeichnet).

3.2.b Insolvenzabkommen

Die [Adjektiv, das den Staat bezeichnet] Rechtsordnung oder bestimmte Gebietskörperschaften innerhalb dieser Rechtsordnung ist/sind Vertragspartei der folgenden Insolvenzabkommen: [falls zutreffend, jene angeben, die Auswirkungen auf dieses Rechtsgutachten haben oder haben könnten].

3.3 Rechtswirksamkeit der Systembedingungen

Vorbehaltlich der nachstehend aufgeführten Punkte sind alle Bestimmungen der Systembedingungen gemäß [Adjektiv, das den Staat bezeichnet] Recht insbesondere im Fall der Eröffnung eines Insolvenzverfahrens oder eines sonstigen Verfahrens gegen den Teilnehmer verbindlich und durchsetzbar.

Wir stellen insbesondere Folgendes fest:

3.3.a Bearbeitung von Zahlungsaufträgen

Die Bestimmungen zur Bearbeitung von Zahlungsaufträgen [Auflistung der relevanten Bedingungen] sind rechtsgültig und durchsetzbar. Alle Zahlungsaufträge, die gemäß diesen Bedingungen bearbeitet werden, sind gemäß [Adjektiv, das den Staat bezeichnet] Recht rechtsgültig, rechtsverbindlich und durchsetzbar. Die Klausel, die den genauen Zeitpunkt festlegt, ab dem vom Teilnehmer beim System eingereichte Zahlungsaufträge rechtswirksam und unwiderruflich werden (Artikel 21 der Bedingungen), ist nach [Adjektiv, das den Staat bezeichnet] Recht ebenfalls rechtsgültig, rechtsverbindlich und durchsetzbar.

3.3.b Befugnis der Deutschen Bundesbank zur Erfüllung ihrer Aufgaben

Die Eröffnung eines Insolvenzverfahrens oder eines sonstigen Verfahrens hinsichtlich des Teilnehmers hat keine Auswirkungen auf die sich aus den Systembedingungen ergebenden Befugnisse der Deutschen Bundesbank. [[Falls zutreffend] genau angeben, dass dieses Rechtsgutachten auch für andere Rechtssubjekte gilt, die den Teilnehmern zur Teilnahme am System unmittelbar erforderliche Dienstleistungen erbringen (z. B. der Netzwerkdienstleister)].

3.3.c Rechtsschutz bei Ausfallereignissen

[Soweit sie auf den Teilnehmer anwendbar sind, sind die Vorschriften in Artikel 31 der Bedingungen über die sofortige Fälligkeit von noch nicht fälligen Forderungen, die Aufrechnung mit Forderungen aus Einlagen des Teilnehmers, die Realisierung eines Pfandrechts, die Suspendierung und Beendigung der Teilnahme, Verzugszinsen sowie über die Beendigung/Kündigung von Vereinbarungen und Transaktionen (Artikel 28-32 der Bedingungen) gemäß [Adjektiv, das den Staat bezeichnet] Recht rechtsgültig und durchsetzbar.]

3.3.d Suspendierung und Beendigung/Kündigung

Soweit sie auf den Teilnehmer anwendbar sind, sind Artikel 28 und 29 der Bedingungen (über die Suspendierung und Beendigung/Kündigung der Teilnahme des Teilnehmers am System bei Eröffnung eines Insolvenzverfahrens oder sonstigen Verfahrens oder in sonstigen Fällen der Nichterfüllung im Sinne der Systembedingungen oder wenn der Teilnehmer ein systemisches Risiko jedweder Art darstellt oder schwerwiegende technische Probleme hat) gemäß [Adjektiv, das den Staat bezeichnet] Recht rechtsgültig und durchsetzbar.

3.3.e Abtretung von Rechten und Pflichten

Die Rechte und Pflichten des Teilnehmers sind ohne vorherige schriftliche Zustimmung der Deutschen Bundesbank nicht abtretbar, veränderbar oder anderweitig vom Teilnehmer auf Dritte übertragbar.

3.3.g Anwendbares Recht und Gerichtsbarkeit

Die Bestimmungen in Artikel 35 und 38 der Bedingungen, insbesondere bezüglich des geltenden Rechts, der Beilegung von Rechtsstreitigkeiten, der zuständigen Gerichte und gerichtlicher Zustellungen, sind gemäß [Adjektiv, das den Staat bezeichnet] Recht rechtsgültig und durchsetzbar.

3.4 Insolvenzanfechtung

Wir stellen fest, dass weder die aus den Systembedingungen erwachsenden Verpflichtungen, noch ihre Ausübung oder Erfüllung vor der Eröffnung eines Insolvenzverfahrens oder sonstigen Verfahrens gegen den Teilnehmer eine Insolvenzanfechtung oder automatische Nichtigkeit oder sonst vergleichbare Rechtsfolge gemäß [Adjektiv, das den Staat bezeichnet] Recht nach sich ziehen können.

Wir bestätigen dies insbesondere im Hinblick auf alle von den Teilnehmern des Systems eingereichten Zahlungsaufträge. Wir bestätigen insbesondere, dass die Regelungen in Artikel 21 der Bedingungen zur Rechtswirksamkeit und Unwiderruflichkeit von Zahlungsaufträgen rechtsgültig und rechtswirksam sind und dass ein von einem Teilnehmer eingereichter Zahlungsauftrag, der gemäß Titel IV der Bedingungen bearbeitet wird, gemäß [Adjektiv, das den Staat bezeichnet] Recht keine Insolvenzanfechtung, automatische Nichtigkeit oder sonst vergleichbare Rechtsfolge nach sich ziehen kann.

3.5 Pfändung

Wenn ein Gläubiger des Teilnehmers einen Pfändungsbeschluss (einschließlich Arrestbeschlüssen, Beschlagnahmeanordnungen oder anderen privatrechtlichen oder öffentlich-rechtlichen Maßnahmen im öffentlichen Interesse oder zum Schutz der Rechte der Gläubiger des Teilnehmers) eines zuständigen Gerichts oder einer zuständigen Regierungs-, Justiz- oder sonstigen öffentlichen Behörde in [Staat] gemäß [Adjektiv, das den Staat bezeichnet] Recht beantragt (nachfolgend als „Pfändung“ bezeichnet), stellen wir fest, dass [Analyse und Erörterung einfügen].

3.6 Sicherheiten (falls zutreffend)

3.6.a Übertragung von Rechten oder hinterlegten Vermögenswerten zur Besicherung, als Pfand, Pensionsgeschäft und/oder Garantie

Die Übertragung zum Zwecke der Besicherung ist gemäß den Rechtsvorschriften von [Staat] rechtsgültig und durchsetzbar. Ferner ist die Begründung und Realisierung eines Pfandrechts oder Pensionsgeschäfts entsprechend den „Besonderen Geschäftsbedingungen für die Eröffnung und Führung eines PM-Kontos in TARGET2-Bundesbank (TARGET2-BBk) im Rahmen des internetbasierten Zugangs“ gemäß [Adjektiv, das den Staat bezeichnet] Recht rechtsgültig.

3.6.b Vorrang der Interessen der Rechtsnachfolger/Zessionare, Pfandgläubiger oder Pensionsnehmer vor jenen anderer Anspruchsberechtigter

Bei einem Insolvenzverfahren oder sonstigen Verfahren gegen den Teilnehmer hat die Zentralbank als Sicherheitsnehmerin der zum Zwecke der Besicherung übertragenen oder verpfändeten Rechte oder Vermögenswerte Vorrang vor den Ansprüchen aller anderen Gläubiger des Teilnehmers. Die Sicherheiten unterliegen keinem Vorrang oder Zugriff (anderer) bevorrechtigter Gläubiger.

3.6.c Verwertung der Sicherheiten

Auch im Falle eines Insolvenzverfahrens oder sonstigen Verfahrens gegen den Teilnehmer steht es anderen Systemteilnehmern und der Deutschen Bundesbank als Pfandgläubiger immer noch frei, die Sicherheiten des Teilnehmers selbst zu verwerten.

3.6.d Form- und Registrierungsvorschriften

Es bestehen keine Formvorschriften für die Übertragung von Rechten und Vermögenswerten des Teilnehmers zu Besicherungszwecken oder für die Begründung und Vollstreckung eines Pfandrechts oder Pensionsgeschäfts im Hinblick auf diese Rechte und Vermögenswerte. Ferner ist es nicht erforderlich, dass [die Übertragung zum Zweck der Besicherung, das Pfand oder Pensionsgeschäft] oder die Daten einer/s solchen [Übertragung, Pfands oder Pensionsgeschäfts] bei einem zuständigen Gericht oder einer zuständigen Regierungs-, Justiz- oder sonstigen öffentlichen Behörde in [Staat] registriert oder beantragt wird.

3.7 Zweigstellen [falls zutreffend]

3.7.a Anwendbarkeit des Gutachtens auf Handeln über Zweigstellen

Alle der oben angeführten Aussagen und Stellungnahmen im Hinblick auf den Teilnehmer sind gemäß [Adjektiv, das den Staat bezeichnet] Recht gleichermaßen richtig und gültig, wenn der Teilnehmer über eine oder mehrere außerhalb von [Staat] belegene Zweigstelle(n) agiert.

3.7.b Einhaltung der Gesetze

Die Wahrnehmung der Rechte und Pflichten im Rahmen der Systembedingungen und die Einreichung, Übermittlung oder der Empfang von Zahlungsaufträgen durch eine Zweigstelle des Teilnehmers führen in keiner Weise zu einem Verstoß gegen [Adjektiv, das den Staat bezeichnet] Recht.

3.7.c Erforderliche Befugnisse

Weder die Wahrnehmung der Rechte und Pflichten im Rahmen der Systembedingungen noch die Einreichung, Übermittlung oder der Empfang von Zahlungsaufträgen durch eine Zweigstelle des Teilnehmers erfordern Ermächtigungen, Genehmigungen, Zustimmungen, Eintragungen, Zulassungen, notarielle Beglaubigungen oder sonstige Bescheinigungen eines Gerichts oder einer Regierungs-, Justiz- oder sonstigen öffentlichen in [Staat] zuständigen Behörde.

Dieses Rechtsgutachten gilt mit dem angegebenen Datum und richtet sich, zum gegebenen Zeitpunkt, ausschließlich an die Deutsche Bundesbank und den [Teilnehmer]. Weder können sich andere Personen auf dieses Gutachten berufen, noch darf der Inhalt dieses Gutachtens ohne unsere vorherige schriftliche Zustimmung anderen Personen als den vorgesehenen Empfängern und deren Rechtsberatern zugänglich gemacht werden. Ausgenommen hiervon sind die Europäische Zentralbank und die nationalen Zentralbanken des Europäischen Systems der Zentralbanken [sowie [die nationale Zentralbank/zuständige Aufsichtsbehörde] von [Staat]].

Mit freundlichen Grüßen

[Unterschrift]

AUFRECHTERHALTUNG DES GESCHÄFTSBETRIEBS (*BUSINESS CONTINUITY*) UND NOTFALLVERFAHREN

1. Allgemeine Bestimmungen

a) Die in dieser Anlage enthaltenen Regelungen zwischen der Bank und den Teilnehmern oder Nebensystemen gelten für den Fall, dass eine oder mehrere Komponenten der SSP oder des Telekommunikationsnetzes ausfallen oder von außergewöhnlichen externen Ereignissen betroffen sind oder der Ausfall einen Teilnehmer oder ein Nebensystem betrifft.

b) Alle in dieser Anlage enthaltenen Verweise auf bestimmte Zeiten beziehen sich auf die die Ortszeit am Sitz der EZB, d.h. Mitteleuropäische Zeit (MEZ)[12].

2. Business-Continuity- und Notfallmaßnahmen

a) Wenn ein außergewöhnliches externes Ereignis eintritt und/oder es zu einem Ausfall der Gemeinschaftsplattform oder des Telekommunikationsnetzes kommt und dies Auswirkungen auf den normalen Betrieb von TARGET2 hat, ist die Bank berechtigt, Business-Continuity- und Notfallmaßnahmen einzuleiten.

b) In TARGET2 stehen im Wesentlichen folgende Business-Continuity- und Notfallmaßnahmen zur Verfügung:

   i) Verlagerung des Betriebs der SSP auf einen anderen Standort

   ii) Änderung der Betriebszeiten der SSP und

   iii) Einleitung der Notfallabwicklung sehr kritischer und kritischer Zahlungen gemäß Abschnitt 6 Buchstaben c und d.

c) Es steht im alleinigen Ermessen der Bank, ob und welche Business-Continuity- und Notfallmaßnahmen zur Abwicklung von Zahlungsaufträgen sie einleitet.

3. Nachrichtenübermittlung bei Störungen

a) Informationen über einen Ausfall der Gemeinschaftsplattform und/oder ein außergewöhnliches externes Ereignis werden den Teilnehmern über die nationalen Kommunikationskanäle, das ICM und das T2IS übermittelt. Nachrichten an die Teilnehmer enthalten insbesondere folgende Informationen:

   i) eine Beschreibung des Ereignisses

   ii) die erwartete Abwicklungsverzögerung (falls bekannt)

   iii) Informationen über die bereits getroffenen Maßnahmen und

   iv) Hinweise an die Teilnehmer.

[12] Der Begriff „MEZ“ berücksichtigt die Umstellung zur Mitteleuropäischen Sommerzeit.

b) Darüber hinaus kann die Bank die Teilnehmer über etwaige andere gegenwärtige oder erwartete Ereignisse, die potenziell Auswirkungen auf den normalen Betrieb von TARGET2 haben könnten, in Kenntnis setzen.

4. Verlagerung des Betriebs der Gemeinschaftsplattform auf einen anderen Standort

a) Wenn eines der in Abschnitt 2 Buchstabe a beschriebenen Ereignisse eintritt, kann der Betrieb der SSP auf einen anderen Standort in derselben oder einer anderen Region verlagert werden.

b) Wenn der Betrieb der SSP von einer Region (Region 1) in eine andere Region (Region 2) verlagert wird, werden sich die Teilnehmer bemühen, ihre Positionen bis zum Zeitpunkt des Ausfalls oder des Eintretens der außergewöhnlichen externen Ereignisse abzustimmen, und der Bank alle in diesem Zusammenhang relevanten Informationen zur Verfügung stellen.

5. Änderung der Betriebszeiten

a) Die Tagesbetrieb-Phase von TARGET2 kann verlängert bzw. der Zeitpunkt des Beginns eines neuen Geschäftstages verschoben werden. Bei verlängerten TARGET2-Betriebszeiten werden Zahlungsaufträge im Einklang mit den „Besonderen Geschäftsbedingungen für die Eröffnung und Führung eines PM-Kontos in TARGET2-Bundesbank (TARGET2-BBk) im Rahmen des internetbasierten Zugangs“, vorbehaltlich der in dieser Anlage enthaltenen Änderungen, bearbeitet.

b) Wenn ein Ausfall der SSP während des Tages eingetreten ist, aber vor 18.00 Uhr behoben wurde, *kann* die Tagesbetrieb-Phase und damit die Annahmeschlusszeit verlängert werden. Eine solche Verlängerung der Annahmeschlusszeit geht in der Regel nicht über zwei Stunden hinaus und wird den Teilnehmern so früh wie möglich bekannt gegeben. Wenn eine solche Verlängerung vor 16.50 Uhr bekannt gegeben wird, bleibt es bei der Mindestfrist von einer Stunde zwischen der Annahmeschlusszeit für Kunden- und derjenigen für Interbankzahlungen. Bekannt gegebene Verlängerungen werden nicht wieder rückgängig gemacht.

c) Die Annahmeschlusszeit wird verlängert, wenn ein Ausfall der SSP vor 18.00 Uhr eintritt und bis 18.00 Uhr nicht behoben wurde. Die Bank teilt den Teilnehmern die Verlängerung der Annahmeschlusszeit unverzüglich mit.

d) Nach Wiederaufnahme des Betriebs der SSP werden folgende Schritte unternommen:

   i) Die Bank bemüht sich, alle sich in der Warteschlange befindlichen Zahlungen innerhalb einer Stunde abzuwickeln; dieser Zeitraum verringert sich auf 30 Minuten, wenn sich der Ausfall der SSP um 17.30 Uhr oder später ereignet (sofern der Ausfall um 18.00 Uhr noch andauert).

   ii) Die Schlussstände/Tagesendsalden der Konten der Teilnehmer werden innerhalb einer Stunde ermittelt; dieser Zeitraum verringert sich auf 30 Minuten, wenn sich der Ausfall der SSP um 17.30 Uhr oder später ereignet (sofern der Ausfall um 18.00 Uhr noch andauert).

   iii) Nach Annahmeschluss für Interbankzahlungen findet auch das Tagesabschlussverfahren statt, einschließlich der Inanspruchnahme der ständigen Fazilitäten des Eurosystems.

e) Nebensysteme, die am frühen Morgen Liquidität benötigen, müssen Maßnahmen vorsehen, um einem verspäteten Beginn der Tagesbetrieb-Phase aufgrund eines Ausfalls der SSP am vorhergehenden Tag Rechnung zu tragen.

6. Notfallabwicklung

a) Wenn die Bank es für notwendig erachtet, kann sie das Notfallabwicklungs-Verfahren für Zahlungsaufträge unter Verwendung der Notfalllösung der SSP einleiten. In solchen Fällen wird den Teilnehmern und den Nebensystemen nur ein Mindestmaß an Service geboten. Die Bank informiert ihre Teilnehmer und Nebensysteme mittels eines der zur Verfügung stehenden Kommunikationsmittel über den Start der Notfallabwicklung.

b) Während der Notfallabwicklung werden Zahlungsaufträge von den Teilnehmern, die nicht den internetbasierten Zugang nutzen, eingereicht und von der Bank genehmigt. Darüber hinaus können die Nebensysteme Dateien einreichen, die Zahlungsanweisungen enthalten, welche von der Bank in die Notfalllösung hochgeladen werden können.

c) Folgende Zahlungen gelten als „sehr kritisch“ und die Bank wird sich nach Kräften bemühen, diese in Notfallsituationen abzuwickeln:

   i) Zahlungen in Verbindung mit der CLS Bank International, mit Ausnahme von Zahlungen in Verbindung mit dem CCP-Dienst der CLS und dem CLSNow-Dienst,

   ii) EURO1-Zahlungsausgleich zum Tagesabschluss,

   iii) Margenausgleich für zentrale Kontrahenten.

d) Zahlungen, die zur Vermeidung von Systemrisiken notwendig sind, gelten als ‚kritisch‘, und die Bank kann für ihre Abwicklung die Notfallabwicklung einleiten.

e) Die Teilnehmer, die nicht den internetbasierten Zugang nutzen, reichen Zahlungsaufträge zur Abwicklung in Notfallsituationen direkt in die Notfalllösung ein; die Übermittlung von Informationen an die Zahlungsempfänger erfolgt über die Notfalllösung. Nebensysteme reichen Dateien mit Zahlungsanweisungen bei der Bank zum Hochladen in die Notfalllösung ein und ermächtigen die Bank, dies zu tun. Die Bank kann Zahlungen in Ausnahmefällen auch manuell im Namen der Teilnehmer, die nicht den internetbasierten Zugang nutzen, eingeben. Informationen über Kontostände sowie Belastungen und Gutschriften können über die Bank eingeholt werden. f) Zahlungsaufträge, die bereits in TARGET2-BBk eingereicht wurden, sich aber noch in der Warteschlange befinden, können ebenfalls in die Notfallabwicklung einbezogen werden. In solchen Fällen ist die Bank bestrebt, die doppelte Ausführung solcher Zahlungsaufträge zu verhindern. Das Risiko einer möglichen Doppelausführung tragen jedoch die Teilnehmer.

g) Für die Abwicklung von Zahlungsaufträgen in der Notfallabwicklung stellen die Teilnehmer notenbankfähige Sicherheiten als Sicherheit bereit. Während der Notfallabwicklung können eingehende Notfallzahlungen zur Finanzierung von ausgehenden Notfallzahlungen verwendet

werden. Die Bank wird die verfügbare Liquidität der Teilnehmer für die Zahlungsabwicklung im Rahmen der Notfallabwicklung nicht berücksichtigen.

7. Ausfälle von Teilnehmern oder Nebensystemen

a) Wenn bei einem Teilnehmer ein Problem auftritt, aufgrund dessen er keine Zahlungen in TARGET2 abwickeln kann, obliegt es ihm, das Problem zu beheben. Der Teilnehmer kann insbesondere auf interne Lösungen oder die ICM-Funktionalität, d. h. auf Ersatzzahlungen zur Liquiditätsumverteilung und Notfallzahlungen (z. B. CLS, EURO1), zurückgreifen.

b) Wenn die in Buchstabe a genannten Maßnahmen erschöpft oder unwirksam sind, kann der Teilnehmer die Bank um Unterstützung bitten.

c) Wenn ein Nebensystem von einem Ausfall betroffen ist, obliegt es diesem System, den Ausfall zu beheben. Auf Wunsch des Nebensystems kann die Bank in dessen Auftrag handeln. Die Bank entscheidet nach eigenem Ermessen über die Unterstützung für das Nebensystem, einschließlich der Unterstützung während des Nachtbetriebs des Nebensystems. Folgende Notfallmaßnahmen können eingeleitet werden:

   i) Das Nebensystem veranlasst reine („clean“) Zahlungen (d. h. Zahlungen, die nicht mit der zugrunde liegenden Transaktion verbunden sind) über die Teilnehmer-Schnittstelle (PI);

   ii) die Bank erstellt und/oder verarbeitet im Auftrag des Nebensystems XML-Anweisungen/-Dateien; und/oder

   iii) die Bank leistet im Auftrag des Nebensystems reine Zahlungen.

d) Konkrete Regelungen zu Notfallmaßnahmen im Hinblick auf Nebensysteme sind in den bilateralen Vereinbarungen zwischen der Bank und dem entsprechenden Nebensystem enthalten.

8. Sonstige Bestimmungen

a) Für den Fall, dass bestimmte Daten nicht verfügbar sind, weil eines der in Abschnitt 3 Buchstabe a genannten Ereignisse eingetreten ist, ist die Bank berechtigt, mit der Bearbeitung von Zahlungsaufträgen zu beginnen oder fortzufahren und/oder TARGET2-BBk auf Basis der letzten verfügbaren, von der Bank ermittelten Daten zu betreiben. Auf Anforderung der Bank übermitteln die Teilnehmer und Nebensysteme ihre FileAct/Interact-Nachrichten erneut oder treffen sonstige von der Bank für geeignet erachtete Maßnahmen.

b) Bei einem Ausfall der Bank können deren Aufgaben in Bezug auf TARGET2-BBk ganz oder teilweise von anderen Eurosystem-Zentralbanken oder von dem Operational Team der SSP wahrgenommen werden.

c) Die Bank kann verlangen, dass die Teilnehmer an regelmäßigen oder ad-hoc-Tests der Business-Continuity- und Notfallmaßnahmen, Schulungen oder sonstigen Präventivmaßnahmen, die sie für notwendig erachtet, teilnehmen. Alle den Teilnehmern durch diese Tests oder sonstige Maßnahmen entstehenden Kosten werden ausschließlich von den Teilnehmern selbst getragen.

ÖFFNUNGSZEITEN UND TAGESABLAUF

1. TARGET2 ist täglich außer samstags, sonntags, an Neujahr, am Karfreitag und Ostermontag (nach dem am Sitz der EZB gültigen Kalender), am 1. Mai sowie am 25. und 26. Dezember geöffnet.
2. Die maßgebliche Zeit für das System ist die Ortszeit am Sitz der EZB, d.h. die MEZ.
3. Der laufende Geschäftstag wird am Abend des vorhergehenden Geschäftstages eröffnet und hat folgenden Ablauf:

Zeit	Beschreibung
06.45 Uhr - 07.00 Uhr	Geschäftsbetrieb-Fenster zur Vorbereitung des Tagesgeschäfts*
07.00 Uhr - 18.00 Uhr	Tagverarbeitung
17.00 Uhr	Annahmeschluss für Kundenzahlungen (d. h. Zahlungen, die im System an der Verwendung des Nachrichtenformats MT 103 oder MT 103+ zu erkennen sind, bei denen der Auftraggeber und/oder Begünstigte einer Zahlung kein direkter oder indirekter Teilnehmer ist)
18.00 Uhr	Annahmeschluss für Interbankzahlungen (d. h. Zahlungen, die keine Kundenzahlungen sind)
18.00 Uhr – 18.45 Uhr**	Tagesabschlussverfahren
18.15 Uhr**	Allgemeiner Annahmeschluss für die Inanspruchnahme der ständigen Fazilitäten
(Kurz nach) 18.30 Uhr***	Daten zur Aktualisierung der Bilanzierungssysteme stehen den Zentralbanken zur Verfügung
18.45 Uhr - 19.30 Uhr***	Tagesbeginn-Verarbeitung (neuer Geschäftstag)
19:00 Uhr *** – 19:30 Uhr**	Bereitstellung von Liquidität auf dem PM-Konto
19.30 Uhr***	Nachricht „Beginn des Verfahrens“ (start of procedure) und Abwicklung der Daueraufträge zur Liquiditätsübertragung von PM-Konten auf Unterkonten/Spiegelkonten (Nebensystem-Abwicklung)
19.30 Uhr*** - 22.00 Uhr	Ausführung weiterer Liquiditätsübertragungen über das ICM für Abwicklungsverfahren 6 (‚Echtzeit‘); Ausführung weiterer Liquiditätsübertragungen über das ICM, bevor das Nebensystem die Nachrichten ‚Beginn des Zyklus‘ (‚start of cycle‘) für Abwicklungsverfahren 6

	(‚Schnittstelle‘) sendet; Abwicklungszeitraum für den Nachtbetrieb der Nebensysteme (nur für das Nebensystem-Abwicklungsverfahren 6 (‚Echtzeit‘) und das Nebensystem-Abwicklungsverfahren 6 (‚Schnittstelle‘))
22.00 Uhr - 01.00 Uhr	Wartungszeitraum
01.00 Uhr - 07.00 Uhr	Abwicklungsverfahren für den Nachtbetrieb der Nebensysteme (nur für das Nebensystem-Abwicklungsverfahren 6 (‚Echtzeit‘) und das Nebensystem-Abwicklungsverfahren 6 (‚Schnittstelle‘))

* Tagesgeschäft: Tagverarbeitungs-Phase und Tagesabschlussverfahren.

** Endet am letzten Tag der Mindestreserve-Erfüllungsperiode 15 Minuten später.

*** Beginnt am letzten Tag der Mindestreserve-Erfüllungsperiode 15 Minuten später.

4. Das ICM steht von 19.30 Uhr*** bis 18.00 Uhr am folgenden Tag für Liquiditätsübertragungen zur Verfügung, mit Ausnahme des Wartungszeitraums von 22.00 Uhr bis 01.00 Uhr.

5. Die Öffnungszeiten können geändert werden, wenn Business-Continuity-Maßnahmen gemäß Abschnitt 5 der Anlage IV ergriffen werden.

6. Aktuelle Informationen über den Betriebsstatus der SSP stehen über das TARGET2-Informationssystem (T2IS) auf einer gesonderten Internetseite der EZB-Website zur Verfügung. Die Informationen über den Betriebsstatus der SSP auf T2IS und der Website der EZB werden nur während der üblichen Geschäftszeiten aktualisiert.

GEBÜHRENVERZEICHNIS UND RECHNUNGSSTELLUNG IM RAHMEN DES INTERNETBASIERTEN ZUGANGS

Gebühren für direkte Teilnehmer

1. Die monatliche Gebühr für die Verarbeitung von Zahlungsaufträgen in TARGET2-BBk beträgt für direkte Teilnehmer 70 EUR Internetzugangsgebühr je PM-Konto zuzüglich 150 EUR je PM-Konto zuzüglich einer Transaktionspauschale (je Belastungsbuchung) in Höhe von 0,80 EUR;
2. Direkten Teilnehmern, die eine Veröffentlichung ihres BIC im TARGET2-Directory ablehnen, wird eine zusätzliche monatliche Gebühr von 30 EUR je Konto berechnet.
3. Je Teilnehmer werden für jedes PM-Konto bis zu fünf aktive Zertifikate durch Bank kostenlos ausgestellt und unterhalten. Die Bank erhebt eine Gebühr von 120 EUR für die Ausstellung eines sechsten Zertifikats und für jedes nachfolgende aktive Zertifikat. Die Bank erhebt eine jährliche Unterhaltsgebühr von 30 EUR für das sechste Zertifikat und für jedes nachfolgende aktive Zertifikat. Aktive Zertifikate sind fünf Jahre lang gültig.

Rechnungsstellung

4. Für direkte Teilnehmer gelten die folgenden Regeln für die Rechnungsstellung: Der direkte Teilnehmer erhält die Rechnung für den Vormonat mit Angabe der zu entrichtenden Gebühren spätestens bis zum neunten Geschäftstag des Folgemonats. Die Zahlungen erfolgen spätestens bis zum vierzehnten Arbeitstag dieses Monats auf das von der Bank angegebene Konto oder werden einem vom Teilnehmer angegebenen Konto belastet..

ANFORDERUNGEN AN DAS INFORMATIONSSICHERHEITSMANAGEMENT UND DAS BUSINESS-CONTINUITY-MANAGEMENT

Informationssicherheitsmanagement

Diese Anforderungen gelten für jeden einzelnen Teilnehmer, es sei denn, ein Teilnehmer weist nach, dass eine bestimmte Anforderung auf ihn nicht anwendbar ist. Bei der Festlegung des Anwendungsbereichs der Anforderungen innerhalb seiner Infrastruktur sollte der Teilnehmer die Elemente identifizieren, die Teil der Zahlungstransaktionskette sind. Die Zahlungstransaktionskette beginnt am Point of Entry (PoE), d. h. einem System, das an der Erstellung von Transaktionen beteiligt ist (z. B. Workstations, Front- und Back-Office-Anwendungen, Middleware), und endet beim System, das für die Übermittlung der Nachricht an SWIFT verantwortlich ist (z. B. SWIFT VPN Box) oder beim Internet (Letzteres trifft bei internetbasiertem Zugang zu).

Anforderung 1.1: Informationssicherheitsstrategie

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, das Management von Informationssicherheit und Cyberresilienz innerhalb der gesamten Organisation in Bezug auf Identifikation, Bewertung und Behandlung von Risiken für die Informationssicherheit und die Cyberresilienz sicherzustellen. Die Strategie sollte mindestens folgende Abschnitte beinhalten: Ziele, Umfang (darunter Bereiche wie Organisation, Personal, Verwaltung der Informationswerte usw.), Grundsätze und Zuweisung von Verantwortlichkeiten.

Anforderung 1.2: Interne Organisation

Zur Umsetzung der Informationssicherheitsstrategie innerhalb der Organisation wird ein Informationssicherheitsrahmenwerk geschaffen. Die Geschäftsführung koordiniert und überprüft die Einrichtung des Informationssicherheitsrahmenwerks, damit die organisationsweite Umsetzung der Informationssicherheitsstrategie (gemäß der Anforderung 1.1), darunter auch die Zuteilung ausreichender Ressourcen und die Zuweisung entsprechender Sicherheitsverantwortlichkeiten, gewährleistet ist.

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 ihrer Informationen und informationsverarbeitenden Einrichtungen beeinträchtigen. Der Zugang externer Parteien zu den informationsverarbeitenden Einrichtungen der Organisation ist in jedem Fall zu kontrollieren. Sofern externe Parteien oder Produkte/Dienstleistungen externer Parteien Zugang zu informationsverarbeitenden Einrichtungen der Organisation benötigen, ist eine Risikoprüfung durchzuführen, um die sicherheitsrelevanten Auswirkungen zu ermitteln und die Kontrollanforderungen

zu bestimmen. Die Kontrollen werden mit der externen Partei jeweils einzeln vereinbart und vertraglich festgelegt.

Anforderung 1.4: Verwaltung von Informationswerten

Sämtliche Informationswerte, Geschäftsprozesse und zugrundeliegenden Informationssysteme entlang der Zahlungstransaktionskette, wie Betriebssysteme, Infrastrukturen, Fachsoftware, Standardprodukte, Dienste und von Nutzern entwickelte Anwendungen, 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. Hinweis: Der Eigentümer kann soweit angemessen die Durchführung bestimmter Kontrollen delegieren; er ist jedoch weiterhin für den ordnungsgemäßen Schutz der Informationswerte verantwortlich.

Anforderung 1.5: Klassifizierung von Informationswerten

Die Informationswerte werden nach ihrer Kritikalität für den reibungslosen Betrieb durch den Teilnehmer klassifiziert. Aus der Klassifizierung muss ersichtlich sein, ob, mit welcher Priorität und in welchem Umfang Informationswerte zu schützen sind, während sie in den jeweiligen Geschäftsprozessen und durch die zugrunde liegenden IT-Komponenten verwendet werden. Mithilfe eines von der Geschäftsführung genehmigten Systems zur Klassifizierung von Informationswerten werden für die gesamte Lebensdauer der Informationswerte (einschließlich Löschung und Vernichtung der Informationswerte) angemessene Schutzkontrollen definiert und es wird 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 vertraglichen Beschäftigungsbedingungen festgehalten. Alle Bewerber, Vertragspartner und Drittanwender sind hinreichend zu überprüfen, besonders bei sensiblen Stellen bzw. Aufträgen. Mitarbeiter, Vertragspartner und Dritte, die informationsverarbeitende Einrichtungen nutzen, unterzeichnen eine Vereinbarung, in der ihre Sicherheitsrollen und Verantwortlichkeiten festgelegt sind. Es wird gewährleistet, dass alle Mitarbeiter, Vertragspartner und Dritte hinreichend für Sicherheitsaspekte sensibilisiert sind. Zur Minimierung möglicher Sicherheitsrisiken sind ihnen Fortbildungen und Schulungen zu Sicherheitsverfahren und dem korrekten Einsatz der informationsverarbeitenden Einrichtungen zu ermöglichen. Für Mitarbeiter ist ein formelles Disziplinarverfahren zu schaffen, das bei Verletzung von Sicherheitsbestimmungen zur Anwendung kommt. Durch Zuweisung entsprechender Verantwortlichkeiten ist zu gewährleisten, dass das Ausscheiden eines Mitarbeiters, Vertragspartners oder Dritten bzw. dessen Wechsel innerhalb der Organisation gesteuert wird sowie sämtliche Betriebsmittel zurückgegeben und alle Zugangsberechtigungen entzogen werden.

Anforderung 1.7: Physische und umgebungsbezogene Sicherheit

Kritische oder sensible informationsverarbeitende Einrichtungen werden in Sicherheitsbereichen untergebracht, 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 werden Verfahren und Standards festgelegt, 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 und Verluste in Bezug auf Betriebsmittel oder Informationen zu verhindern, ist es erforderlich, dass sämtliche (auch außerhalb des Standorts verwendete) 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 besondere Maßnahmen erforderlich sein.

Anforderung 1.8: Betriebsmanagement

Für die Verwaltung und den Betrieb von informationsverarbeitenden Einrichtungen, die durchgängig alle zugrunde liegenden Systeme der Zahlungstransaktionskette abdecken, werden Verantwortlichkeiten und Verfahren festgelegt.
Was die Betriebsprozesse einschließlich der technischen Administration der IT-Systeme betrifft, so ist soweit angemessen 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 im Anschluss an eine formale Risikoanalyse kompensierende Kontrollen zu implementieren. Es werden Kontrollen eingerichtet, um das Eindringen von Schadsoftware (Malware) in die Systeme der Zahlungstransaktionskette zu verhindern und aufzudecken. Es werden zudem Kontrollen (einschließlich der Nutzersensibilisierung) eingeführt, 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.
Es müssen Konzepte zur Datensicherung und -wiederherstellung von der Geschäftsführung umgesetzt werden. Hierzu zählt auch ein Wiederherstellungsplan, der in regelmäßigen Abständen, jedoch mindestens jährlich, zu testen ist.
Zudem werden die für die Sicherheit des Zahlungsverkehrs kritischen Systeme überwacht und relevante Informationssicherheitsvorfälle dokumentiert. Durch den Einsatz von Betreiberprotokollen ist sicherzustellen, dass Probleme im Bereich der Informationssysteme erkannt werden. Die Betreiberprotokolle werden in regelmäßigen Abständen – je nach der Kritikalität des Betriebsprozesses – stichprobenartig überprüft. 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 und im Rahmen von zwischen den betroffenen Parteien abgeschlossenen Austauschvereinbarungen erfolgen. Hierbei sind die einschlägigen Rechtsvorschriften einzuhalten. Werden Software-Komponenten von Drittanbietern im Informationsaustausch mit TARGET2 verwendet (z. B. wenn, wie im zweiten Anforderungsszenario der TARGET2-Selbstzertifizierung beschrieben, Software von einem Servicebüro bezogen wird), so muss hierfür eine formale Vereinbarung mit dem Dritten abgeschlossen werden.

Anforderung 1.9: Zugangskontrolle

Der Zugang zu Informationswerten ist durch die fachlichen Anforderungen (‚Kenntnis nur soweit nötig'[13]) und im Einklang mit dem bestehenden Regelungsrahmen der Organisation (einschließlich der Informationssicherheitsstrategie) zu begründen. Es sind eindeutige Regeln für die Zugriffskontrolle auf Basis des Grundsatzes der minimalen Rechtevergabe[14] festzulegen, die den Erfordernissen des jeweiligen Geschäftszwecks und der IT-Prozesse genau Rechnung tragen. Soweit relevant (z. B. zur Backup-Verwaltung), müssen die logischen mit den physischen Zugriffskontrollen übereinstimmen, es sei denn, es bestehen angemessene 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 umgesetzt werden. Diese Verfahren müssen den gesamten Lebenszyklus des Nutzerzugangs abdecken – 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 ihr Missbrauch zu einer schwerwiegenden Beeinträchtigung der betrieblichen Prozesse des Teilnehmers führen kann (z. B. Zugriffsrechte im Zusammenhang mit der Systemadministration, dem Umgehen von Systemkontrollen oder dem direkten Zugriff auf Geschäftsdaten).
Es sind angemessene Kontrollen einzurichten, um die Nutzer an bestimmten Punkten des Netzwerks der Organisation, beispielsweise für den lokalen oder Fernzugang zu Systemen der Zahlungstransaktionskette, zu ermitteln, 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. für die Komplexität und zeitlich begrenzte Gültigkeit der Passwörter) festgelegt und durch spezielle Kontrollen durchgesetzt werden. Es ist ein Protokoll für die sichere Wiederherstellung bzw. Zurücksetzung von Passwörtern zu erstellen.

---

13 Der Grundsatz ‚Kenntnis nur soweit nötig' bezieht sich auf die Ermittlung der Gesamtheit derjenigen Informationen, auf die eine einzelne Person Zugriff haben muss, um ihre Aufgaben zu erledigen.

14 Nach dem Grundsatz der minimalen Rechtevergabe wird der Zugriff einer Person auf ein IT-System so gestaltet, dass er ihrer fachlichen Zuständigkeit entspricht.

Es muss eine Leitlinie zur Anwendung kryptografischer Kontrollen entwickelt und umgesetzt werden, um die Vertraulichkeit, Authentizität und Integrität von Informationen zu schützen. Zur Unterstützung dieser Kontrollen 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 leeren Bildschirms (Clear Screen Policy) oder des aufgeräumten Schreibtisches (Clear Desk Policy), um das Risiko eines unberechtigten Zugriffs zu reduzieren.
Bei Arbeit mit Fernzugriff 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 unter Umständen für Systeme erforderlich, die sensible, wertvolle oder kritische Informationen verarbeiten oder diese beeinflussen. Solche Kontrollen sind auf Basis der Sicherheitsanforderungen und einer Risikobewertung in Übereinstimmung mit den bestehenden Leitlinien und Konzepten (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, umgesetzt 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 Quellcodes 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 unterziehen. Dies gilt auch für Änderungen in der Produktionsumgebung. Bei wesentlichen Änderungen an der Produktionsumgebung ist eine Risikobewertung durchzuführen.
Zudem müssen regelmäßige Sicherheitstests der produktiven Systeme durchgeführt werden. Diese sind auf Grundlage der Ergebnisse einer Risikobewertung 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[15]

Um den Schutz der den Anbietern zugänglichen internen Informationssysteme des Teilnehmers zu gewährleisten, sind Informationssicherheitsanforderungen zu dokumentieren und in einer formalen Vereinbarung mit dem Anbieter festzuhalten, durch welche die mit dem Zugang des Anbieters verbundenen Risiken begrenzt werden.

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, sind sowohl auf fachlicher als auch auf technischer Ebene Rollen, Verantwortlichkeiten und Verfahren festzulegen und zu testen, damit nach Informationssicherheitsvorfällen eine rasche, wirksame und 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 Kontrollen) entsprechen.

Anforderung 1.14: Virtualisierung

Gast-VMs (virtuelle Maschinen) müssen sämtliche Sicherheitsanforderungen erfüllen, die auch für physische Hardware und Systeme gelten (z. B. Härten, Protokollierung). Als Anforderungen für Hypervisoren sind vorgeschrieben: Härten 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.

[15] Als Anbieter ist in diesem Zusammenhang 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.

Bei der Nutzung einer hybriden Cloud-Lösung wird davon ausgegangen, dass die Kritikalitätsstufe des Gesamtsystems der des angebundenen Systems mit der höchsten Kritikalität entspricht. 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: Pläne zur Aufrechterhaltung des Geschäftsbetriebs sind erstellt, und Verfahren zu deren Pflege sind umgesetzt.

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 zeitgleich von derselben Störung betroffen sind. So sollte 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 verhältnismäßig zur 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.