DEUTSCHE BUNDESBANK EUROSYSTEM

Selbstzertifizierungserklärung

1 Kontaktdaten

In der nachstehenden Tabelle sind der Name des TARGET2-Teilnehmers und die Kontaktdaten der Person anzugeben, die als Ansprechpartner zur Verfügung steht, wenn weitere Informationen benötigt werden.

Name des TARGET2-Teilnehmers	
Anschrift	
BIC/Kontonummer	
Kontaktperson (Name in Druckbuchstaben)	
Kontaktperson (Telefon)	
Kontaktperson (E-Mail)	

2 Selbstzertifizierende Organisation

TARGET2-Teilnehmer können sich entweder direkt oder über eine gemeinsame technische Infrastruktur mit der TARGET2-Gemeinschaftsplattform verbinden. In diesem Zusammenhang ist zu klären, ob alle TARGET2-Teilnehmer, die eine gemeinsame technische Infrastruktur nutzen, eine Selbstzertifizierungserklärung bei ihrer Zentralbank einreichen müssen, oder ob nur der TARGET2-Teilnehmer, der diese gemeinsame technische Infrastruktur betreibt, eine solche Erklärung vorlegen muss. Eine multinational tätige Bank verfügt beispielsweise über eine Reihe von Zweigstellen; dabei nutzen alle Zweigstellen die von der Zentrale betriebene technische Infrastruktur. Hier stellt sich die Frage, ob alle Zweigstellen eine Selbstzertifizierungserklärung bei der Zentralbank, mit der sie eine Geschäftsbeziehung unterhalten, einreichen müssen oder nur die Zentrale als Betreiberin der technischen Infrastruktur.

Die Sicherheitsanforderungen gelten nicht nur für eine zentrale technische Plattform, sondern grundsätzlich auch für die Zweigstellen einer Bank, selbst wenn diese eine zentrale Infrastruktur nutzen. Die physischen Sicherheitskontrollen beispielsweise sind sowohl von dem TARGET2-Teilnehmer, der die gemeinsame technische Infrastruktur betreibt, als auch von der Zweigstelle zu gewährleisten. Der Anwendungsbereich ist jedoch unterschiedlich. Der als Betreiber der gemeinsamen technischen Infrastruktur fungierende TARGET2-Teilnehmer muss Kontrollen zum Schutz des Rechenzentrums durchführen, während eine Zweigstelle dafür Sorge zu tragen hat, dass die für die Anbindung an die gemeinsame technische Infrastruktur verwendeten Komponenten angemessen geschützt sind.

Bei den obigen Ausführungen handelt es sich lediglich um ein Beispiel, das veranschaulichen soll, warum jeder einzelne TARGET2-Teilnehmer eine Selbstzertifizierungserklärung bei der Zentralbank, mit der er eine Geschäftsbeziehung unterhält, vorlegen muss.

Darüber hinaus ist es wichtig zu beachten, dass es letztendlich in der Hauptverantwortung des jeweiligen TARGET2-Teilnehmers liegt, genau zu prüfen, welche Sicherheitsanforderungen für die spezifischen technischen und organisatorischen Strukturen seiner Institution gelten. Wenn ein TARGET2-Teilnehmer seinen Geschäftsbetrieb ganz oder teilweise an einen Dritten (z. B. ein Servicebüro) ausgelagert hat, muss er sicherstellen, dass dieser Dritte die vom Eurosystem für TARGET2-Teilnehmer festgelegten Sicherheitsanforderungen erfüllt.

Zusammenfassend ist festzuhalten, dass alle TARGET2-Teilnehmer (d. h. sowohl direkte Teilnehmer als auch Nebensysteme) eine Selbstzertifizierungserklärung bei der Zentralbank, mit der sie eine Geschäftsbeziehung unterhalten, einreichen sollten. Wenn Teile des Geschäftsbetriebs und/oder der für den Zugang zu TARGET2 verwendeten technischen Infrastruktur von verschiedenen TARGET2-Teilnehmern gemeinsam genutzt werden, hat jeder TARGET2-Teilnehmer seine eigene Selbstzertifizierungserklärung bei der jeweiligen Zentralbank vorzulegen. Wenn eine oder mehrere Sicherheitsanforderungen nicht anwendbar sind, muss der TARGET2-Teilnehmer dies in der unten stehenden Tabelle zur Prüfung der Umsetzung angeben. Ferner sollte in der entsprechenden, in der Selbstzertifizierungserklärung enthaltenen Rubrik (mit der Bezeichnung „Umsetzungsfortschritt“) erläutert werden, warum eine bestimmte Sicherheitsanforderung nicht anwendbar ist.

In Zweifelsfällen werden die TARGET2-Teilnehmer gebeten, sich mit der Zentralbank, mit der sie eine vertragliche Beziehung unterhalten, in Verbindung zu setzen, um den Umfang ihrer Selbstzertifizierung zu klären.

3 Servicebüro

Neben einer direkten Anbindung an die TARGET2-Gemeinschaftsplattform kann die Anbindung auch über ein Servicebüro erfolgen.

Ist Ihre Organisation über ein Servicebüro an die TARGET2-Gemeinschaftsplattform angeschlossen?	☐ Ja	☐ Nein
Wenn ja, geben Sie bitte den Namen des Servicebüros an.		

4 Prüfung der Umsetzung (Compliance Check)

Für jede der vom Eurosystem festgelegten Anforderungen muss der TARGET-Nutzer in der Selbstzertifizierungserklärung angeben, inwieweit diese umgesetzt wurden.

Im Falle der Nichtumsetzung (Stufe 2 oder 3) dieser Anforderungen sind in der entsprechenden, in der Selbstzertifizierung enthaltenen Rubrik (mit der Bezeichnung „Umsetzungsfortschritt“) die größten Risiken[1] zu beschreiben. Darüber hinaus sollte 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 Durchführung der Maßnahmen zur Risikominderung überwachen.

Umsetzungsgrad

TARGET2-Teilnehmer sind verpflichtet anzugeben, inwieweit die vom Eurosystem in seiner Funktion als TARGET2-Systembetreiber festgelegten Anforderungen zum Informationssicherheitsmanagement umgesetzt wurden.

Durch Ankreuzen der entsprechenden Kästchen gibt der TARGET2-Teilnehmer bekannt, inwieweit die Vorgaben umgesetzt wurden.

- **Vollständige Umsetzung**
  Der Teilnehmer hat die in der Selbstzertifizierungserklärung aufgeführte Anforderung vollständig umgesetzt.

- **Stufen der Nichtumsetzung**
  - **Stufe 1:** keine wesentlichen Bereiche der Nichtumsetzung; es kann mit hinreichender Sicherheit davon ausgegangen werden, dass dies nicht zu einer Beeinträchtigung der reibungslosen Funktion von TARGET2 und/oder negativen Auswirkungen auf andere Systemteilnehmer führen wird.
  - **Stufe 2:** wesentliche Bereiche der Nichtumsetzung; eine Zusicherung wie in Stufe 1 kann nicht gegeben werden; eine Ausnutzung der ermittelten Schwachstellen könnte zu einer Beeinträchtigung der reibungslosen Funktion von TARGET2 und/oder negativen Auswirkungen auf andere Systemteilnehmer führen.
  - **Stufe 3:** Nichtumsetzung; eine Zusicherung wie in Stufe 1 kann nicht gegeben werden; eine Ausnutzung der ermittelten Schwachstellen würde zu einer erheblichen Beeinträchtigung der reibungslosen Funktion von TARGET2 und/oder negativen Auswirkungen auf andere Systemteilnehmer führen.

[1] Ein großes Risiko könnten beispielsweise sein: unzureichende Vorkehrungen gegen Denial-of-Service-Angriffe, eine nicht vorhandene unterbrechungsfreie Stromversorgung u. Ä.

	Vollständige Umsetzung	Nichtumsetzung			Nicht anwendbar
		Stufe 1	Stufe 2	Stufe 3	
1 Anforderungen an das Informationssicherheitsmanagement					
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	☐	☐	☐	☐	☐

	Vollständige Umsetzung	Nichtumsetzung			Nicht anwendbar
		Stufe 1	Stufe 2	Stufe 3	
2 Anforderungen an das Business-Continuity-Management (HINWEIS: gilt nur für kritische Teilnehmer)					
Anforderung 2.1	☐	☐	☐	☐	☐
Anforderung 2.2	☐	☐	☐	☐	☐
Anforderung 2.3	☐	☐	☐	☐	☐
Anforderung 2.4	☐	☐	☐	☐	☐
Anforderung 2.5	☐	☐	☐	☐	☐
Anforderung 2.6	☐	☐	☐	☐	☐

Welcher Informationssicherheitsstandard wird für Sicherheitskontrollen hauptsächlich verwendet?	

Umsetzungsfortschritt

Sofern Bereiche der Nichtumsetzung gemäß Stufe 2 oder 3 ermittelt wurden, ist auch der folgende Abschnitt auszufüllen.

Geben Sie bitte für jede in der obigen Tabelle als „nicht anwendbar“ gekennzeichnete Anforderung eine kurze Begründung an. Anmerkungen
Wurden Risiken infolge einer Nichtumsetzung (gemäß Stufe 2 oder 3) der Anforderungen 1.1 bis 1.13 und 2.1 bis 2.6 ermittelt? Anmerkungen
Welche Schritte werden eingeleitet, damit eine vollständige Umsetzung der Anforderungen erreicht wird bzw. der Grad der Nichterfüllung nur noch der Stufe 1 entspricht? Anmerkungen
Bis zu welchem Datum soll die vollständige Umsetzung erreicht werden bzw. der Grad der Nichterfüllung nur noch der Stufe 1 entsprechen? Anmerkungen

5 Unterzeichner

Die Selbstzertifizierungserklärung ist von einer Führungskraft (auf Vorstandsebene oder einer vergleichbaren Ebene) zu unterzeichnen, die für den entsprechenden Geschäftsbereich verantwortlich ist. Angesichts der wichtigen Rolle, die der Informationstechnologie (IT) zukommt, sollte die Selbstzertifizierung zusätzlich von einer Führungskraft (ebenfalls auf Vorstands- oder vergleichbarer Ebene) aus dem IT Bereich des Teilnehmers unterzeichnet werden. Wenn eine Führungskraft sowohl für den Geschäfts- als auch den IT-Bereich zuständig ist, reicht eine Unterschrift aus.

Bei kritischen TARGET2-Teilnehmern ist die Selbstzertifizierung mit Wirkung ab dem Jahr 2019 zusätzlich vom (externen oder internen) Revisor des jeweiligen kritischen Teilnehmers zu unterzeichnen.

Zertifizierung

Die Unterzeichner bestätigen, dass sie die in dieser Selbstzertifizierungserklärung aufgeführten Anforderungen gelesen und verstanden haben. Die Erklärung gilt für ein Jahr und muss spätestens ein Jahr nach dem Datum der ersten Unterschrift erneuert werden.

Die Unterzeichner bestätigen, dass die in der Erklärung enthaltenen Informationen ein zutreffendes und genaues Bild der aktuellen Situation vermitteln. Sie bestätigen ferner, dass die Erklärung unter ihrer Leitung und Kontrolle erstellt wurde und die ausgewiesenen Angaben von qualifiziertem Personal ordnungsgemäß erhoben und ausgewertet wurden. Alle Angaben sind nach bestem Wissen und Gewissen der Unterzeichner zutreffend, korrekt und vollständig. Den Unterzeichnern ist bekannt, dass die Einreichung dieser Daten eine wesentliche Verpflichtung ist und die Einreichung falscher, ungenauer oder irreführender Angaben einen Verstoß gegen Artikel 34 Absatz 2 Buchstabe c der TARGET2-Leitlinie darstellt, was ein Grund für den Ausschluss des betreffenden Instituts von TARGET2 ist.

Die Unterzeichner bestätigen ferner, dass es in ihrer Organisation einen Mechanismus gibt, der sicherstellt, dass die Einhaltung der Anforderungen im folgenden Jahr gewährleistet bleibt, oder – sofern die Maßnahmen noch nicht vollständig umgesetzt wurden – dass angemessene Vorkehrungen getroffen werden, die zufriedenstellende Fortschritte bei der Durchführung der im Aktionsplan aufgeführten Punkte ermöglichen.

Erste Unterschrift

Name der Führungskraft aus dem Geschäftsbereich (in Druckbuchstaben)	
Titel	
Datum	
Unterschrift	

Zweite Unterschrift

Name der Führungskraft aus dem IT-Bereich (in Druckbuchstaben)	
Titel	
Datum	
Unterschrift	

Unterschrift des Revisors – auszufüllen von kritischen TARGET2-Teilnehmern (ab 2019)

Name des Prüfers (in Druckbuchstaben)	
Titel (Angabe, ob interner oder externer Revisor)	
Datum	
Unterschrift	

Diese Selbstzertifizierungserklärung bitte zurücksenden an

Name der Zentralbank	bitte auswählen:
Anschrift	