DEUTSCHE BUNDESBANK EUROSYSTEM

Name des Inhabers eines RTGS-Geldkontos oder des Nebensystems	
BIC	

TARGET-Regelungen zur Selbstzertifizierung für Inhaber von RTGS-Geldkonten und Nebensysteme[1]
– Sicherheitsanforderungen und Selbstzertifizierungserklärung –

Das vorliegende Dokument ist eine Übersetzung des englischen Originaltextes durch die Deutsche Bundesbank.
Der englische und rechtlich verbindliche Originaltext ist auf der Webseite der Deutschen Bundesank als pdf-Download verfügbar. Dort ist auch diese Übersetzung als pdf-Datei abrufbar.

Einleitung

Der Ausschuss für Zahlungsverkehr und Marktinfrastrukturen (Committee on Payments and Market Infrastructures – CPMI) und die Internationale Organisation der Wertpapieraufsichtsbehörden (International Organization of Securities Commissions – IOSCO) geben Prinzipien für Finanzmarktinfrastrukturen (FMI)[2] heraus. Darin werden den Betreibern von Zahlungssystemen bestimmte Verantwortlichkeiten zugewiesen, denen sie nachkommen müssen. So bezieht sich etwa das Prinzip 17 auf Aspekte im Zusammenhang mit der Sicherheit und der Zuverlässigkeit des Betriebs von Finanzmarktinfrastrukturen wie beispielsweise systemrelevanten Zahlungssystemen.

Um die Betriebsrisiken im Zusammenhang mit den Teilnehmern zu steuern, besagt Prinzip 17, dass „eine FMI für ihre Teilnehmer die Einführung von betrieblichen Mindestanforderungen erwägen sollte. So könnte eine FMI je nach Rolle und Systemrelevanz eines Teilnehmers Betriebs- und Business-Continuity-Anforderungen für ihre Teilnehmer definieren." Die Anforderungen haben zum Ziel, potenzielle teilnehmerbedingte betriebliche Schwachstellen für die FMI zu beseitigen und im Einklang mit der entsprechenden CPMI-Strategie das mit der Endpunktsicherheit zusammenhängende Betrugsrisiko bei Großbetragszahlungen zu verringern.[3]

Vor diesem Hintergrund hat das Eurosystem in seiner Funktion als Betreiber des TARGET-Systems eine Reihe von Anforderungen zum Umgang mit Risiken für die Informationssicherheit und Cyberresilienz[4] erarbeitet, die alle Inhaber von RTGS-Geldkonten und Nebensysteme (kritische und nichtkritische Teilnehmer)[5] unter

---

[1] Der „Leitfaden für TARGET-Nutzer" (im Folgenden „TARGET-Leitfaden") definiert TARGET-Nutzer (einschließlich der Nutzer von RTGS) als Kreditinstitute, Nebensysteme und sonstige Einrichtungen, die Zahlungen in TARGET abwickeln. Gemäß dem Leitfaden ist außerdem zwischen kritischen und nichtkritischen Teilnehmern zu unterscheiden, was in beiden Fällen Kreditinstitute oder Nebensysteme sein können. Im Rahmen des vorliegenden Textes werden die Begriffe „Teilnehmer" und „Nutzer" synonym verwendet.

[2] Eine umfassende Beschreibung der internationalen Standards für Finanzmarktinfrastrukturen ist auf der Website der BIZ abrufbar.

[3] Eine vollständige Beschreibung der CPMI-Strategie zur Verringerung des mit der Endpunktsicherheit zusammenhängenden Betrugsrisikos bei Großbetragszahlungen findet sich in dem Bericht Reducing the risk of wholesale payments fraud related to endpoint security auf der Website der BIZ

[4] Gemäß der „Guidance on Cyber Resilience for Financial Market Infrastructures" des CPMI und der IOSCO vom Juni 2016 ist Cyberresilienz als die Fähigkeit eines FMI definiert, Cyberangriffe zu antizipieren, abzuwehren und zu begrenzen sowie den Betrieb nach einem Cyberangriff rasch wiederherzustellen.

[5] Zentralbanken fallen ebenfalls unter die TARGET-Regelungen zur Selbstzertifizierung und müssen daher die in diesem Dokument festgelegten Anforderungen zum Umgang mit Risiken für die Informationssicherheit und Cyberresilienz erfüllen.

Berücksichtigung ihrer internen Systeme im Zusammenhang mit der in diesem Dokument definierten Zahlungstransaktionskette (Payment Transaction Chain – PTC) derzeit erfüllen müssen. Darüber hinaus wurde festgelegt, dass Inhaber von RTGS-Geldkonten, die Dritten Zugang zu ihren RTGS-Geldkonten ermöglichen [über einen Multi-Adressaten-Zugang] oder erreichbare BIC-Inhaber registrieren, das Risiko, das durch einen solchen Zugang Dritter oder durch die Registrierung erreichbarer BIC-Inhaber entsteht, steuern und dass sie die ihnen auferlegten Sicherheitsanforderungen somit erfüllen.

Außerdem hat das Eurosystem eine Reihe von Anforderungen definiert, die das Business-Continuity-Risiko reduzieren sollen und ausschließlich für die internen Systeme von Teilnehmern gelten, die laut den Regeln des TARGET-Leitfadens als kritisch eingestuft wurden. Alle Inhaber von RTGS-Geldkonten und Nebensysteme[6] müssen im Rahmen einer Selbstzertifizierung dokumentieren, inwieweit sie die nachstehenden Anforderungen umsetzen.

Anforderungen zum Informationssicherheitsmanagement und Business-Continuity-Management

Informationssicherheitsmanagement (gilt für alle Inhaber von RTGS-Geldkonten und Nebensysteme)

Das Setup der internen Systeme (Back-Office-Systeme, Front-Office-Systeme, Middleware, interne Netzwerke und Infrastruktur für die Anbindung an externe Netzwerke), die von den Teilnehmern zur Vornahme von Transaktionen in TARGET verwendet werden, kann wegen der verschiedenen Architekturen zur Anbindung an TARGET sehr unterschiedlich aussehen.

Folglich kann auch der Anwendungsbereich der Sicherheitsanforderungen aufgrund der vom Teilnehmer implementierten spezifischen Architektur variieren. Zur Festlegung des Anwendungsbereichs sollte der Teilnehmer die Bestandteile der Zahlungstransaktionskette identifizieren. Konkret beginnt diese an einem Point of Entry (PoE), d. h. einem in die Erzeugung von Transaktionen involvierten System (z. B. Workstations, Front-Office- und Back-Office-Anwendungen, Middleware) und endet bei dem System, das für die Übermittlung der Nachricht an den Netzwerkdienstleister (NSP) zuständig ist.

Es bleibt den einzelnen Organisationen überlassen, zu beurteilen, ob alle oder nur ein Teil der Sicherheitsanforderungen für sie gelten. Der Wortlaut in der englischen Originalfassung der Anforderungen richtet sich nach der im Standard ISO/IEC 27000:2018(en) verwendeten Terminologie.

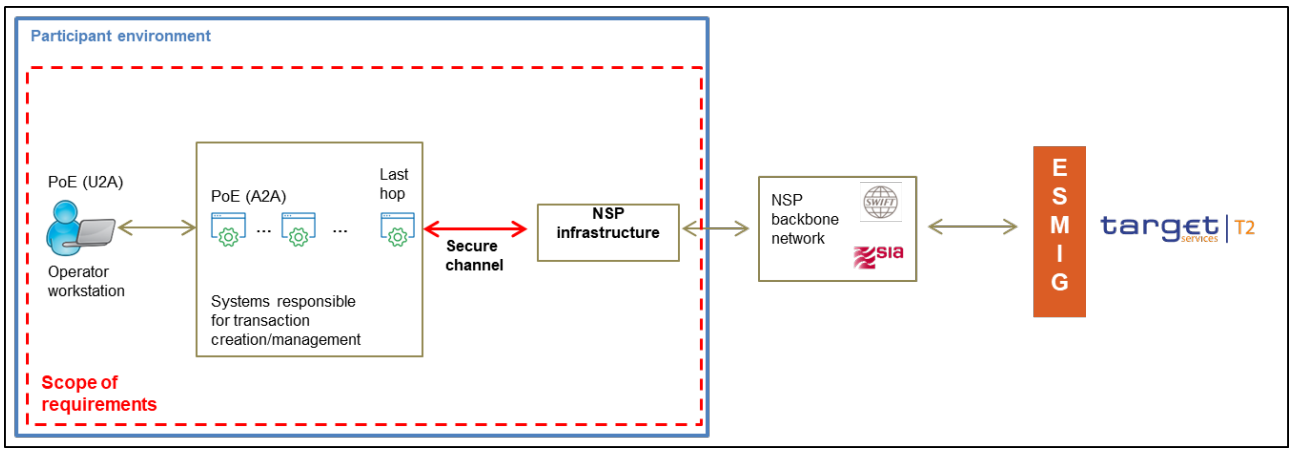
Zu Anschauungszwecken werden nachfolgend zwei mögliche Architekturen mit Hinweis auf die jeweiligen Zahlungstransaktionsketten und möglichen PoEs beschrieben.

Teilnehmer mit NSP-Infrastruktur innerhalb der eigenen Umgebung

Die zur Anbindung an TARGET verwendete NSP-Infrastruktur befindet sich innerhalb der Umgebung des Teilnehmers (siehe Abbildung).

---

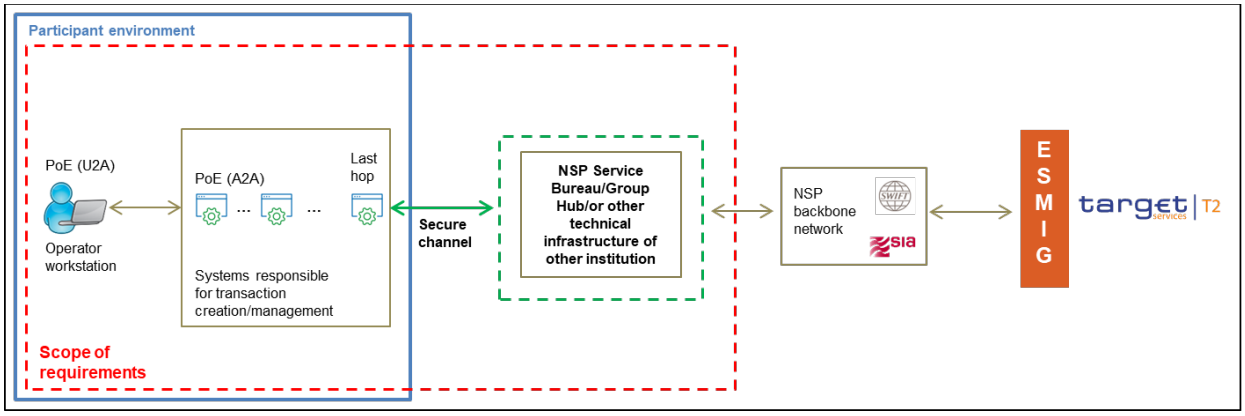
6 Sämtliche Nebensysteme müssen im Rahmen einer Selbstzertifizierung dokumentieren, inwieweit sie die in diesem Dokument genannten Anforderungen erfüllen, und zwar unabhängig von den übernommenen TARGET-Konten.



Der Anwendungsbereich umfasst: a) die vom Betreiber verwendete Workstation, b) die für die Erzeugung oder Verwaltung von Transaktionen zuständigen Systeme (z. B. Middleware, Front-Office- und Back-Office-Anwendungen), c) den sicheren Kanal zwischen der NSP-Infrastruktur und dem letzten Teilstück (Last Hop), d) die NSP-Infrastruktur und e) die physische Umgebung des Teilnehmers.

Teilnehmer mit Anbindung über ein NSP-Servicebüro, einen Gruppen-Hub oder eine sonstige technische Infrastruktur eines anderen Instituts

Da keine Komponente der NSP-Infrastruktur in der Umgebung des Teilnehmers angesiedelt ist, kommunizieren Middleware und Back-Office-Anwendungen direkt mit dem NSP-Servicebüro, dem Gruppen-Hub oder einer sonstigen technischen Infrastruktur eines anderen Instituts und nutzen hierfür einen von diesem bereitgestellten sicheren Kanal (z. B. GUI-Anwendung, Middleware-Produkt)



Der Anwendungsbereich umfasst: a) die vom Betreiber verwendete Workstation, b) die für die Erzeugung oder Verwaltung von Transaktionen zuständigen Systeme (z. B. Middleware, Front-Office- und Back-Office-Anwendungen), c) den sicheren Kanal zwischen der NSP-Infrastruktur (diese ist im vorliegenden Beispiel beim Servicebüro, beim Gruppen-Hub oder bei einer sonstigen technischen Infrastruktur eines anderen Instituts angesiedelt) und dem letzten Teilstück, und d) die physische Umgebung des Teilnehmers.

Einige der geltenden Sicherheitsanforderungen können vom NSP-Servicebüro, vom Gruppen-Hub oder von einer sonstigen technischen Infrastruktur eines anderen Instituts abgedeckt werden. Die Unterzeichner der Selbstzertifizierungserklärung bleiben jedoch weiterhin für die Einhaltung der Sicherheitsanforderungen verantwortlich, d. h., sie müssen dafür Sorge tragen, dass diese Anforderungen „in ihrem Namen“ erfüllt werden. Allgemein müssen die Inhaber von RTGS-Geldkonten und Nebensysteme sicherstellen, dass ihre

unterzeichnete Selbstzertifizierungserklärung die Sicherheitslage ihrer Organisation zutreffend und genau wiedergibt; dies schließt auch extern erbrachte Dienstleistungen ein.

Bei international tätigen Kreditinstituten kann die für die Anbindung an TARGET verwendete Infrastruktur bei der Zentrale angesiedelt sein und dort betrieben werden und dann von mehreren lokalen Zweigstellen innerhalb eines bestimmten Gruppen-Hubs genutzt werden.

In diesem Fall gilt für die Zentrale der Anwendungsbereich, der unter „Teilnehmer mit NSP-Infrastruktur innerhalb der eigenen Umgebung“ genannt ist. Einige Sicherheitsanforderungen sind allerdings auch für die lokalen Zweigstellen relevant.[7] Beispielsweise sind Kontrollen der physischen Sicherheit sowohl vom TARGET-Teilnehmer, bei dem die gemeinsame technische Infrastruktur angesiedelt ist, als auch von den Zweigstellen zu erfüllen. Der TARGET-Teilnehmer, bei dem die gemeinsame technische Infrastruktur angesiedelt ist, muss Kontrollen zum Schutz des Rechenzentrums durchführen, während die Zweigstellen dafür Sorge zu tragen haben, dass die für die Anbindung an die gemeinsame technische Infrastruktur verwendeten Komponenten (z. B. die vom Betreiber verwendete Workstation) angemessen geschützt sind.

Auch für Inhaber von RTGS-Geldkonten und Nebensysteme, die ein NSP-Servicebüro in Anspruch nehmen, gilt der gleiche Grundsatz: Sie müssen nach wie vor beurteilen, welche Kontrollen in ihren Anwendungsbereich fallen und welche nicht (und gegebenenfalls sicherstellen, dass das jeweilige NSP-Servicebüro diese Anforderungen erfüllt).

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 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 Sicherheitsstrategie, 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

[7] Diese Regeln und dieser Anwendungsbereich gelten auch, wenn die zur Anbindung an TARGET verwendete technische Infrastruktur von einer Zentrale mit Sitz außerhalb des EWR gemanagt wird.

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 zugrunde liegenden 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 eines Informationswerts (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/-innen in einer entsprechenden Stellenbeschreibung benannt und in den vertraglichen Beschäftigungsbedingungen festgehalten. Alle Bewerber/-innen, Vertragspartner und Drittanwender sind hinreichend zu überprüfen, besonders bei sensiblen Stellen bzw. Aufträgen. Mitarbeiter/-innen, Vertragspartner und Drittanwender, die informationsverarbeitende Einrichtungen nutzen, unterzeichnen eine Vereinbarung, in der ihre Sicherheitsrollen und Verantwortlichkeiten festgelegt sind. Es wird gewährleistet, dass alle Mitarbeiter/-innen, Vertragspartner und Drittanwender 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/-innen ist ein formelles Disziplinarverfahren zu schaffen, das bei Verletzung von Sicherheitsbestimmungen zur Anwendung kommt. Durch Zuweisung entsprechender Verantwortlichkeiten ist zu gewährleisten, dass das Ausscheiden einer Mitarbeiterin/eines Mitarbeiters, Vertragspartners oder Drittanwenders bzw. deren/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 verwendeten) Betriebsmittel geschützt und Vorkehrungen zum Schutz vor Entwendung von Eigentum getroffen werden. Zur Abwehr physischer Bedrohungen und zum Schutz der unterstützenden Infrastruktur wie der Stromversorgung und der Verkabelung können besondere Maßnahmen erforderlich sein.

Anforderung 1.8: Betriebsmanagement

Für die Verwaltung und den Betrieb von informationsverarbeitenden Einrichtungen, die durchgängig alle zugrundeliegenden 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 Ausgleichskontrollen 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. Ein 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 geschlossenen Austauschvereinbarungen erfolgen. Hierbei sind die einschlägigen Rechtsvorschriften einzuhalten. Werden Software-Komponenten von Drittanbietern für den Informationsaustausch mit TARGET verwendet (wenn z. B. – wie im zweiten Anforderungsszenario der TARGET-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“[8]) und im Einklang mit dem bestehenden Regelungsrahmen der Organisation (einschließlich der Informationssicherheitsstrategie) zu begründen. Es sind eindeutige Regeln für die Zugriffskontrolle auf Basis einer minimalen Rechtevergabe[9] 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

[8] Der Grundsatz „Kenntnis nur soweit nötig“ bezieht sich auf die Identifikation der Gesamtheit derjenigen Informationen, auf die eine einzelne Person Zugriff haben muss, um ihre Aufgaben zu erledigen.

[9] Der Grundsatz der minimalen Rechtevergabe bezieht sich darauf, dass der Zugriff einer Person auf IT-Systeme entsprechend ihrer fachlichen Zuständigkeit zugeschnitten sein sollte.

den physischen Zugriffskontrollen übereinstimmen, es sei denn, es bestehen angemessene Ausgleichskontrollen (z. B. Verschlüsselung, Anonymisierung personenbezogener Daten).

Um die Zuweisung von Rechten für den 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.

Es muss eine Leitlinie für die 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 die 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 dem Arbeiten 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 von Sicherheitsanforderungen und einer Risikobewertung in Übereinstimmung mit den bestehenden Leitlinien und Strategien (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[10]

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, wodurch 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 sicherzustellen (wozu auch die Meldung von Sicherheitsereignissen und -schwachstellen zählt), 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 Verfahren) entsprechen.

Anforderung 1.14: Virtualisierung

Gast-VMs (virtuelle Maschinen) müssen sämtliche Sicherheitsanforderungen erfüllen, die auch für physische Hardware und Systeme gelten (z. B. Härtung, Protokollierung). Als Anforderungen für Hypervisoren sind vorgeschrieben: Härtung des Hypervisors und des Host-Betriebssystems, regelmäßige Patches und strikte Trennung der unterschiedlichen Umgebungen (z. B. Produktions- und Entwicklungsumgebung). Auf Basis einer Risikoanalyse sind eine zentralisierte Steuerung, Protokollierung, Überwachung und Verwaltung der Zugriffsrechte, insbesondere für Konten mit privilegierten Berechtigungen, zu implementieren. Verwaltet ein Hypervisor mehrere Gast-VMs, müssen diese ein ähnliches Risikoprofil haben.

---

[10] Als Anbieter ist hier jede dritte Partei (einschließlich ihrer Mitarbeiter/-innen) zu verstehen, mit der das Institut eine vertragliche Vereinbarung zur Erbringung einer Dienstleistung abgeschlossen hat und die (einschließlich ihrer Mitarbeiter/-innen) 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 TARGET-Selbstzertifizierung erhält.

Anforderung 1.15: Cloud Computing

Die Verwendung öffentlicher und/oder hybrider Cloud-Lösungen in der Zahlungstransaktionskette muss durch eine formale Risikoanalyse begründet sein, bei der die technischen Kontrollen und Vertragsbestimmungen der Cloud-Lösung geprüft werden.

Bei 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 Inhaber eines RTGS-Geldkontos oder jedes Nebensystem, der bzw. das vom Eurosystem im Hinblick auf das reibungslose Funktionieren des RTGS-Systems 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 verhindert 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/-innen 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/-innen sind in geeigneter Weise zu schulen. Der Abstand zwischen den Tests darf nicht länger als ein Jahr sein.

Selbstzertifizierende Institute

Inhaber von RTGS-Geldkonten und Nebensysteme können sich entweder direkt oder über eine gemeinsame technische Infrastruktur mit TARGET verbinden. Im letzteren Fall liegt es schlussendlich in der Hauptverantwortung des jeweiligen Inhabers eines RTGS-Geldkontos oder Nebensystems, genau zu prüfen, welche Sicherheitsanforderungen für die spezifische technische Infrastruktur sowie die organisatorische Struktur seines Instituts gelten.

Alle Inhaber von RTGS-Geldkonten und alle Nebensysteme (d. h. kritische und nichtkritische Teilnehmer) müssen der Zentralbank, mit der sie eine Geschäftsbeziehung unterhalten, eine Selbstzertifizierungserklärung vorlegen. Werden Teile der für den TARGET-Zugang eingesetzten Verfahren und/oder technischen Infrastruktur von verschiedenen Inhabern von RTGS-Geldkonten oder Nebensystemen gemeinsam genutzt, so hat jeder dieser Teilnehmer bei der betreffenden Zentralbank eine eigene Selbstzertifizierungserklärung einzureichen.

Ein solches, gemeinsames technisches Konzept würde auch Strukturen umfassen, bei der mehrere Teilnehmer z. B. dieselbe Technik oder Anwendung verwenden, um Barmittelüberträge bzw. -überweisungen/ Bargeldüberweisungen zu erstellen/zu verarbeiten, die an TARGET gesendet werden. Die Nutzung solcher gemeinsamen technischen Infrastrukturen ist ebenfalls im Rahmen der Selbstzertifizierungserklärung zu melden.

Wenn ein Inhaber eines RTGS-Geldkontos oder ein Nebensystem seinen Geschäftsbetrieb ganz oder teilweise an einen Dritten (z. B. ein NSP-Servicebüro, einen Gruppen-Hub oder eine sonstige technische Infrastruktur eines anderen Instituts) ausgelagert hat, muss er sicherstellen, dass dieser Dritte die vom Eurosystem für Inhaber von RTGS-Geldkonten und Nebensysteme festgelegten Sicherheitsanforderungen erfüllt.[11]

Falls eine oder mehrere Sicherheitsanforderungen nicht anwendbar sind, sollten die Inhaber von RTGS-Geldkonten und Nebensysteme dies in der nachstehenden Tabelle zur Prüfung der Umsetzung (Compliance Check) vermerken. Außerdem ist in der entsprechenden Rubrik der Selbstzertifizierung (mit der Bezeichnung „Umsetzungsfortschritt“) zu erläutern, warum eine bestimmte Sicherheitsanforderung nicht anwendbar ist.

Die Inhaber von RTGS-Geldkonten und Nebensysteme werden gebeten, sich in Zweifelsfällen mit der Zentralbank, mit der sie eine vertragliche Beziehung unterhalten, in Verbindung zu setzen, um den Umfang ihrer Selbstzertifizierung zu klären.

Unterzeichner

Die Selbstzertifizierungserklärung ist von einer Führungskraft auf Vorstands- oder vergleichbarer Ebene[12] zu unterzeichnen, die innerhalb der Organisation des Inhabers eines RTGS-Geldkontos oder eines Nebensystems für das Risikomanagement im Bereich der Informationssicherheit verantwortlich ist.

Handelt es sich bei den Inhabern von RTGS-Geldkonten oder Nebensystemen um kritische Teilnehmer, so ist die Selbstzertifizierung zusätzlich vom (externen oder internen) Revisor dieses Teilnehmers zu unterzeichnen.

Prüfung der Umsetzung (Compliance Check)

In der Selbstzertifizierungserklärung müssen die Inhaber von RTGS-Geldkonten und Nebensysteme für jede der vom Eurosystem festgelegten Anforderungen angeben, ob sie diese umgesetzt oder nicht umgesetzt haben bzw. ob diese nicht anwendbar ist.

---

[11] Ein *Servicebüro* ist eine Organisation, die selbst NSP-Nutzer sein kann (aber nicht sein muss) und NSP-Nutzern einen technischen Zugang zum NSP-Netz ermöglicht. NSP-Nutzer und Servicebüro sind organisatorisch nicht miteinander verbunden. Zu den von einem Servicebüro angebotenen Diensten gehören die Bereitstellung und der Betrieb von NSP-Nachrichten- und/oder NSP-Konnektivitätskomponenten im Auftrag von NSP-Nutzern. Ein *Gruppen-Hub* ist eine Organisation, die selbst NSP-Nutzer sein kann (aber nicht sein muss) und NSP-Nutzern einen technischen Zugang zum NSP-Netz ermöglicht; die NSP-Nutzer gehören zur gleichen Organisation wie der Gruppen-Hub. Ein *anderes Institut* ist ein Institut, das eine technische Infrastruktur für Inhaber von RTGS-Geldkonten oder Nebensysteme bereitstellt.

[12] Hierbei handelt es sich um hochrangige Vertreter/-innen eines Unternehmens, die unternehmensweite Entscheidungen treffen. Beispiele für hochrangige Führungskräfte sind der Chief Executive Officer (CEO), der Chief Operating Officer (COO) und der Chief Information Officer (CIO). Sofern entsprechende Funktionen vorhanden sind, könnte der Unterzeichner auch ein Chief Risk Officer (CRO) oder Chief Information Security Officer (CISO) sein.

Im Falle der Nichtumsetzung einer bestimmten Anforderung sind in der entsprechenden Rubrik der Selbstzertifizierung (mit der Bezeichnung „Umsetzungsfortschritt“) die größten Risiken[13] zu beschreiben. Darüber hinaus sollten ein Aktionsplan zur Behebung des Problems beigefügt sowie der vorgesehene Termin für die Umsetzung jeder einzelnen Maßnahme benannt werden. Die zuständige Zentralbank muss diese Angaben auswerten und die zeitnahe Durchführung der Maßnahmen zur Risikominderung überwachen. Zudem wird das Leitungsorgan des Eurosystems, das für den sicheren und zuverlässigen Betrieb von TARGET zuständig ist, über das Ergebnis der Selbstzertifizierung sowie über den Umsetzungsfortschritt der zur Risikominderung ergriffenen Maßnahmen unterrichtet.

Umsetzungsgrad

Inhaber von RTGS-Geldkonten und Nebensysteme sind verpflichtet anzugeben, inwieweit die vom Eurosystem in seiner Funktion als TARGET-Systembetreiber festgelegten Anforderungen zum Informationssicherheitsmanagement umgesetzt wurden.

Bei der Beurteilung der Frage, inwieweit die Inhaber von RTGS-Geldkonten und Nebensysteme die Vorgaben insgesamt einhalten, verwendet der TARGET-Betreiber einen quantitativen Ansatz (die Umsetzung der Business-Continuity-Anforderungen wird nur bei kritischen Teilnehmern geprüft). Dabei werden folgende Kriterien zugrunde gelegt:

- **Vollständige Umsetzung:** Die Inhaber von RTGS-Geldkonten und Nebensysteme erfüllen 100 % der Anforderungen (d. h. alle 15 Anforderungen an die Informationssicherheit und alle 6 Business-Continuity-Anforderungen (nur bei kritischen Teilnehmern)).

- **Geringfügige Nichtumsetzung:** Die Inhaber von RTGS-Geldkonten und Nebensysteme erfüllen weniger als 100 %, aber mindestens 66 % der Anforderungen (d. h. 10 Anforderungen an die Informationssicherheit und 4 Business-Continuity-Anforderungen (nur bei kritischen Teilnehmern)).

- **Gravierende Nichtumsetzung:** Die Inhaber von RTGS-Geldkonten und Nebensysteme erfüllen weniger als 66 % der Anforderungen (d. h. weniger als 10 Anforderungen an die Informationssicherheit oder weniger als 4 Business-Continuity-Anforderungen (nur bei kritischen Teilnehmern))

Inhabern von RTGS-Geldkonten oder Nebensystemen, die nachweisen, dass eine bestimmte Anforderung nicht auf sie anwendbar ist, wird im Rahmen der obigen Beurteilung in Bezug auf die betreffende Anforderung eine Umsetzung bescheinigt.

Meldung im Auftrag anderer Inhaber von RTGS-Geldkonten/Nebensysteme

Ein Inhaber eines RTGS-Geldkontos oder Nebensystem kann eine eigene Selbstzertifizierungserklärung bei der betreffenden Zentralbank einreichen und gleichzeitig auch den Stand der Umsetzung im Auftrag anderer Inhaber von RTGS-Geldkonten/Nebensysteme melden. Solche Meldungen sind möglich, wenn die beiden folgenden Bedingungen erfüllt sind:

(i) Alle Teilnehmer gehören zur selben „Bankengruppe“ im Sinne der Definition der TARGET-Leitlinie und nutzen dieselbe technische Infrastruktur für die Einreichung von Zahlungen.

[13] Hierzu gehören beispielsweise unzureichende Vorkehrungen gegen Denial-of-Service-Angriffe oder das Fehlen einer unterbrechungsfreien Stromversorgung.

Dabei nutzen Inhaber von RTGS-Geldkonten und Nebensysteme, die durch eine einzige Selbstzertifizierungserklärung erfasst sind, dieselbe Infrastruktur für die Übermittlung von Zahlungen an TARGET, auch wenn sie mit unterschiedlichen Zentralbanken eine Geschäftsbeziehung unterhalten.

Sollte sich in einer Bankengruppe ein kritischer Teilnehmer befinden, so obliegt es diesem kritischen Teilnehmer, die Selbstzertifizierungserklärung bei der betreffenden Zentralbank einzureichen. Zugleich nimmt er auch die Meldungen für die anderen Teilnehmer seiner Gruppe vor.

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

Innerhalb einer Bankengruppe kann es vorkommen, dass einige Inhaber von RTGS-Geldkonten und Nebensysteme als kritisch und andere als nichtkritisch eingestuft werden. Deshalb wird in der Selbstzertifizierungserklärung (mithilfe des Feldes „Meldung für“ zu jeder Art von Anforderung) unterschieden, welche Teilnehmer nur die Anforderungen an die Informationssicherheit und welche Teilnehmer darüber hinaus die Business-Continuity-Anforderungen umsetzen müssen.

Wenn eine bestimmte Anforderung von einigen Teilnehmern umgesetzt wird, während sie für andere Teilnehmer nicht anwendbar ist, sollten in der Selbstzertifizierungserklärung für diese Anforderung beide Felder (d. h. „Anforderung umgesetzt“ und „Anforderung nicht anwendbar“) angekreuzt werden. In dem entsprechenden separaten Feld der Erklärung ist genauer zu erläutern, weshalb eine bestimmte Anforderung für einen bestimmten Teilnehmer nicht anwendbar ist.

Im Falle der Nichtumsetzung einer oder mehrerer Anforderungen durch einen Inhaber eines RTGS-Geldkontos oder ein Nebensystem muss dieser bzw. dieses seine eigene Selbstzertifizierungserklärung bei der betreffenden Zentralbank einreichen. Die Vorgehensweise, dass jeder Teilnehmer einer Gruppe, der eine Anforderung nicht umsetzt, eine eigene Selbstzertifizierungserklärung abgeben muss, ist auch einzuhalten, wenn die fehlende Anforderung für alle Teilnehmer der Gruppe identisch ist.

Selbstzertifizierungserklärung

Kontaktdaten

Nachstehend sind der Name des Inhabers eines RTGS-Geldkontos oder des Nebensystems und die Kontaktdaten der Person anzugeben, die als Ansprechpartner zur Verfügung steht, wenn weitere Informationen benötigt werden.

Name des Inhabers eines RTGS-Geldkontos oder des Nebensystems	
Anschrift	
BIC	
Kontaktperson (Name in Druckbuchstaben)	
Kontaktperson (Telefon)	
Kontaktperson (E-Mail)	

Verwendung eines NSP-Servicebüros, Gruppen-Hubs oder einer sonstigen technischen Infrastruktur eines anderen Instituts

Neben einer direkten Anbindung an TARGET kann die Anbindung auch über ein NSP-Servicebüro, einen Gruppen-Hub oder eine sonstige technische Infrastruktur eines anderen Instituts erfolgen.

Ist Ihre Organisation über ein NSP-Servicebüro an TARGET angeschlossen?	☐ Ja	☐ Nein
Wenn ja, geben Sie bitte den Namen und den BIC des NSP-Servicebüros an.		

Ist Ihre Organisation über einen Gruppen-Hub an TARGET angeschlossen?	☐ Ja	☐ Nein
Wenn ja, geben Sie bitte den Namen und den BIC des Gruppen-Hubs an.		

Ist Ihre Organisation über eine technische Infrastruktur eines anderen Instituts, das weder als NSP-Servicebüro noch als Gruppen-Hub eingestuft ist, an TARGET angeschlossen?	☐ Ja	☐ Nein
Wenn ja, geben Sie bitte den Namen und den BIC des anderen Instituts/der anderen Institute an.		

Anforderungen an das Informationssicherheitsmanagement (gilt für alle Inhaber von RTGS-Geldkonten und Nebensysteme[14])

	Anforderung umgesetzt	**Anforderung nicht umgesetzt**	**Anforderung nicht anwendbar**
Anforderung 1.1	☐	☐	☐
Anforderung 1.2	☐	☐	☐
Anforderung 1.3	☐	☐	☐
Anforderung 1.4	☐	☐	☐
Anforderung 1.5	☐	☐	☐
Anforderung 1.6	☐	☐	☐
Anforderung 1.7	☐	☐	☐
Anforderung 1.8	☐	☐	☐
Anforderung 1.9	☐	☐	☐
Anforderung 1.10	☐	☐	☐
Anforderung 1.11	☐	☐	☐
Anforderung 1.12	☐	☐	☐
Anforderung 1.13	☐	☐	☐
Anforderung 1.14	☐	☐	☐
Anforderung 1.15	☐	☐	☐
Welcher Standard für das Informationssicherheitsmanagement (z. B. ISO 27001, COSO, ISACA, COBIT, NIST) wird in Ihrer Organisation verwendet?			
Nutzt Ihre Organisation für die Zahlungstransaktionskette relevante Dienste, die von einem Cloud-Anbieter zur Verfügung gestellt werden (d. h. öffentliche oder hybride Cloud-Lösungen oder externe Dokumentenablagesysteme)?			

[14] Alle **Inhaber von RTGS-Geldkonten und Nebensysteme** müssen also die in dieser Tabelle aufgeführten unterschiedlichen Anforderungen an das Informationssicherheitsmanagement erfüllen (Auswahlkästchen) und die Fragen des nachfolgenden Abschnitts beantworten.

Meldung der **Anforderungen zum Informationssicherheitsmanagement** im Auftrag anderer Inhaber von RTGS-Geldkonten oder Nebensysteme (soweit anwendbar)	
BIC des Teilnehmers	Jeweilige Zentralbank des Teilnehmers

Business-Continuity-Anforderungen (gilt ausschließlich für kritische Teilnehmer)

	Anforderung umgesetzt	**Anforderung nicht umgesetzt**	**Anforderung nicht anwendbar**
Anforderung 2.1	☐	☐	☐
Anforderung 2.2	☐	☐	☐
Anforderung 2.3	☐	☐	☐
Anforderung 2.4	☐	☐	☐
Anforderung 2.5	☐	☐	☐
Anforderung 2.6	☐	☐	☐

Meldung der **Business-Continuity-Anforderungen** im Auftrag anderer Inhaber von RTGS-Geldkonten oder Nebensysteme (soweit anwendbar)	
BIC des Teilnehmers	Jeweilige Zentralbank des Teilnehmers

Umsetzungsfortschritt

Dieser Abschnitt ist auszufüllen, wenn bei einem Teilnehmer a) eine Nichtumsetzung einer Sicherheitsanforderung festgestellt wurde oder b) eine Anforderung als „nicht anwendbar“ gekennzeichnet wurde.

Geben Sie bitte für jede in der obigen Tabelle als „nicht anwendbar“ gekennzeichnete Anforderung eine kurze Begründung hierfür an. Anmerkungen:
Welche Risiken infolge der Nichtumsetzung der Anforderungen 1.1 bis 1.15 bzw. 2.1 bis 2.6 wurden ermittelt? (Bitte antworten Sie für jede mit „nicht umgesetzt“ gekennzeichnete Anforderung getrennt.) Anmerkungen:
Welche Schritte werden eingeleitet, um eine vollständige Umsetzung aller Anforderungen zu erreichen? (Bitte antworten Sie für jede mit „nicht umgesetzt“ gekennzeichnete Anforderung getrennt.) Anmerkungen:
Bis zu welchem Datum soll die vollständige Umsetzung erreicht werden?

Zertifizierung

Die Unterzeichner bestätigen, dass sie die in dieser Selbstzertifizierungserklärung aufgeführten Anforderungen gelesen und verstanden haben. Die Erklärung ist jährlich zu erneuern. In der Zwischenzeit ist jede festgestellte Nichtumsetzung unverzüglich der zuständigen Zentralbank zu melden.

Die Unterzeichner bestätigen, dass die in der Erklärung enthaltenen Informationen die aktuelle Situation zutreffend und genau beschreiben. Sie bestätigen ferner, dass die Erklärung unter ihrer Leitung und Kontrolle erstellt wurde und die ausgewiesenen Angaben von qualifiziertem Personal ordnungsgemäß erhoben und ausgewertet wurden. Alle Angaben sind nach bestem Wissen und Gewissen der Unterzeichner zutreffend, korrekt und vollständig. Den Unterzeichnern ist bekannt, dass die Einreichung dieser Daten eine wesentliche Verpflichtung ist und falsche, ungenaue oder irreführende Angaben einen Verstoß gegen Artikel 25 Absatz 2 Buchstabe c von Teil I, Anhang I der TARGET-Leitlinie darstellen, was ein Grund für den Ausschluss des betreffenden Instituts von TARGET ist.

Die Unterzeichner bestätigen zudem, dass es in ihrer Organisation einen Prozess gibt, der sicherstellt, dass die Einhaltung der Anforderungen im folgenden Jahr gewährleistet bleibt. Sofern die Maßnahmen noch nicht vollständig umgesetzt wurden, bestätigen die Unterzeichner, dass angemessene Vorkehrungen getroffen werden, die eine vollständige Umsetzung spätestens bis zum Ende des nächsten Kalenderjahrs ermöglichen.

Reicht ein Teilnehmer die Erklärung und Meldung für einen anderen oder mehrere andere Inhaber von RTGS-Geldkonten oder Nebensysteme ein, bestätigen die Unterzeichner die vorstehenden Punkte für alle in der Erklärung aufgeführten Teilnehmer. Den Unterzeichnern ist bekannt, dass die Einreichung dieser Informationen eine wesentliche Verpflichtung des Teilnehmers ist, für den sie die Unterschrift leisten, und dass falsche, ungenaue oder irreführende Angaben einen Verstoß gegen Artikel 25 Absatz 2 Buchstabe c von Teil I, Anhang I der TARGET-Leitlinie darstellen, was ein Grund für den Ausschluss des betreffenden Instituts von der Teilnahme an TARGET ist.

Unterschrift

Name des/der Unterzeichnenden (in Druckbuchstaben)	
Titel/Funktion (Führungskraft auf Vorstandsebene o. Ä.)	
Datum	
Unterschrift	

Unterschrift des Revisors – nur von kritischen Teilnehmern auszufüllen

Name des/der Prüfer/-in (in Druckbuchstaben)	
Titel (Angabe, ob interner oder externer Revisor)	
Datum	
Unterschrift	

Diese Selbstzertifizierungserklärung bitte zurücksenden an

Kundenbetreuungsservice	bitte auswählen:
E-Mail-Adresse des KBS	
Kontaktperson	