Benutzerhandbuch zur Public-Key-Zertifizierung für den Internetzugang

Version 1.3 / Mai 2015

INHALTSVERZEICHNIS

1 ALLGEMEINES

1.1 Einleitung

Dieses Handbuch enthält die Regelungen, die die Banca d'Italia als anerkannte Zertifizierungsstelle bei der Vergabe und Nutzung digitaler Zertifikate im Rahmen des Internetzugangs zu TARGET2 anwendet.

Der Zertifizierungsdienst wird von der Banca d'Italia im Auftrag des Eurosystems erbracht.

Das Handbuch richtet sich an:

1. Zentralbanken, die am TARGET2-System teilnehmen bzw. daran angeschlossen sind,
2. Kreditinstitute und sonstige Einrichtungen, die gemäß dem Leitfaden für TARGET2-Nutzer (siehe TARGET2-Internetseite der Bundesbank) berechtigt sind, über den Internetzugang an TARGET2 teilzunehmen[1],
3. Zertifikatsinhaber, die von den Teilnehmern bevollmächtigt wurden.

2 IDENTIFIKATIONSDATEN

2.1 Zertifizierungsstelle

Name	Banca d'Italia
Sitz	Via Nazionale, 91 – 00184 ROMA
Gesetzlicher Vertreter	Präsident
Internetseite	www.bancaditalia.it

2.2 Benutzerhandbuch

Bei dem vorliegenden Dokument handelt es sich um die Version 1.2 des Benutzerhandbuchs für die Public-Key-Zertifizierung durch die Banca d'Italia (Stand: 5. Februar 2014). Es ist auf der TARGET2-Internetseite der Deutschen Bundesbank verfügbar.

[1] http://www.bundesbank.de/Redaktion/DE/Standardartikel/Aufgaben/Unbarer_Zahlungsverkehr/target2_veroeffentlichungen_leitfaden.html

3 PFLICHTEN DER ZERTIFIZIERUNGSSTELLE, DER NATIONALEN ZENTRALBANKEN, DER TEILNEHMER UND DER ZERTIFIKATSINHABER

3.1 Pflichten der Zertifizierungsstelle

Die Zertifizierungsstelle

1. ergreift alle organisatorischen und technischen Maßnahmen zum Schutz Dritter,
2. stellt umfassende und klare Informationen über das Zertifizierungsverfahren, die für den Zugang erforderlichen technischen Voraussetzungen und die Nutzungsbeschränkungen zur Verfügung,
3. bietet einen sicheren und zeitnahen Dienst für die Vergabe, Sperrung, Reaktivierung, den Widerruf oder die Erneuerung digitaler Zertifikate und gewährleistet eine effiziente, zeitnahe und sichere Funktionsweise der Listen ausgestellter, gesperrter und widerrufener Signaturzertifikate,
4. gewährleistet die genaue Festlegung des Zeitpunkts (Datum, Uhrzeit) der Ausstellung, eines Widerrufs oder einer Sperrung digitaler Zertifikate,
5. fertigt keine Kopie der persönlichen Signaturschlüssel des Zertifikatsinhabers an und bewahrt diese nicht auf,
6. stellt sämtliche erforderlichen Informationen, insbesondere die genauen Nutzungsbedingungen für Zertifikate einschließlich der Nutzungsbeschränkungen zusammen und stellt diese Informationen allen an den Zertifizierungsdiensten interessierten Parteien zur Verfügung,
7. verwendet zuverlässige Systeme für die Verwaltung des Verzeichnisses der Zertifikate, bei denen sichergestellt ist, dass ausschließlich dazu befugte Personen Eintragungen hinzufügen oder verändern können, dass die Echtheit der Daten geprüft werden kann und dass die bevollmächtigte Person von jedem Vorfall Kenntnis erlangt, der die Sicherheit gefährdet,
8. teilt im Falle der Einstellung ihrer Tätigkeit den Inhabern mindestens sechzig Tage vorher mit, dass alle Zertifikate, die bis dahin nicht ausgelaufen sind, widerrufen werden, und widerruft diese zu gegebener Zeit und
9. ergreift Sicherheitsmaßnahmen für den Umgang mit persönlichen Daten gemäß der aktuellen italienischen Gesetzgebung (Gesetz zum Schutz personenbezogener Daten, Decreto Legislativo Nr. 196 vom 30. Juni 2003).

Die Zertifizierungsstelle zeichnet für die Erfüllung sämtlicher gesetzlicher und in diesem Handbuch genannter Verpflichtungen verantwortlich.

Die Zertifizierungsstelle haftet nicht für:

1. die Folgen aus der Nichterfüllung der in diesem Handbuch genannten Verfahrensweisen und Modalitäten seitens des Zertifikatsinhabers und
2. die Nichterfüllung ihrer Verpflichtungen aufgrund höherer Gewalt.

3.2 Pflichten der Zentralbanken

Die Zentralbank

1. stellt den Teilnehmern und Zertifikatsinhabern sämtliche relevanten Dokumente der Zertifizierungsstelle zur Verfügung,
2. prüft die Identität des Antragstellers eines Zertifikats,
3. prüft die Echtheit des Antrags,
4. lässt der Zertifizierungsstelle unverzüglich sämtliche Formulare und sonstigen Mitteilungen zukommen, die sie von den Teilnehmern gemäß den in diesem Handbuch festgelegten Verfahrensweisen erhalten hat, und
5. lässt den Teilnehmern unverzüglich sämtliche Formulare und sonstigen Mitteilungen zukommen, die sie von der Zertifizierungsstelle gemäß den in diesem Handbuch festgelegten Verfahrensweisen erhalten hat.

3.3 Pflichten der TARGET2-Teilnehmer

Die Teilnehmer

1. beantragen Zertifikate gemäß den in diesem Handbuch festgelegten Verfahrensweisen,
2. beantragen die Sperrung und Reaktivierung sowie den Widerruf und die Erneuerung von Zertifikaten gemäß den in diesem Handbuch festgelegten Verfahrensweisen, wenn sich die Grundlage, auf der ein Zertifikat vergeben wurde, ändert bzw. nicht mehr existiert oder der Teilnehmer selbst seine Geschäftstätigkeit einstellt (z. B. infolge einer Fusion oder Liquidierung),
3. treffen alle Vorkehrungen und organisatorischen Maßnahmen, um sicherzustellen, dass die Zertifikate im Einklang mit den in diesem Handbuch festgelegten Regelungen verwendet werden,
4. setzen die Zertifizierungsstelle durch die kontoführende Zentralbank unverzüglich über sämtliche Änderungen der Informationen in Kenntnis, die zum Ausstellungszeitpunkt der Zertifikate in den Formularen vermerkt und für die Nutzung der Zertifikate relevant sind, und
5. stellen sicher, dass der Zertifikatsinhaber sich seiner im Nachfolgenden aufgeführten Pflichten bewusst ist und diesen nachkommt.

3.4 Pflichten des Zertifikatsinhabers

Der Inhaber eines Zertifikats ist gehalten, die sichere Aufbewahrung der Sicherheitsvorrichtungen (Smartcard [enthält das komplette Zertifikat einschließlich der Schlüssel/Token] und zugehörige/r PIN/PUK) zu gewährleisten und alle organisatorischen und technischen Maßnahmen zu ergreifen, um Dritte zu schützen und die personengebundene Verwendung der Sicherheitsvorrichtungen sicherzustellen.

Der Zertifikatsinhaber

1. stellt auch alle Informationen zur Verfügung, die von der kontoführenden Zentralbank angefordert werden und übernimmt die Verantwortung für deren Verlässlichkeit,
2. setzt die Zertifizierungsstelle durch die kontoführende Zentralbank über sämtliche Änderungen von Informationen in Kenntnis, die zum Zeitpunkt der Registrierung mitgeteilt wurden: persönliche Daten, Anschrift, Telefonnummern, E-Mail-Adresse usw.,
3. bewahrt die/das das Zertifikat enthaltende Smartcard/Token mit größter Sorgfalt und getrennt von den Passwörtern (PIN und PUK) auf, um die Integrität und maximale Vertraulichkeit zu gewährleisten,
4. nutzt die Zertifikate ausschließlich für die Funktionen oder Zwecke, für die sie ausgestellt wurden,
5. übermittelt Informationen über und Anträge auf Sperrung und Reaktivierung sowie Widerruf und Erneuerung eines Zertifikats gemäß den in diesem Handbuch festgelegten Verfahrensweisen,
6. beantragt unverzüglich die Sperrung der Zertifikate für die Schlüssel in Smartcards/Tokens, die defekt oder nicht mehr in seinem Besitz sind,
7. setzt die kontoführende Zentralbank über den Verlust oder Diebstahl der Sicherheitsvorrichtungen in Kenntnis.

4 BENUTZERIDENTIFIKATION UND REGISTRIERUNG

Im Folgenden wird das Verfahren für die erstmalige Vergabe von Zertifikaten einschließlich der Identifizierung des Antragstellers und der Registrierung beschrieben.

4.1 Ausfüllen des Antragsformulars

Personen, die ein Zertifikat beantragen, müssen von dem Kreditinstitut, in dessen Namen sie aufgrund eines Beschäftigungs- oder Vertretungsverhältnisses agieren, identifiziert und bevollmächtigt werden; die kontoführende Zentralbank garantiert die korrekte Identifizierung des Antragstellers gemäß den auf nationaler Ebene mit den Teilnehmern vereinbarten Regelungen.

Der Teilnehmer bestätigt, dass er die Inhalte dieses Handbuchs versteht, und sichert zu, seinen Pflichten nachzukommen.

Der designierte Empfänger (Zertifikatsinhaber) erstellt und unterzeichnet den Antrag, welcher Folgendes beinhaltet:

1. die Identifikationsdaten des Antragstellers (Zertifikatsinhabers) einschließlich einer eindeutigen Identifikationsnummer (z. B. Steuernummer oder Personalausweis-Nummer),
2. eine Erklärung des Antragstellers (Zertifikatsinhabers), in der dieser die Richtigkeit der gemachten Angaben bestätigt und versichert, etwaige Änderungen mitzuteilen,
3. eine Bestätigung des Antragstellers (Zertifikatsinhabers), dass er das Informationsschreiben über den Schutz persönlicher Daten empfangen hat,
4. eine Kopie eines gültigen Ausweisdokuments des Antragstellers (Zertifikatsinhabers) und
5. die Gegenzeichnung durch eine zur Genehmigung autorisierte Person beim Teilnehmer.

Die oben genannten Dokumente sind der kontoführenden Zentralbank vorzulegen.

4.2 Registrierung der Nutzer

Nach Durchführung der Prüfungen innerhalb ihres Zuständigkeitsbereichs leitet die kontoführende Zentralbank den Zertifikatsantrag an den SSP Service Desk weiter, welcher die für die Ausstellung der Zertifikate erforderlichen Daten im Registrationsarchiv eingibt.

Wird ein Antrag abgelehnt, setzt der SSP Service Desk die kontoführende Zentralbank darüber in Kenntnis, welche wiederum den Teilnehmer informiert.

4.3 Bereitstellung der Sicherheitsvorrichtungen

Die kontoführende Zentralbank übersendet die Umschläge mit einer Smartcard (einem USB-Token) und den Passwörtern (PIN, PUK)[2] nach Erhalt an die antragstellenden Teilnehmer zur Weiterleitung an die Antragsteller (Zertifikatsinhaber). Die kontoführende Zentralbank stellt dem entsprechenden Antragsteller (Zertifikatsinhaber) eine elektronische Fassung dieses Benutzerhandbuchs zur Verfügung.

Die Teilnehmer erstellen ein Übergabeprotokoll, das von der für die Lieferung an den Zertifikatsinhaber beim Teilnehmer verantwortlichen Person und vom Zertifikatsinhaber zu unterzeichnen ist.

Die Teilnehmer informieren die kontoführende Zentralbank darüber, dass die Zertifikate an den Zertifikatsinhaber geliefert wurden. Die kontoführende Zentralbank muss dem SSP Service Desk die Lieferung melden, damit das Zertifikat aktiviert werden kann.

5 VERFAHREN FÜR DIE VERGABE VON ZERTIFIKATEN

Ein Zertifikat ordnet den öffentlichen Schlüssel eines asymmetrischen Schlüsselpaars einem Datensatz zu, der den Inhaber des entsprechenden persönlichen Schlüssels (Zertifikatsinhaber) identifiziert.

Eine solche Zuordnung wird durch die Signatur der Zertifizierungsstelle durch ihren persönlichen Zertifizierungsschlüssel auf dem Zertifikat gewährleistet.

5.1 In den Zertifikaten enthaltene Informationen

Das Zertifikat enthält:

1. die Seriennummer oder eine andere Identifikationsnummer des Zertifikats,
2. den Namen der Zertifizierungsstelle mit Angabe des Landes, in dem ihr Sitz liegt,
3. die Identifikationsnummer des Inhabers bei der Zertifizierungsstelle,

[2] Die PIN muss für Signaturen und andere Vorgänge im Zusammenhang mit der Nutzung des zugehörigen Zertifikats eingegeben werden und ist vom Zertifikatsinhaber bei Erstverwendung zu ändern. Der PUK dient zur Entsperrung der Smartcard/des Token, wenn die PIN bei einer festgelegten Anzahl von Versuchen falsch eingegeben wurde.

4. Name, Nachname, eindeutige Identifikationsnummer und Geburtsdatum des Inhabers,
5. die Gültigkeitsdauer des Zertifikats,
6. die digitale Signatur der Zertifizierungsstelle,
7. die Nummer des öffentlichen Schlüssels,
8. die verwendbaren Generierungs- und Verifikationsalgorithmen,
9. den Algorithmus der Zertifikatsignatur und
10. den Typ des Schlüsselpaars entsprechend der jeweils vorgesehenen Verwendung.

Die Identifikation des Inhabers erfolgt gemäß ISO 9594-1 (1997) mittels des „Distinguished Name“ (DN, eindeutiger Name).

Die im Zertifikat enthaltenen persönlichen Daten dürfen ausschließlich zur Identifizierung des Inhabers im Zusammenhang mit Transaktionen genutzt werden, zu deren Durchführung er berechtigt ist.

Die Zertifizierungsstelle speichert die zertifikatsbezogenen Informationen für einen Zeitraum von mindestens zwanzig Jahren ab dem Ablauf- oder Widerrufsdatum des Zertifikats.

5.2 Gültigkeitsdauer der Schlüssel und der entsprechenden Zertifikate

Die den Inhabern ausgestellten Signaturzertifikate sind bis zu 5 Jahre gültig.

6 VERFAHREN FÜR DIE SPERRUNG UND DEN WIDERRUF VON ZERTIFIKATEN

Die Zertifizierungsstelle sperrt oder widerruft Zertifikate, indem sie die Seriennummer der betreffenden Zertifikate in die Liste der gesperrten bzw. widerrufenen Zertifikate einträgt.[3]

Die Sperrung bzw. der Widerruf ist ab dem Zeitpunkt der Aufnahme des betreffenden Zertifikats in die genannten Listen wirksam.

Bei Sperrung eines Zertifikats wird dessen Gültigkeit vorübergehend aufgehoben. Bei Widerruf eines Zertifikats endet dessen Gültigkeit vorzeitig.

6.1 Sperrung oder Widerruf von Zertifikaten

Der Inhaber eines Zertifikats oder der Teilnehmer kann die Sperrung eines Zertifikats oder dessen Widerruf aus den in Absatz 6.2 genannten Gründen beantragen.

[3] Die beiden Listen sind derzeit in Form einer einheitlichen Liste, in der sowohl gesperrte als auch widerrufene Zertifikate unter Angabe der verschiedenen „Gründe“ aufgeführt werden, zur Konsultation gestellt.

Die Zertifizierungsstelle kann Zertifikate nach entsprechender Benachrichtigung der Zertifikatsinhaber über den SSP Service Desk und die kontoführende Zentralbank sperren, wenn sie Kenntnis über einen mutmaßlichen Missbrauch, eine Fälschung oder Fahrlässigkeit erlangt. In Notfällen kann das Zertifikat vor Benachrichtigung des Zertifikatsinhabers gesperrt werden.

Im Fall von

- Verlust,
- Diebstahl oder
- Verletzung der Sicherheit der Smartcard oder des USB-Token

ist der Inhaber oder die teilnehmende Bank dazu verpflichtet, den National Service Desk der kontoführenden Zentralbank zu kontaktieren und die dringliche Sperrung bzw. den dringlichen Widerruf der Zugangsberechtigung für TARGET2 im „Identity and Access Management (IAM)“ zu veranlassen. Die National Service Desks sind in der Regel an allen TARGET2-Geschäftstagen von 6.30 Uhr bis 18.45 Uhr erreichbar. Möglicherweise davon abweichende nationale Öffnungszeiten sind bei der kontoführenden Zentralbank in Erfahrung zu bringen. Die kontoführende Zentralbank hat den SSP Service Desk unverzüglich zu informieren, damit dieser den jeweiligen Nutzer umgehend im IAM sperren oder dessen Berechtigung widerrufen kann.

Im Anschluss daran schickt der Teilnehmer das Antragsformular für die Sperrung oder den Widerruf des Zertifikats gemäß den auf lokaler Ebene festgelegten Verfahren an die kontoführende Zentralbank.

Nach Erhalt des Formulars prüft die kontoführende Zentralbank dessen Echtheit und initiiert das beantragte Verfahren durch Weiterleitung des Formulars an den SSP Service Desk. Dieser erfasst den Antrag im zertifizierten PKI-System und setzt die kontoführende Zentralbank über Datum und Uhrzeit des tatsächlichen Inkrafttretens des Widerrufs oder der Sperrung in Kenntnis.

Die kontoführende Zentralbank informiert den Inhaber und den Teilnehmer über die Sperrung oder den Widerruf des Zertifikats unter Angabe des Zeitpunkts (Datum und Uhrzeit), ab dem das Zertifikat nicht mehr gültig ist.

6.2 Gründe für die Sperrung oder den Widerruf von Zertifikaten

Der Inhaber eines Zertifikats oder der Teilnehmer kann die kontoführende Zentralbank aus den in nachfolgender Tabelle angeführten Gründen um Sperrung oder Widerruf eines Zertifikats ersuchen. Die Zertifizierungsstelle kann Zertifikate nach entsprechender Benachrichtigung der Zertifikatsinhaber über die kontoführende Zentralbank widerrufen, wenn sie Kenntnis über einen mutmaßlichen Missbrauch, eine Fälschung oder Fahrlässigkeit erlangt.

ANTRAGSTELLER GRUND	INHABER (externe Person oder Mitarbeiter)	Teilnehmende Bank
VERLUST DER SMARTCARD/DES TOKEN	X	X
DIEBSTAHL DER SMARTCARD/DES TOKEN	X	X
VERLETZUNG DER SICHERHEIT	X	X
BESCHÄDIGUNG DER SMARTCARD/DES TOKEN	X	X
ÄNDERUNG DER POSITION DES INHABERS[4]	--	X
SONSTIGES[5]	X	X

Bei Anträgen, in denen „Sonstiges“ angegeben ist, ist dies angemessen zu begründen.

Mit Ausnahme von Verlust oder Diebstahl ist der Inhaber verpflichtet, die sich in seinem Besitz befindliche Smartcard (oder das in seinem Besitz befindliche USB-Token) an den Teilnehmer zurückzugeben, nachdem er sie durch Zerschneiden des Chips unbrauchbar gemacht hat.

6.3 Reaktivierung gesperrter Zertifikate

Wird eine Sperrung beantragt, die Smartcard/das Token jedoch später wieder aufgefunden, kann die Reaktivierung des gesperrten Zertifikats beantragt werden. Bestätigt sich allerdings der Verlust, muss der Inhaber einen Antrag auf Widerruf stellen.

Der Antrag auf Reaktivierung ist gemäß dem oben beschriebenen Verfahren für Anträge auf Sperrung einzureichen.

Die Zertifizierungsstelle reaktiviert das Zertifikat durch Streichung von der Liste der gesperrten Zertifikate (Certificate Suspension List).

Die Zertifizierungsstelle setzt den Inhaber der Karte bzw. des Token und den Teilnehmer über die kontoführende Zentralbank von der Reaktivierung des Zertifikats und über den Zeitpunkt (Datum und Uhrzeit), ab dem das Zertifikat wieder gültig ist, in Kenntnis.

[4] Dieser Grund ist beispielsweise anzuführen, wenn der Inhaber seine Erwerbstätigkeit einstellt.
[5] Jegliche sonstigen Gründe, zum Beispiel Anträge auf Widerruf, die von Dritten, die infolge einer Fusion, Liquidierung usw. ihre Geschäfte einstellen, einzureichen sind.

6.4 Widerruf der Schlüsselzertifikate der Zertifizierungsstelle

Unter folgenden außergewöhnlichen Umständen werden die Zertifikate für das Zertifizierungsschlüssel-Paar, das in den internen Datenbanken gespeichert ist, von der Zertifizierungsstelle widerrufen:

1. Verletzung der Sicherheit des persönlichen Schlüssels, z. B. durch einen Vorfall, der die Verlässlichkeit seiner Sicherheitsmerkmale beeinträchtigt und
2. Einstellung der Tätigkeit.

Der Widerruf wird durch die Aufnahme des Zertifikats in die Liste der widerrufenen Zertifikate (Certificate Revocation List) umgesetzt.

Beruht der Widerruf auf einer Verletzung der Sicherheit des persönlichen Schlüssels der Zertifizierungsstelle, so widerruft die Zertifizierungsstelle in eigener Verantwortung alle mit diesem Schlüssel signierten Zertifikate.

7 VERFAHREN FÜR DIE ERNEUERUNG VON ZERTIFIKATEN

Die elektronischen Schlüssel sind fünf Jahre gültig.

Der Teilnehmer muss die kontoführende Zentralbank mittels des dafür vorgesehenen Formulars und gemäß den von der jeweiligen kontoführenden Zentralbank festgelegten Verfahren um die Ausgabe eines mit den ablaufenden Zertifikaten identischen Satzes von Zertifikaten ersuchen.

Die NZB leitet das Formular an den SSP Service Desk weiter, der anschließend die Sicherheitsvorrichtungen, die die neuen digitalen Zertifikate enthalten, an die kontoführende Zentralbank versendet.

Für die Bereitstellung und Entgegennahme erneuerter Zertifikate gelten die in Abschnitt 4.3 („Bereitstellung der Sicherheitsvorrichtungen“) genannten Regelungen.