In.Te.S.A. S.p.A.

Qualified Trust Service Provider

Verfahrenshandbuch für Remote-Verfahren für die qualifizierte elektronische Signatur im Bank- und Finanzwesen

Dokument-Nummer:

MO_REMBAN OID:

1.3.76.21.1.50.110

Verfasst von: Antonio Raia

Genehmigt durch: Franco Tafini

Ausstellungsdatum: 01.07.2019

Version: 04

VERSIONEN

Version Nr. 04		***Datum der Überarbeitung:***	***01.07.2019***
Beschreibung der Änderungen:	Änderung der Unternehmensdaten und des Logos Aktualisierung von Definitionen und Verweisen auf Rechtsvorschriften Überarbeitung des grafischen Layouts Einfügung des Verfahrens zur Unterzeichnung für potenzielle Kunden (I.2.3)		
Gründe:	Aktualisierungen bezüglich Rechtsvorschriften: Verordnung (EU) 910/2014 (eIDAS), italienische gesetzesvertretende Rechtsverordnung 179/2016 (DSGVO) Organisatorische Veränderungen des TSP Neues Kundenakquisitionsverfahren		
Version Nr. 03		***Datum der Überarbeitung:***	***13.06.2012***
Beschreibung der Änderungen:	Ausdehnung des Handbuchs auf das Finanzwesen (Zahlungsinstitute) und das Bankwesen		
Gründe:	Aktualisierung		
Version Nr. 02		***Datum der Überarbeitung:***	***02.04.2012***
Beschreibung der Änderungen:	B.4.2. - Einführung des Systems zur Erkennung der Identität des Inhabers (Due Diligence) ohne dessen persönliche Anwesenheit. C.5. - Einführung von Methoden des Systems zur Erkennung der Identität des Inhabers (Due Diligence). F.1.3. - Einfügung einer Standard-Anwendungsbeschränkung. G. - Einfügung der E-Mail-Kommunikationsmethode der operativen Bestätigungen.		
Gründe:	Aktualisierung		
Version Nr. 01		***Datum der Überarbeitung:***	***01.11.2011***
Beschreibung der Änderungen:	keine		
Gründe:	Erste Version		

Inhalt

Verweise auf Gesetze

Einheitstext - DPR 445/00 mit späteren Änderungen und Ergänzungen	Dekret des Präsidenten der Republik Nr. 445 vom 28. Dezember 2000. *„Einheitstext der gesetzlichen und regulatorischen Bestimmungen betreffend Verwaltungsunterlagen.“* Im Folgenden auch nur als TU bezeichnet.
CAD - italienische gesetzesvertretende Rechtsverordnung 82/05 mit späteren Änderungen und Ergänzungen	Gesetzesvertretende Rechtsverordnung Nr. 82 vom 7. März 2005 *„Italienischer Digitaler Verwaltungskodex“*. Im Folgenden auch nur als CAD bezeichnet.
Italienische Verordnung des Präsidenten des Ministerialrats vom 22.02.2013 *Neue Technische Regeln* mit späteren Änderungen und Ergänzungen	Italienische Verordnung des Präsidenten des Ministerialrats (DPCM) vom 22. Februar 2013 *„Technische Regeln betreffend die Generierung, Einfügung und Überprüfung fortgeschrittener elektronischer, qualifizierter und digitaler Signaturen gemäß den Artikeln 20, Absatz 3, 24, Absatz 4, 28, Absatz 3,* *32 Absatz 3, Buchstabe b), 35 Absatz 2, 36 Absatz 2 und 71“ (des CAD, Anmerk. d. V.).* Im Folgenden auch nur als *DPCM* bezeichnet.
EU-Verordnung Nr. 910/2014 (eIDAS-Verordnung) mit späteren Änderungen und Ergänzungen	Verordnung (EU) Nr. 910/2014 des Europäischen Parlaments und des Rates vom 23. Juli 2014 über elektronische Identifizierung und Vertrauensdienste für elektronische Transaktionen im Binnenmarkt und zur Aufhebung der Richtlinie 1999/93/EG. Im Folgenden auch nur als *eIDAS-Verordnung* bezeichnet.
DSGVO Datenschutzgrund-verordnung mit späteren Änderungen und Ergänzungen	Verordnung (EU) 2016/679 des Europäischen Parlaments und des Rates vom 27. April 2016 zum Schutz natürlicher Personen bei der Verarbeitung personenbezogener Daten, zum freien Datenverkehr und zur Aufhebung der Richtlinie 95/46/EG (Datenschutz-Grundverordnung) Im Folgenden auch nur als *DSGVO* bezeichnet.
BESCHLUSS Nr. 147/2019 mit späteren Änderungen und Ergänzungen	Richtlinien mit den technischen Vorschriften und Empfehlungen zur Generierung von qualifizierten elektronischen Zertifikaten, Unterschriften und qualifizierten elektronischen Siegeln sowie qualifizierten elektronischen Zeitstempeln. Im Folgenden auch nur als *DSGVO* bezeichnet.

Definitionen und Akronyme

AgID	*Agenzia per l’Italia Digitale* (Agentur für das Digitale Italien, ehemals CNIPA und DigitPA) - www.agid.gov.it. Aufsichtsorgan im Sinne der EU- Verordnung 910/2014 (eIDAS). Im Folgenden auch nur *Agentur*.
QTSP *Qualified Trust Service Provider Akkreditierter Zertifizierungsdienstea nbieter*	Qualifizierter Vertrauensdiensteanbieter. Natürliche oder juristische Person, die einen oder mehrere Vertrauensdienste anbietet. Auch *Zertifizierungsdiensteanbieter* im Sinne des CAD. In diesem Dokument ist der QTSP In.Te.S.A. S.p.A.
Qualifizierter Vertrauensdienst	Von einem QTSP bereitgestellter elektronischer Service, der die Elemente gemäß Artikel 3, Punkte 16) und 17) der Verordnung 910/2014 (eIDAS) umfasst. In diesem Dokument ist der QTSP In.Te.S.A. S.p.A.. Das Unternehmen stellt die Dienstleistungen Qualifizierte Elektronische Signaturerstellung und/oder Zeitstempel der Qualifizierten Signatur sowie andere mit diesen Leistungen verbundene Dienstleistungen bereit.
Qualifiziertes Zertifikat der elektronischen Signatur	Elektronische Bescheinigung zur Verknüpfung der Validierungsdaten einer elektronischen Signatur mit einer natürlichen Person und Bestätigung mindestens des Namens oder Pseudonyms dieser Person. Die Bescheinigung wird von einem qualifizierten Vertrauensdiensteanbieter ausgegeben und erfüllt die Anforderungen der Anlage I der EU- Verordnung 910/2014 (eIDAS).

Signaturschlüssel	Auf asymmetrischen Verschlüsselungsverfahren basierender Unterzeichnungsschlüssel, den der Inhaber verwendet, um unter ein elektronisches Dokument eine digitale Unterschrift zu setzen.
Öffentlicher Unterzeichnungs-schlüssel	Auf asymmetrischen Verschlüsselungsverfahren basierender Unterzeichnungsschlüssel, mit dem die digitale Unterschrift eines elektronischen Dokuments geprüft werden kann.
CRL	Eine Zertifikatsperrliste (englisch: certificate revocation list, CRL) ist eine Liste, die die Ungültigkeit von Zertifikaten beschreibt. Sie ermöglicht es, festzustellen, ob ein Zertifikat gesperrt oder widerrufen wurde, und warum.
OCSP	Das Online Certificate Status Protocol (OCSP) ist ein Netzwerkprotokoll, das es Clients ermöglicht, den Status von Zertifikaten bei einem Validierungsdienst abzufragen.
Elektronisches Dokument	Ein elektronisches Dokument enthält elektronisch dargestellte rechtserhebliche Akten, Fakten oder Daten.
QES - Qualifizierte elektronische Signatur *DS - Digitale Signatur*	Von einem Gerät für die Erstellung einer qualifizierten elektronischen Signatur erstellte elektronische Signatur, die auf einem qualifizieren Zertifikat für elektronische Signaturen basiert. Entspricht in Italien der *Digitalen Unterschrift* gemäß Definition im CAD, Artikel 1, Absatz 1, Punkt s): Qualifizierte elektronische Signatur auf der Grundlage eines Verschlüsselungssystems mit einem persönlichen und einem öffentlichen Signaturschlüssel, die miteinander verbunden sind. Der Inhaber kann mit dem persönlichen Signaturschlüssel und der Empfänger kann mit dem öffentlichen Signaturschlüssel die Herkunft und Unversehrtheit eines elektronischen Dokuments oder von mehreren elektronischen Dokumenten feststellen und überprüfen.
E-Signatur	Besonderes Verfahren der qualifizierten elektronischen Signatur oder der digitalen Signatur; die Signatur wird auf einem überwachten und verwalteten HSM unter der Verantwortung des Zertifizierungsdiensteanbieters generiert, wodurch die ausschließliche Kontrolle der persönlichen Schlüssel durch die Inhaber dieser garantiert werden kann.
HSM- Hardware-Sicherheitsmodul	Geräte für die Generierung der qualifizierten elektronischen Signatur, die die Anforderungen von Anlage II der EU-Verordnung 910/2014 erfüllen. Sie werden auch als *Signatur-Erstellungseinheiten* bezeichnet.
Qualified Electronic Time Stamp (Zeitstempel)	*Qualifizierter Zeitstempel zur elektronischen Validierung von Daten*; hierbei werden andere Daten in elektronischem Format mit einer bestimmten Uhrzeit oder einem Datum verknüpft, um die Existenz dieser Daten zum entsprechenden Zeitpunkt zu belegen. Erfüllt die Anforderung von Artikel 42 der eIDAS-Verordnung.
CA - Certification Authority	Behörde/öffentliche Stelle, die die Zertifikate für die elektronische Signatur erstellt.
RA- Registration Authority	*Registrierungsbehörde*: Stelle, die im Auftrag des QTSP für die Registrierung und Überprüfung der Informationen (insbesondere der Identität des Inhabers) zuständig ist, welche der QTSP für die Ausgabe der Qualifizierten Zertifikats benötigt.
Zertifikate-Register	Vom Zertifizierungsdiensteanbieter geführtes digitales Archiv, oder eine Kombination mehrerer Archive, aller ausgegebenen Zertifikate.
Antragsteller	Die natürliche Person, die ein Zertifikat beantragt.
Inhaber	Die natürliche Person, für die das Zertifikat ausgegeben wird und die für seine Nutzung autorisiert ist, um die eigene digitale Signatur unter ein Dokument zu setzen.
Kunde *Potenzieller Kunde*	Der Kunde (oder potenzielle Kunde, auch Prospect genannt) der Bank / des Finanzinstituts.
Zeitbezug	Information, die die Uhrzeit und das Datum enthält, die mit einem oder mehreren elektronischen Dokumenten assoziiert werden.
TSA- Time Stamping Authority	Für die Ausgabe der elektronischen Zeitstempel zuständige Stelle.

A. Einführung

Dieses Dokument stellt das Verfahrenshandbuch *für Remote-Verfahren für die qualifizierte elektronische Signatur im Bank- und Finanzwesen* (nachstehend *Verfahrenshandbuch* oder auch nur VH) des QTSP In.Te.S.A. S.p.A. dar.

Der Inhalt dieses Verfahrenshandbuchs entspricht den Technischen Regeln, die in der *Italienischen Verordnung des Präsidenten des Ministerialrats (DPCM) vom 22. Februar 2013 (*nachstehend *DPCM*) enthalten sind, sowie der *Gesetzesvertretenden Verordnung Nr. 82 vom 7. März 2005* die den *„Italienischen Digitalen Verwaltungskodex" mit seinen späteren Änderungen und Ergänzungen (nachstehend „CAD"*) enthält, und ist konform mit der *Verordnung (EU) 910/2014* (nachstehend *eIDAS-Verordnung*).

Soweit in diesem Verfahrenshandbuch nicht ausdrücklich vorgesehen, wird auf bestehende und künftige Vorschriften verwiesen, die den konkreten Sachverhalt regeln.

Dieses Dokument beschreibt die Regeln und operativen Verfahren des *QTSP In.Te.S.A. S.p.A.* (nachstehend *QTSP INTESA, Zertifizierungsdiensteanbieter* oder auch nur *INTESA*) für die Ausgabe der qualifizierten Zertifikate, die Generierung und Überprüfung der qualifizierten elektronischen Signatur sowie die Verfahren des Dienstes für den Zeitstempel der Qualifizierten Signatur im Einklang mit den geltenden Vorschriften für die Verwaltung dieser innerhalb von Bank- oder Finanzprojekten.

Für diese Art von Projekten fungieren die Bank- oder Finanzinstitute, die Homebanking-Dienste und Schalter-Anwendungen bereitstellen, auch als Local Registration Authority (nachstehend LRA) im Namen des QTSP INTESA. Im Folgenden werden diese Bank- oder Finanzinstitute als *Bank* oder *Zahlungsinstitut* (oder auch nur *Bank / Institut*) bezeichnet.

In diesem Kontext sind Inhaber eines Qualifizierten Zertifikats nur diejenigen Personen, welche von der Bank / dem Institut, das kraft einer spezifischen Vereinbarung mit dem QTSP INTESA zur Ausübung der Funktion der Registration Authority autorisiert ist, identifiziert werden.

Daher wird darauf hingewiesen, dass alle Verfahren zur Unterzeichnung von Dokumenten, die Gegenstand dieses Verfahrenshandbuchs sind, ausschließlich im Rahmen von Bank- oder Finanzanwendungen implementiert werden.

Die Ausübung der in diesem Verfahrenshandbuch beschriebenen Aktivitäten erfolgt im Einklang mit der Verordnung 910/2014 (eIDAS).

A.1. Geistiges Eigentum

Diese Betriebsanleitung ist alleiniges Eigentum der In.Te.S.A. S.p.A., die Inhaber aller entsprechenden geistigen Rechte ist.

Die hier beschriebenen Vorgaben für die Durchführung der QTSP-Aktivitäten sind durch Rechte auf geistiges Eigentum gedeckt.

A.2. Gültigkeit

Der Inhalt dieses Dokuments gilt für den QTSP INTESA (d. h. seine logistischen und technischen Infrastrukturen sowie seine Beschäftigten), für die Inhaber der vom QTSP ausgegebenen Zertifikate und für diejenigen, die diese Zertifikate auch unter Verwendung der vom QTSP INTESA ausgegebenen qualifizierten Zeitstempel nutzen, um die Authentizität und Unversehrtheit von mit einer qualifizierten elektronischen Signatur versehenen Dokumenten zu prüfen, sowie für die Bank / das Zahlungsinstitut in der Eigenschaft der Local Registration Authority.

Die Verwendung der Schlüssel und der zugehörigen ausgegebenen Zertifikate wird durch die Bestimmungen von Artikel 5, Absatz 4 des DPCM geregelt, wonach die Schlüssel für die Erstellung und Überprüfung der Signatur und die entsprechenden Dienstleistungen sich nach folgenden Arten unterscheiden:

a) Zeichnungsschlüssel zur Generierung und Überprüfung von in Dokumente eingefügten oder mit diesen assoziierten Signaturen;
b) Zertifizierungsschlüssel, die bestimmt sind für die Generierung und Überprüfung der Signaturen auf qualifizierten Zertifikaten, für Angaben zum Stand der Gültigkeit des Zertifikats oder für die

Unterzeichnung von Zertifikaten im Zusammenhang mit Zeitstempeln für die elektronische Validierung;

c) Zeitstempel-Schlüssel, die für die Generierung und Überprüfung von Zeitstempeln bestimmt sind.

B. Allgemeines

Zweck dieses Dokuments ist die allgemeine Beschreibung der Verfahren und entsprechenden Regeln für die Ausgabe qualifizierter Zertifikate durch den QTSP INTESA.

Die vorgenannten Regeln und Verfahren ergeben sich aus der Umsetzung der derzeitigen Bezugsnormen, deren Einhaltung es INTESA ermöglicht, im Verzeichnis der Zertifizierungsdiensteanbieter geführt zu werden.

Um den genannten Vorschriften zu entsprechen, müssen daher mehrere Einrichtungen involviert werden, die weiter unten im Dokument näher identifiziert werden.

B.1. Identifizierungsdaten der Version der Betriebsanleitung

Dieses Dokument stellt die Version Nr. *04* des *Verfahrenshandbuchs für Remote-Verfahren für die qualifizierte elektronische Signatur im Bank- und Finanzwesen* dar und wurde im Einklang mit Artikel des DPCM erstellt.

Der Object Identifier dieses Dokuments lautet **1.3.76.21.1.50.110**.

Diese Betriebsanleitung wird veröffentlicht und ist online abrufbar:

- auf der Internetseite des QTSP *https://www.intesa.it/e-trustcom/*
- auf der Internetseite der Agentur für das Digitale Italien *www.agid.gov.it*
- innerhalb der institutionellen Website der Bank / des Instituts.

Hinweis: Die Veröffentlichung von überarbeiteten Versionen dieses Verfahrenshandbuchs kann nur nach Genehmigung durch die Agentur für das Digitale Italien erfolgen.

B.2. Identifizierungsdaten des QTSP – Qualified Trust Service Provider

Der QTSP (Qualifizierter Vertrauensdiensteanbieter/Zertifizierungsdiensteanbieter) ist das Unternehmen ***In.Te.S.A. S.p.A.*** mit den nachstehend angeführten Identifizierungsdaten

Unternehmensname	**In.Te.S.A. S.p.A.**
Anschrift - Rechtssitz	**Strada Pianezza, 289 10151 Torino**
Gesetzlicher Vertreter	**Geschäftsführender Direktor**
Firmenregister Turin	**Eingetragen unter der Nummer 1692/87**
Umsatzsteuer-Identifizierungsnummer	**05262890014**
Telefonnummer (Vermittlung)	**+39 +39011.19216.111**
Website	**www.intesa.it**
E-Mail-Adresse	**marketing@intesa.it**
URL Zertifikate-Register	**ldap://x500.e-trustcom.intesa.it**
ISO Object Identifier (OID)	**1.3.76.21.1**

Das für die Zertifizierungstätigkeiten zuständige Personal umfasst im Einklang mit Artikel 38 des DPCM folgende Personen:

a) Leiter der Sicherheitsabteilung

b) Verantwortlicher des Dienstes für die Zertifizierung und die Zeitstempel der Qualifizierten Signatur

c) Verantwortlicher des technischen Betriebs der Systeme.

d) Verantwortlicher der technischen und logistischen Dienste.

e) Verantwortlicher der Kontrollen und Prüfungen (Auditing).

Alle vorgenannten Figuren gehören zur Organisation des QTSP INTESA.

B.3. Verantwortlicher des Verfahrenshandbuchs

Gemäß Artikel 40, Absatz 3, Buchstabe c) des DPCM ist die Certification Authority INTESA verantwortlich für dieses Verfahrenshandbuch und sorgt für seine Erstellung und Veröffentlichung.

INTESA freut sich über eventuelle Kommentare und Anfragen zu diesem Dokument, die an folgende Stellen gerichtet werden können:

E-Mail: *marketing@intesa.it*

Telefonisch:	+39 011.192.16.111
HelpDesk	Für Anrufe aus Italien: 800.80.50.93
	Für Anrufe aus dem Ausland: +39 02.871.193.396

B.4. An den Verfahren beteiligte Instanzen

Innerhalb der Struktur des QTSP werden Instanzen identifiziert, die an den entsprechenden Verfahren für die Ausgabe der Zertifikate beteiligt sind.

Diese Akteure handeln im Einklang mit den Regeln und Verfahren des QTSP, indem sie die ihnen übertragenen Aufgaben im Rahmen ihrer Zuständigkeit wahrnehmen.

B.4.1. Certification Authority (CA)

INTESA handelt im Einklang mit den Bestimmungen des DPCM, CAD und der eIDAS-Verordnung und nimmt die Aktivitäten als Qualified Trust Service Provider wahr. Diese Aktivitäten umfassen die qualifizierten Vertrauensdienste für die Erstellung, Überprüfung und Validierung elektronischer Signaturen, elektronischer Siegel oder Zeitstempel.

Die Identifizierungsdaten des QTSP INTESA sind im vorherigen Abschnitt *B.2* aufgeführt.

B.4.2. Local Registration Authority (LRA)

Für die besondere Art der angebotenen und in diesem Verfahrenshandbuch beschriebenen Dienstleistung (qualifizierte E-Signatur im Bereich von Bank- und Finanzanwendungen) überträgt der QTSP INTESA die Ausübung der Funktionen an die Registration Authority und die Bank / das Institut, die den Dienst erworben haben.

Die LRA verpflichtet sich zur Ausübung der folgenden Tätigkeiten:

- Identifizierung des Inhabers;
- Registrierung des Inhabers.

Die Bank / das Institut muss bei der Erfüllung der Funktion der Registration Authority dafür sorgen, dass die Maßnahmen zur Identifizierung vorschriftsmäßig und im Einklang mit den Vorgaben dieses Verfahrenshandbuchs ablaufen.

Insbesondere kann die Bank / das Institut im Einklang mit den Vorschriften zur Bekämpfung von Geldwäsche den Inhaber identifizieren (*Due Diligence*), auch wenn dieser nicht persönlich in einer Filiale erscheint.

In einem solchen Fall muss die Bank / das Institut:

- die Identität mittels Dokumenten, Daten oder zusätzlichen Informationen wie öffentlichen Urkunden, beglaubigten Privatschriften, für die Erstellung einer qualifizierten elektronischen Signatur in Verbindung mit elektronischen Dokumenten verwendeten Zertifikaten oder mit Hilfe einer Erklärung der italienischen Konsularbehörden sicherstellen;
- ergänzende Maßnahmen zur Überprüfung der vorgelegten Dokumente ergreifen, beispielsweise die Zertifizierung der Bestätigung eines unter die Richtlinie fallenden Kredit- oder Finanzinstituts;

- die Unterlagen verwenden, die belegen, dass der Deckungsbericht von einem auf den Kunden eingetragenen Konto stammt.

C. Pflichten

C.1. Pflichten des Qualifizierten Vertrauensdiensteanbieters (QTSP)

Bei der Ausübung seiner Aktivität handelt der Qualifizierte Vertrauensdiensteanbieter (*Zertifizierungs-diensteanbieter*) im Einklang mit den Bestimmungen:

- der Gesetzesvertretenden Rechtsverordnung Nr. 82 vom 7. März 2005 und ihren späteren Änderungen
- der Italienischen Verordnung des Präsidenten des Ministerialrats (DPCM) vom 22. Februar 2013
- der EU-Verordnung 2016/679 (DSGVO)
- der Verordnung 910/2014 (eIDAS).

Der QTSP:

- ergreift alle organisatorischen und technischen Maßnahmen, die geeignet sind, Schaden Dritter zu vermeiden;
- hält die im DPCM mit seinen späteren Änderungen und Ergänzungen spezifizierten technischen Regeln ein;
- garantiert die Konformität des eigenen Qualitätssystems mit den Normen ISO 9001;
- gewährleistet, dass die Signaturerstellungseinheit (HSM) die vorgesehenen Sicherheitsanforderungen gemäß Artikel 29 der eIDAS-Verordnung erfüllt;
- gibt das qualifizierte Zertifikat aus und veröffentlicht es im Einklang mit den Vorgaben von Artikel 32 des CAD, sofern der Inhaber nichts anderes festgelegt hat;
- informiert die Antragsteller auf deutliche und klare Weise über das Zertifizierungsverfahren, die entsprechenden erforderlichen technischen Voraussetzungen, die Eigenschaften und die Nutzungsbeschränkungen der ausgegebenen Signaturen basierend auf dem Zertifizierungsdienst;
- befolgt die Sicherheitsmaßnahmen für die Verarbeitung personenbezogener Daten (DSGVO);
- macht sich nicht zum Verwahrer von Daten für die Erstellung der Signatur des Inhabers;
- veröffentlicht bei einer entsprechenden Anfrage des Inhabers oder des beteiligten Dritten den Widerruf und die Aussetzung des elektronischen Zertifikats;
- gewährleistet die präzise Bestimmung des Datums und der Uhrzeit der Ausgabe, des Widerrufs sowie der Aussetzung der elektronischen Zertifikate;
- führt 20 (zwanzig) Jahre lang ein Register, auch in elektronischer Form, aller Informationen betreffend das qualifizierte Zertifikat, insbesondere zu dem Zweck, im Fall eventueller gerichtlicher Verfahren einen Beweis für die Zertifizierung vorlegen zu können;
- ☐ stellt sicher, dass die jedem Inhaber zugeordnete Identifizierungsnummer (die ausschließlich vom QTSP stammt) innerhalb des eigenen Benutzerkreises einmalig ist;
- stellt mit nachhaltigen Kommunikationsmitteln alle nützlichen Informationen für diejenigen Personen bereit, die einen Zertifizierungsdienst beantragen. Hierzu gehören: die genauen Geschäftsbedingungen für die Nutzung des Zertifikats, einschließlich aller Nutzungsbeschränkungen, die Existenz eines freiwilligen Akkreditierungssystems sowie die Verfahren für Beschwerden und die Auflösung von Streitigkeiten. Diese Informationen, die elektronisch übermittelt werden können, müssen in klarer Sprache verfasst und vor der Einigung zwischen dem Antragsteller und dem QTSP bereitgestellt werden;
- verwendet zuverlässige Systeme für die Verwaltung des Zertifikate-Registers mit Methoden, die garantieren, dass nur autorisierte Personen Daten eingeben und ändern können, dass die Authentizität der Informationen überprüfbar ist, dass die Zertifikate nur in den vom Inhaber des Zertifikats genehmigten Fällen der Öffentlichkeit zur Einsichtnahme zugänglich sind und dass der Betreiber erkennen kann, wenn Ereignisse eintreten, die die Sicherheitsauflagen gefährden;
- registriert die Ausgabe der qualifizierten Zertifikate im Prüfungsbuch mit Angabe von Datum und

Uhrzeit der Generierung.

Gemäß den Bestimmungen von Artikel 14 des DPCM stellt der Zertifizierungsdienstanbieter mindestens ein System bereit, oder benennt dieses, welches die Durchführung der Überprüfung der digitalen Signaturen ermöglicht.

Ferner hat der QTSP folgende Aufgaben:

- Generierung eines qualifizierten Zertifikats für jede von der Agentur für das Digitale Italien für die Unterzeichnung des öffentlichen Verzeichnisses der Zertifizierungsanbieter verwendete fortgeschrittene elektronische Signatur und Veröffentlichung dieses Zertifikats im eigenen Zertifikate-Register gemäß Artikel 42 des DPCM;
- Verweis auf ein System zur Überprüfung der elektronischen Signatur gemäß Artikel 10 des DPCM;
- Verwahrung einer Kopie der von der Agentur für das Digitale Italien unterzeichneten Liste der Zertifikate für die Zertifizierungsschlüssel gemäß Artikel 43 des DPCM und Gewährleistung der Zugänglichkeit auf elektronischem Weg gemäß den Bestimmungen von Artikel 42, Absatz3 des DPCM.

C.2. Pflichten des Inhabers

Der antragstellende Inhaber eines qualifizierten Zertifikats für die in diesem Verfahrenshandbuch beschriebenen Dienste ist ein Kunde der Bank oder des Zahlungsinstituts, die jeweils als Registration Authority fungieren.

Der Inhaber wird ein qualifiziertes Zertifikat für die qualifizierte E-Signatur erhalten, mit der er Verträge und Unterlagen im Zusammenhang mit von der Bank /dem Institut angebotenen Erzeugnissen und/oder Dienstleistungen auf die in Abschnitt ... beschriebene Weise unterzeichnen kann.

Der Inhaber muss die für die Verwendung seines eigenen Signaturschlüssels notwendigen Informationen auf angemessene Weise aufbewahren und alle geeigneten organisatorischen und technischen Maßnahmen ergreifen, um Schäden für Dritte zu vermeiden (CAD, Artikel 32, Absatz 1).

Darüber hinaus muss der Inhaber:

- unter eigener Verantwortung alle vom QTSP angeforderten Informationen bereitstellen und deren Zuverlässigkeit garantieren;
- den Zertifizierungsantrag auf die in diesem Verfahrenshandbuch angegebene Weise weiterleiten;
- dem QTSP, auch durch die LRA, eventuelle Veränderungen der bei der Registrierung übermittelten Informationen mitteilen: persönliche Daten, Wohnort, Telefonnummern, E-Mail-Adresse usw.;
- die Informationen für die Aktivierung des Signaturschlüssels für die Nutzung gewissenhaft und mit größter Sorgfalt aufbewahren;
  - bei Verlust oder Diebstahl der Codes und/oder Geräte für den Zugang zu den eigenen Signaturschlüsseln sofort bei den zuständigen Behörden und der Bank/Institut Meldung erstatten; die Bank / das Institut wird unverzüglich für den Widerruf des Zertifikats sorgen;
- eventuelle Anträge auf Widerruf oder Aussetzung des qualifizierten Zertifikats im Einklang mit den Angaben in diesem Verfahrenshandbuch weiterleiten.

C.3. Pflichten der Benutzer der Zertifikate

Benutzer (*Relying Party*) ist jede Person, die ein Dokument mit einer digitalen Unterschrift erhält und zwecks Überprüfung der Gültigkeit der Unterschrift auf das vom Inhaber beim Unterzeichnen des Dokuments verwendete Qualifizierte Zertifikat zurückgreift.

Die Überprüfung der digitalen Unterschrift und das anschließende Extrahieren der unterzeichneten Objekte können mit jeder beliebigen Software ausgeführt werden, die in der Lage ist, unterzeichnete Dokumente im Einklang mit der eIDAS-Verordnung zu verarbeiten.

Personen, die zur Überprüfung der Gültigkeit eines Dokuments mit einer digitalen Unterschrift Gebrauch von einem Qualifizierten Zertifikat machen, müssen:

- gemäß den zum Zeitpunkt der Emission des Zertifikats geltenden Normen die Gültigkeit des Zertifikats überprüfen, welches den öffentlichen Signaturschlüssel des unterzeichnenden Inhabers der Nachricht enthält;
- den Gültigkeitsstatus des Zertifikats mithilfe des OCSP-Protokolls oder durch Zugriff auf die Zertifikatssperrlisten überprüfen;
- die Gültigkeit des Zertifizierungsverfahren basierend auf der öffentlichen Liste der QTSP überprüfen;
- das Vorhandensein möglicher Nutzungsbeschränkungen für das vom Inhaber verwendete Zertifikat überprüfen.

C.4. Pflichten des beteiligten Dritten

Der an den in diesem Verfahrenshandbuch beteiligte Dritte ist die Bank oder das Zahlungsinstitut. Daher muss die Bank / das Institut in der Eigenschaft als beteiligter Dritter:

- überprüfen, dass der Kunde im Besitz aller erforderlichen Voraussetzungen ist, und den Kunden autorisieren, die Ausgabe des Qualifizierten Zertifikats für die E-Signatur zu beantragen;
- dem Inhaber Support-Leistungen bereitstellen;
- dem QTSP eventuelle weitere Nutzungsbeschränkungen des Qualifizierten Zertifikats für die digitale Unterschrift mitteilen, die über diejenigen hinaus gelten, die gemäß Par. *F.1.1* vorgesehen sind.

Folglich kann die Bank / das Institut in der Eigenschaft als beteiligter Dritter den QTSP über eventuelle Nutzungsbeschränkungen für das Zertifikat und eventuelle Vertretungsbefugnisse unterrichten und muss ihn über jegliche Veränderung dieser in Kenntnis setzen. Im Folgenden werden hierfür einige Beispiele angeführt:

- Änderung oder Aufhebung der Vertretungsbefugnisse;
- Änderung der internen Rollen und Qualifikationen;
- Beendigung des Abhängigkeitsverhältnisses.

Der bei der LRA eingegangene Antrag auf Widerruf oder Aussetzung seitens des beteiligten Dritten muss sofort an die CA weitergeleitet werden, wenn die Voraussetzungen, auf deren Grundlage dem Inhaber ein qualifiziertes Zertifikat für die elektronische Signatur ausgegeben worden war, nicht mehr erfüllt werden.

C.5. Pflichten der externen Registration Authority (LRA)

Der QTSP INTESA greift bei Bedarf im Zusammenhang mit der Bereitstellung des Dienstes im gesamten Landesgebiet auf weitere Personen (nachstehend externe RA oder LRA - Local Registration Authority- genannt) zurück, um einen Teil der Aktivitäten des Registrierungsbüros auszuüben.

Der QTSP In.Te.S.A. S.p.A. überträgt durch einen spezifischen, von beiden Seiten unterschriebenen *Mandatsvertrag* die Ausübung der Funktionen der Registration Authority an die Bank oder das Zahlungsinstitut.

Im Einzelnen führen die externen RA die folgenden Aktivitäten aus:

- eindeutige Identifizierung des Antragstellers der Zertifizierung (nachstehend Inhaber des Zertifikats);
- Registrierung des Antragstellers / Inhabers;
- Aushändigung an den Inhaber der Geräte und/oder Codes, mit denen er im Einklang mit Artikeln 8 und 10, Absatz 2 des DPCM auf seinen Signaturschlüssel zugreifen kann;
- Senden der unterzeichneten Unterlagen an das RA-Büro des QTSP INTESA, es sei denn, im Mandatsvertrag wurden andere Vereinbarungen festgelegt.

Der Mandatsvertrag legt im Einzelnen die Pflichten fest, welche die Bank /das Institut, in ihrer Eigenschaft als vom QTSP INTESA beauftragte LRA erfüllen und deren Einhaltung der QTSP überwachen muss.

Insbesondere hat die LRA folgende Aufgaben:

- Sicherstellung, dass die Identifizierung im Einklang mit den geltenden Rechtsvorschriften erfolgt (CAD mit späteren Änderungen und Ergänzungen, DPCM, eIDAS-Verordnung sowie Regelungen und Vorschriften zur Bekämpfung von Geldwäsche);
- Nutzung und Verarbeitung der für die Anerkennung erhobenen personenbezogenen Daten im Einklang mit der DSGVO;
- Bereitstellung des bei der Identifizierung und Registrierung erfassten Materials für den QTSP INTESA.

Die Identifizierung (Due Diligence) kann auf drei unterschiedliche Weisen durchgeführt werden, und zwar:

- *Standard*: Der Antragsteller wird in einer Filiale der Bank oder des Zahlungsinstituts identifiziert;
- *On Demand*: Bei der Eröffnung eines neuen Kontos kann der Antragsteller um Kontaktaufnahme durch einen *Personal Financial Adviser* bitten; dieser begleitet nach Festlegung eines Termins den Kunden bei allen für die Eröffnung eines Kontos notwendigen Schritten. In dieser Phase wird der Kunde (nach seiner Identifizierung und Registrierung) auch bei der Beantragung eines Zertifikats für die elektronische Signatur unterstützt.
- *Online*: Wählt der Antragsteller hingegen die direkte Beitrittsmethode und besitzt bereits ein Konto bei einer Bank im Landesgebiet kann er zu seiner rechtmäßigen Identifizierung:
  - eine SEPA- (oder SDD - SEPA Direct Debit)-Prozedur anwenden;
  - von seinem bereits bei einer Bank eröffneten Konto eine Kontoüberweisung anweisen.

Durch die oben genannten Verfahren erhält die LRA der Bank oder des Zahlungsinstituts alle gesetzlich vorgeschriebenen Informationen auf vollkommen sichere Weise und unter uneingeschränkter Wahrung der Privatsphäre.

D. Haftung und Beschränkung von Entschädigungszahlungen

D.1. Haftung des QTPS P – Beschränkung von Entschädigungszahlungen

Der QTSP INTESA haftet gegenüber den Inhabern für die Erfüllung aller Verpflichtungen, die sich aus der Durchführung der vom DPCM, der DSGVO, dem CAD und der eIDAS-Verordnung (und ihrer späteren Änderungen und Ergänzungen) vorgesehenen Tätigkeiten ergeben, wie sie im Abschnitt *C.1 Pflichten des Qualifizierten Vertrauensdiensteanbieters (QTSP)* beschrieben sind.

Außer bei Vorsatz oder Verschulden (Artikel 13 eIDAS-Verordnung) haftet INTESA in keinem Fall für die Folgen, die sich aus einer anderen als durch Artikel 5 des DPCM vorgesehenen Nutzung ergeben, und insbesondere aus der Nichteinhaltung seitens des Inhabers oder des beteiligten Dritten der Vorgaben dieses Verfahrenshandbuchs und/oder der geltenden Rechtsvorschriften.

Gleichermaßen kann INTESA nicht für die Folgen haftbar gemacht werden, die auf nicht durch INTESA verschuldete Ursachen zurückzuführen sind, wie zum Beispiel: Naturkatastrophen, Betriebsstörungen und/oder technische und logistische Störungen außerhalb der eigenen Kontrolle, Eingriffe von Behörden, Unruhen oder Kriegshandlungen, die auch oder nur diejenigen Personen treffen, auf deren Aktivitäten INTESA für die Bereitstellung der eigenen Zertifizierungsdienste zurückgreift.

Der QTSP INTESA haftet nicht für Schäden, die auf eine nicht konforme Nutzung des Qualifizierten Zertifikats für die e-Signatur in Verbindung mit den in Abschnitt *F.1.1* genannten Nutzungsbeschränkungen zurückzuführen sind.

Der Inhaber muss nach Kenntnisnahme dieses Verfahrenshandbuchs alle Due-Diligence-Maßnahmen ergreifen, die sicherstellen, dass Dritten keine Schäden in Verbindung mit einer unsachgemäßen Nutzung des vom Zertifizierungsdiensteanbieter bereitgestellten Services entstehen. Insbesondere wird daran erinnert, dass die OTP-Geräte sowie die geheimen Codes, die für den Zugriff auf die Signaturschlüssel unerlässlich sind, mit der nötigen Sorgfalt verwahrt werden müssen.

D.2. Versicherung

Der QTSP INTESA ist der Begünstigte von Versicherungsverträgen zur Deckung von Dritten verursachten Geschäfts- und Schadensrisiken, deren Inhalt den Anforderungen für die Ausübung der entsprechenden beruflichen Tätigkeit entspricht.

Eine Erklärung über den Abschluss dieses Versicherungsvertrags wird an die AgID gesendet.

E. Gebühren

Die Bank oder das Zahlungsinstitut stellt den eigenen Kunden den Dienst gegen Bezahlung bereit: die Gebühren für die Ausgabe, die Verlängerung, den Widerruf und die Aussetzung des qualifizierten Zertifikats werden in den zwischen Kunde und Bank / Institut aufgesetzten Verträgen festgelegt.

F. Identifizierungs- und Registrierungsmethoden der Benutzer

F.1. Identifizierung der Benutzer

Der QTSP muss bei der ersten Beantragung der Ausgabe eines qualifizierten Zertifikats die Identität des Antragstellers eindeutig sicherstellen.

Dieser Vorgang wird der Bank /dem Institut übertragen, welche(s) als LRA und im Einklang mit den Bestimmungen der geltenden Vorschriften zur Bekämpfung von Geldwäsche den Inhaber identifiziert und registriert.

Für spätere Verlängerungen muss dieser Vorgang nicht wiederholt werden, sofern die Verlängerung erfolgt, während das qualifizierte Zertifikat noch gültig ist: Der Inhaber muss den QTSP durch die Bank /das Institut über eventuelle Änderungen seiner Registrierungsdaten unterrichten.

Für die Erbringung des Dienstes, der Gegenstand dieses Dokuments ist, sind unter anderem folgende Registrierungsdaten notwendig:

- Vor- und Nachname;
- Geburtsdatum;
- Geburtsort (italienische Stadt oder ausländischer Staat);
- Steuernummer;
- Wohnanschrift;
- Anschrift, an die die Schriftstücke gesendet werden;
- Mobiltelefonnummer;
- E-Mail-Adresse:
- Art und Nummer des vorgelegten Ausweises;
- Ausstellende Behörde des Ausweises, Ausgabeort -und -datum sowie Ablaufdatum.

Am Ende dieser Registrierungsphase kann dem Inhaber als kostenlose Leihgabe ein „One Time Password“-Gerät überlassen werden, das ein Display hat und Zahlencodes zur einmaligen Verwendung generieren kann (nachstehend *OTP-Codes* oder einfach *OTPs* genannt).

Alternativ zum OTP-Gerät kann die Bank oder das Zahlungsinstitut dem Inhaber erklären, wie er ein Software-Authentifizierungssystem für mobile Geräte aktivieren kann (falls der Inhaber ein solches Gerät besitzt oder diese Methode der Verwendung eines OTP-Geräts zur Generierung von Tokens vorzieht). Dieses Software-System ermöglicht die Generierung eines einmaligen Passworts auf dem mobilen Gerät des Inhabers und kann daher als Instrument zur Authentifizierung von E-Signatur-Systemen eingesetzt werden.

Zusammen mit dem OTP erhält der Inhaber alle notwendigen Informationen sowie eine *Personal Identification Number* (*PIN*), die ihm einen sicheren Zugang zum E-Signatur-Dienst garantieren können, der ihm von der Bank / dem Institut angeboten wird.

Die gleiche PIN kann als Notfall-Code (beispielsweise bei Verlegen und/oder Verlust des Token OTP oder des

mobilen Geräts) verwendet werden, um das auf ihn ausgegebene qualifizierte Zertifikat schnellstens auszusetzen (Abschnitt *H.2.2*).

Der Inhaber kann die PIN später ändern oder aktualisieren, indem er die Dienste nutzt, die ihm die Bank oder das Zahlungsinstitut zur Verfügung stellt.

In dieser Phase werden dem Inhaber auch die erforderlichen Informationen bereitgestellt, die ihm ermöglichen, seine zuvor übermittele Mobiltelefonnummer jederzeit zu ändern.

Darüber hinaus muss der Inhaber, direkt am Schalter der Bank / des Instituts oder über den von der Bank /dem Institut angebotenen Online-Banking-Dienst, jedoch in jedem Fall vor der Beantragung der Ausgabe eines qualifizierten Zertifikats:

- das Verfahrenshandbuch des QTSP INTESA lesen;
- die Bank oder das Zahlungsinstitut zur Verarbeitung seiner personenbezogenen Daten für die mit der Ausgabe eines qualifizierten Zertifikats für die elektronischen Signatur verbundenen Zwecke autorisieren.

Die vorgenannten Unterlagen in Verbindung mit der Registrierung der Inhaber werden für die Dauer von 20 (zwanzig) Jahren ab dem Ablauf des Zertifikats aufbewahrt.

F.1.1. Nutzungsbeschränkungen

Für das qualifizierte Zertifikat für die E-Signatur, das im Rahmen der in diesem Verfahrenshandbuch beschriebenen und von der Bank /dem Institut angebotenen Dienste ausgegeben wird, gilt stets eine Nutzungsbeschränkung.

Die Standardformel lautet wie folgt:

Dieses Zertifikat darf nur in Beziehungen mit Name der Bank / des Instituts verwendet werden.

This certificate may only be used in dealings with Nome Banca / Istituto.

Spezielle Nutzungsbeschränkungen können mit der Bank oder dem Zahlungsinstitut vereinbart werden.
INTESA haftet nicht für durch die Nutzung eines qualifizierten Zertifikats entstandenen Schaden, der die darin festgelegten Grenzen überschreitet, oder für Schäden, die aus einer Überschreitung dieser Grenzen resultieren.

F.1.2. Berufsbezogene Angaben und berufliche Qualifikationen

Falls im qualifizierten Zertifikat berufliche Befähigungsnachweise anzugeben sind (z. B. die Zugehörigkeit zu einem Berufsverband), muss der Antragsteller geeignete Unterlagen als Beweis für das tatsächliche Vorhandensein dieser Befähigungsnachweise oder gleichwertige Unterlagen vorlegen.

Eine Kopie dieser Unterlagen wird für die Dauer von 20 (zwanzig) Jahren ab dem Ablauf des Zertifikats aufbewahrt.

Die Unterlagen zur Unterstützung der beantragten Einfügung von berufsbezogenen Angaben und beruflichen Qualifikationen in das qualifizierte Zertifikat dürfen nicht mehr als 10 (zehn) Tage vor dem Datum der Vorlage des Ausgabeantrags des Zertifikats erstellt worden sein.

INTESA haftet nicht für Schäden, die auf eine unlautere Nutzung eines qualifizierten Zertifikats mit Informationen betreffend berufliche Qualifikationen zurückzuführen sind.

Außer bei Vorsatz oder Verschulden (Artikel 13 eIDAS-Verordnung) haftet INTESA im Fall einer Selbstbescheinigung nicht für die Einfügung von durch den Inhaber selbst bescheinigten Angaben in das Zertifikat.

F.1.3. Vertretungsbefugnisse

Falls im qualifizierten Zertifikat Vertretungsbefugnisse anzugeben sind (z. B. die Zugehörigkeit zu einem Unternehmen und die dort gehaltene Position, die Befugnis, im Namen und für einen Kunden zu handeln usw.), muss der Antragsteller geeignete Unterlagen als Beweis für das tatsächliche Vorhandensein dieser Vertretungsbefugnisse vorlegen.

Für die Vertretung natürlicher Personen muss der Antragsteller eine beglaubigte Kopie der von der vertretenen Person unterschriebene Befugnisübertragung oder eine beglaubigte Vollmacht zusammen mit der schriftlichen

Einwilligung der beglaubigten Person zur Einfügung der Rolle in das Zertifikat vorlegen.

Falls im qualifizierten Zertifikat eine Rolle bei der Vertretung privatrechtlicher Organisationen oder Einrichtungen anzugeben ist, muss der Antragsteller geeignete Unterlagen vorlegen, die die Rolle belegen, die in das Zertifikat eingefügt werden soll, sowie eine Erklärung der entsprechenden Organisation oder Einrichtung, mit der die Organisation oder Einrichtung den QTSP für die Einfügung einer spezifischen Rolle in das Zertifikat autorisiert. Dieses letzte Dokument darf nicht mehr als 20 (zwanzig) Tage vor dem Datum der Vorlage des Ausgabeantrags für das qualifizierte Zertifikat erstellt worden sein.

Die Einfügung in das qualifizierte Zertifikat von Informationen über die Wahrnehmung öffentlicher Aufgaben oder Vertretungsbefugnisse in Einrichtungen oder Organisation des öffentlichen Rechts ist an besondere Vereinbarungen mit den betreffenden Einrichtungen gebunden. Basierend auf solchen Vereinbarungen kann die Rolle des Inhabers in der öffentlichen Organisation oder Einrichtung angegeben werden.

Die vorgelegten Unterlagen werden für einen Zeitraum von 20 (zwanzig) Jahren aufbewahrt.

INTESA haftet nicht für Schäden, die auf eine unlautere Nutzung eines qualifizierten Zertifikats mit Informationen betreffend Vertretungsbefugnisse zurückzuführen sind.

F.1.4. Verwendung von Pseudonymen

In besonderen Fällen kann der Inhaber beantragen, dass das Zertifikat anstelle seiner realen persönlichen Daten ein Pseudonym anführt.

Die Informationen über die tatsächliche Identität des Benutzers werden für einen Zeitraum von 20 (zwanzig) Jahren aufbewahrt.

F.2. Registrierung der Benutzer, die eine Zertifizierung beantragen

Nach der Identifizierung des Inhabers werden die Daten des Inhabers in den Archiven der Certification Authority registriert.

Diese Registrierung kann mithilfe einer Softwareanwendung, die direkt von den Anwendungen der Bank oder des Zahlungsinstituts aufgerufen werden kann, ausgeführt werden.

G. Generierung der Schlüssel für die Zertifizierung, den Zeitstempel und die Unterzeichnung

G.1. Generierung der Zertifizierungsschlüssel

Die Generierung der Schlüssel in den Signatur-Geräten erfolgt in Anwesenheit des Zertifizierungsverantwortlichen gemäß Artikel 7 des DPCM.

Dem Vorgang geht eine Initialisierung der Signatur-Geräte für das System der Generierung der Zertifikate voraus, mit denen die Zertifikate der Inhaber und die des Zeitstempel-Systems unterzeichnet werden.

Alles wird nach dem Vier-Augen-Prinzip kontrolliert, um gesetzwidrige Vorgänge zu verhindern.

Die auf die Generierung der Signaturschlüssel-Paare des Zertifizierungsdiensteanbieters folgenden Vorgänge sind nur mittels spezieller Geräte für die Autorisierung (token usb) möglich: Der privilegierte Zugriff auf die HSM kann nur mit den in den vorgenannten Geräten für die Autorisierung enthaltenen Schlüsseln ausgeführt werden.

Zur Erhöhung der Sicherheit werden diese Schlüssel mit einer Logik der Art *„n von m“* auf mehrere Geräte aufgeteilt, so dass nur die gleichzeitige Präsenz von mindestens *n* von *m* Teilen des Schlüssels ein Vorgehen mit den entsprechenden Privilegien zulässt. Dementsprechend werden sie in speziellen gesonderten Safes aufbewahrt.

Die Zertifizierungsschlüssel haben eine Länge von mindestens 2048 Bit.

G.2. Generierung der Schlüssel für das Zeitstempel-System

Die Generierung der Zeitstempel erfolgt im Einklang mit den Bestimmungen von Artikel 49 des DPCM. Die Schlüssel des Zeitstempel-Systems haben eine Länge von mindestens 2048 Bit.

G.3. Generierung der Signaturschlüssel

Nach der Generierung, während der die Daten des Inhabers in den Archiven des Zertifizierungsdiensteanbieters gespeichert werden, kann die Generierung der Signaturschlüssel in die Wege geleitet werden.

Der Inhaber kann das Verfahren für die Generierung der Schlüssel und die Beantragung des mit den Schlüsseln assoziierten Signatur-Zertifikats auf der der im Abschnitt *I. Verfahrensabläufe für die Unterzeichnung der Dokumente* beschriebene Weise beginnen.

Die doppelten Unterzeichnungsschlüssel werden auf sicheren Unterzeichnungsgeräten (HSM – Hardware Security Module) generiert, die die Anforderungen der *Anlage II* der eIDAS-Verordnung erfüllen.

Die Signaturschlüssel haben eine Länge von mindestens 2048 Bit.

H. Zertifikat-Ausgabemethode

H.1. Ausgabeverfahren der Zertifizierungszertifikate

Nach der Generierung der Zertifizierungsschlüssel, wie in Abschnitt *G.1* beschrieben, werden die Zertifikate der öffentlichen Signaturschlüssel gemäß DPCM generiert, mit den entsprechenden persönlichen Signaturschlüsseln unterzeichnet und im Zertifikate-Register auf die vorgesehene Weise registriert.

Die Zertifikate der Zertifizierungsschlüssel werden über das in Artikel 12, Absatz 1 des DPCM beschriebene Kommunikationssystem an die Agentur für das Digitale Italien geschickt.

Der Zertifizierungsdiensteanbieter generiert ein qualifiziertes Zertifikat für jeden von der Agentur für die Unterzeichnung des öffentlichen Verzeichnisses der Zertifizierungsdiensteanbieter verwendeten elektronischen Signaturschlüssel und veröffentlicht dieses im eigenen Zertifikate-Register. Der Zertifizierungsdiensteanbieter muss anschließend eine von der Abteilung unterzeichnete Kopie des Verzeichnisses der Zertifikate für die Zertifizierungsschlüssel aufbewahren und auf elektronischem Weg verfügbar machen (DPCM, Artikel 42, Absätze 1 und 3).

H.2. Ausgabeverfahren der Unterzeichnungszertifikate

INTESA stellt Zertifikate mit einem System aus, das konform mit Artikel 33 des DPCM ist.

Nach der Generierung des Signaturschlüssel-Paares, wie in Abschnitt *G.3* beschrieben, wird ein Antrag für ein neues Zertifikat im Format *PKCS#10* generiert, das automatisch den Nachweis des Besitzes des persönlichen Schlüssels und die Überprüfung der Richtigkeit des Schlüssel-Paares liefert.

Nach Generierung der Schlüssel wird der Antrag für ein Zertifikat unverzüglich von der Anwendung der Bank / des Instituts an die Certification Authority des QTSP geschickt.

Die Generierung der Zertifikate wird im Prüfungsbuch (DPCM, Artikel 18, Absatz 4) registriert.

H.2.1. In den Unterzeichnungszertifikaten enthaltene Informationen

Die im Rahmen dieses Verfahrenshandbuchs ausgegebenen INTESA-Zertifikate sind qualifizierte Zertifikate im Sinne der Verordnung (EU) 910/2014 (eIDAS) und folglich werden ihre Interoperabilität und Anerkennung auf Gemeinschaftsebene garantiert.

Das Qualifizierte Zertifikat definiert den Zertifizierungsdiensteanbieter, der es ausgegeben hat, eindeutig und enthält die notwendigen Daten für die Überprüfung der digitalen Signatur.

Jedes Qualifizierte Zertifikat für die elektronische Signatur ist konform mit der eIDAS-Verordnung und dem AgID-BESCHLUSS Nr. 147/2019 (*Leitfaden mit Technischen Regeln und Empfehlungen betreffend die Generierung von Zertifikaten).*

Alle im Rahmen der Leistungen gemäß diesem Verfahrenshandbuch ausgegebenen Qualifizierten Zertifikate enthalten eine Nutzungsbeschränkung (Abschnitt *F.1.1*).

H.2.2. Notfallcode

Der Zertifizierungsdiensteanbieter garantiert im Einklang mit den Bestimmungen von Artikel 21 des DPCM einen *Notfallcode*, der bei der Beantragung einer **dringenden Aussetzung** des Zertifikats zu verwenden ist.

Für die in diesem Verfahrenshandbuch beschriebenen Anwendungen gilt als Notfallcode die PIN, die dem Inhaber bei seiner Registrierung ausgehändigt wurde.

I. Verfahrensabläufe für die Unterzeichnung der Dokumente

Der QTSP INTESA stellt über die Dienste der Bank oder des Zahlungsinstituts dem Inhaber alles bereit, was für die Generierung der qualifizierten elektronischen Signaturen im Einklang mit den geltenden Rechtsvorschriften notwendig ist.

Die besondere Art von Dienstleistung erfordert nicht die Bereitstellung einer auf dem eigenen PC zu installierenden Unterzeichnungs-App, sondern eher über den Homebanking-Dienst der Bank oder des Zahlungsinstituts oder unmittelbar am Schalter der Bank oder des Zahlungsinstituts abrufbare Unterzeichnungsfunktionen.

Die durch diese Verfahren generierten qualifizierten elektronischen Signaturen sind in Bezug auf die eingesetzten Algorithmen vollkommen konform mit den Bestimmungen von Artikel 4, Absatz 2 des DPCM.

Darüber hinaus enthalten diese Dokumente, gemäß Artikel 4, Absatz 3 des DPCM, keine Makro-Anweisungen oder ausführbaren Codes zur Aktivierung von Funktionen, die ohne Wissen des Unterzeichners Akten, Fakten oder Daten in den entsprechenden Dokumenten verändern könnten.

Im Folgenden werden zwei unterschiedliche Authentifizierungsmethoden beschrieben, die im Einklang mit den geltenden Rechtsvorschriften einem bereits registrierten Inhaber ermöglichen, zunächst die Signaturschlüssel und den Antrag auf ein qualifiziertes Zertifikat zu generieren und diese anschließend zur Nutzung von qualifizierten elektronischen Signaturen zu verwenden.

Zur Bestätigung der Ausführung der Unterzeichnungsvorgänge werden SMS versendet. Sollte der Inhaber ein für das Lesen von Korrespondenz aktiviertes Smartphone verwenden, so können die Benachrichtigungen alternativ, auf Anfrage des Inhabers, auch per E-Mail versendet werden.

I.1. Authentifizierung vom Typ „Call Drop“

Bei dieser Authentifizierungsmethode muss der bereits identifizierte Benutzer mit dem eigenen Mobiltelefon (von der gleichen Nummer, die bei der Identifizierung angegeben wurde) eine spezielle, ihm im Rahmen des Dienstes übermittelte, Telefonnummer wählen, um seine Absicht, ein Dokument zu unterzeichnen, zu bestätigen.

Bei Eingang des vorgenannten Anrufs wird die Herkunft der Telefonnummer (*Call Identifier*), die bei der Registrierung mit dem Benutzer assoziiert wurde, überprüft. Bei Bestätigung der Herkunft wird der Vorgang für die qualifizierte elektronischen Signatur autorisiert.

Wenn also der Inhaber über Zugriff auf das Portal der Bank /des Instituts ein Dokument unterzeichnen möchte, verwendet er eine Zwei-Faktor-Authentifizierung durch die Eingabe einer PIN (die nur der Benutzer kennt) und einer Telefonnummer (die von der SIM stammt, die nur der Benutzer besitzt).

Diese Art von Authentifizierung wird auch *„Call Drop“* genannt, da der Inhaber einen Anruf tätigt, um authentifiziert zu werden: Es wird jedoch kein Gespräch geführt und das Telefonat wird nach wenigen Sekunden beendet.

Der Anruf des Inhabers (Benutzers) wird in keinem Fall angenommen, daher entstehen dem Inhaber keinerlei Telefonkosten.

Zu den Vorteilen dieser Technik gehört, dass sie äußerst kostengünstig und praktisch ist, da keinGerät für die Authentifizierung verwendet werden muss und das Verfahren sehr einfach ist.

Im Folgenden wird deutlich, dass diese soeben beschriebene Methode zur Authentifizierung besonders gerne verwendet wird, wenn der Inhaber Vorgänge an unbemannten Arbeitsstationen durchführen möchte (in der Regel, indem er sich über die von der Bank oder dem Zahlungsinstitut angebotenen Homebanking-Dienste mit den Diensten der Bank oder Zahlungsinstituts verbindet); dagegen ist sie weniger praktisch, wenn der Inhaber sich bei einem externen Anbieter, zum Beispiel einer bemannten Kasse in der Bank oder dem Zahlungsinstitut, befindet.

Für diese Situationen wurde eine Lösung basierend auf einer dynamischen Verwaltung der zu wählenden Telefonnummern vorgesehen, um das Authentifizierungsverfahren an Stellen, die wir als bemannt bezeichnen, durchzuführen.

I.1.1. Unterzeichnungsverfahren an unbemannten Arbeitsstationen (Home Banking)

Nachdem der Inhaber bei der Identifizierung die notwendigen Codes erhalten hat, kann er anschließend das eigene digitale Zertifikat beantragen und dann ein Dokument auf die nachstehend beschriebene Weise unterzeichnen.

1. Der Inhaber stellt mit seinen persönlichen Codes für den Zugriff auf die App eine Verbindung zur Bank- oder Finanz-App her.
2. Er wählt und überprüft das zu unterzeichnende Dokument.
3. Er gibt seine eigene PIN ein.
4. Sofort nach der Validierung der PIN muss der Inhaber, um seine Absicht, das Dokument zu unterzeichnen, zu bestätigen, in einer vorgegebenen Zeit (nicht mehr als eine Minute) unter Verwendung des zuvor angegebenen Mobiltelefons eine Telefonnummer wählen, die ihm in der Zwischenzeit am Bildschirm angezeigt wurde.
5. Das System erkennt die Nummer der anrufenden Person als die zuvor bestätigte und mit dem Inhaber assoziierte Nummer, setzt die Signatur unter das Dokument und sendet eine Bestätigung des erfolgreich ausgeführten Vorgangs an den Inhaber.
6. Wenn jedoch die vorgegebene Zeit vergeht, ohne dass das System einen Anruf unter der unter Punkt 4 angegebenen Nummer registriert, gilt der Vorgang als nichtig und wird ohne Unterzeichnung des Dokuments abgeschlossen.

Soll mehr als ein Dokument unterzeichnet werden, so muss der Inhaber für jedes Dokument die Schritte von Punkt 2 bis 5 wiederholen.

I.1.2. Unterzeichnungsverfahren an bemannten Arbeitsstationen (Bankschalter oder Finanzschalter)

Nachdem der Inhaber das qualifizierte Zertifikat erhalten hat, kann er die Unterzeichnung eines Dokuments durchführen.

Wie bereits gesagt, könnte es für ihn an einem Schalter in der Bank oder im Finanzinstitut vor einem Bankangestellten schwierig sein, persönliche und geheime Codes wie beispielsweise die PIN einzugeben.

Es gibt daher eine alternative Lösung, die ebenfalls höchste Sicherheit gewährleistet:

1. Der Benutzer begibt sich an einen Schalter in einer Niederlassung der Bank / des Instituts (bemannte Arbeitsstation) und wird von den Angestellten (z. B. dem Kassierer) mit den Standardmethoden erkannt.
2. Nach Einsichtnahme in das zu unterzeichnende Dokument kann der Inhaber das Unterzeichnungsverfahren in die Wege leiten.
3. Nun wird in einem für den Inhaber sichtbaren Video eine Telefonnummer angezeigt (die nach dem Zufallsprinzip aus einer großen Anzahl verfügbarer Nummern ausgewählt wird) und gleichzeitig beginnt ein Timer zu laufen.
4. Der Inhaber muss, in einer vorgegebenen Zeit (nicht mehr als eine Minute), die ihm auf dem Bildschirm angezeigte Nummer (unter Verwendung des eigenen zuvor angegebenen Mobiltelefons) wählen, um seine Absicht, das Dokument zu unterzeichnen, zu bestätigen.

5. An dieser Stelle erkennt das System die Richtigkeit des Anrufers, führt die Unterzeichnung des Dokuments aus und sendet per SMS eine Bestätigung des erfolgreich ausgeführten Vorgangs an den Inhaber.
6. Wenn jedoch die vorgegebene Zeit vergeht, ohne dass das System einen Anruf unter der unter Punkt 3 angegebenen Nummer registriert, wird der Vorgang abgebrochen.

Soll mehr als ein Dokument unterzeichnet werden, so muss der Inhaber für jedes Dokument die Schritte von Punkt 2 bis 5 wiederholen.

I.2. Authentifizierung vom Typ „OTP Mobile“

Alternativ zur Call-Drop-Authentifizierung wird eine zweite Authentifizierungsmethode angeboten, Die „*OTP Mobile*“ genannt wird.

Zur Aktivierung dieser Methode muss der Inhaber ein Smartphone besitzen, das zu den von der Bank / dem Institut als für diesen Dienst geeigneten Modellen gehört.

Sobald dies in der Phase der Identifizierung am Schalter der Bank /des Instituts, wo die Registrierung erfolgt, überprüft wurde, wird dem Inhaber eine spezielle Internetadresse der Website der Bank oder des Zahlungsinstituts mitgeteilt, unter der er eine als „*OTP Mobile*”“ definiert App herunterladen kann, und ihm wird eine PIN ausgehändigt.

Auch für diese zweite Authentifizierungsmethode beschreiben wird das Unterzeichnungsverfahren für bemannte und unbemannte Arbeitsstationen.

I.2.1. Unterzeichnungsverfahren an unbemannten Arbeitsstationen (Home Banking)

Sobald der Inhaber das eigene qualifizierte Zertifikat erhalten hat, kann er Dokumente entsprechend den folgenden Schritten unterzeichnen:

1. Der Inhaber stellt mit seinen persönlichen Codes für den Zugriff auf die App eine Verbindung zur Bank- oder Finanz-App her;
2. Er wählt und überprüft das zu unterzeichnende Dokument;
3. Er gibt dann seine PIN ein;
4. Anschließend startet er die vorher auf sein Smartphone heruntergeladene App und erhält von dieser ein einmaliges Passwort, welches er nach seiner PIN eingeben muss;
5. Das System erkennt die Richtigkeit der soeben eingegebenen PIN und des einmaligen Passworts (OTP), leitet den Unterzeichnungsvorgang ein und sendet eine Bestätigung des erfolgreich ausgeführten Vorgangs an den Inhaber.

Soll mehr als ein Dokument unterzeichnet werden, so muss der Inhaber für jedes Dokument die Schritte von Punkt 2 bis 5 wiederholen.

I.2.2. Unterzeichnungsverfahren an bemannten Arbeitsstationen (Bankschalter oder Finanzschalter)

Auch für diesen Fall ist eine Lösung vorgesehen, die vom Inhaber nicht verlangt, dass er vor den Augen der Angestellten der Bank oder der Zahlungsinstituts geheime Codes eingibt, die anschließend zu seinem Schaden auf missbräuchliche Weise wiederverwendet werden könnten.

Sobald der Inhaber das eigene qualifizierte Zertifikat erhalten hat, kann er wie folgt Dokumente unterzeichnen:

1. Der Benutzer begibt sich an einen Schalter in einer Niederlassung der Bank / des Instituts (bemannte Arbeitsstation) und wird von den Angestellten (z. B. dem Kassierer) mit den Standardmethoden erkannt.
2. Bei der Unterzeichnung wird vor dem Benutzer ein spezifischer Monitor mit einer Webcam aktiviert.
3. Nachdem der Inhaber auf diesem Bildschirm das zu unterzeichnende Dokument identifiziert hat und beschließt, dieses zu unterzeichnen, lässt er auf seinem Smartphone ein einmaliges

Passwort generieren, welches auch im Format eines Strichcodes angezeigt wird.

4. Nun kann der Inhaber sein Smartphone vor die Webcam halten, das generierte OTP ablesen lassen und das eigentliche Unterzeichnungsverfahren in die Wege leiten.
5. Wenn das Dokument unterzeichnet wurde, sendet das System zur Bestätigung eine SMS an den Inhaber.

Soll mehr als ein Dokument unterzeichnet werden, sind die Schritte von Punkt 2 bis 5 zu wiederholen.

I.2.3. Unterzeichnungsverfahren für potenzielle Kunden

Das Verfahren für die Ausgabe eines qualifizierten Zertifikats für die qualifizierte E-Signatur kann auch von einem potenziellen Kunden während der Onboarding-Aktivitäten (Kundenakquisition) durchgeführt werden.

Das Verfahren ist kompatibel mit den wichtigsten Browsern (Chrome, Firefox, Edge, Safari) sowie den neusten mobilen Geräten der Familien Android und Apple.

Die Vorgehensweise ist wie folgt:

1. Zu Beginn des Verfahrens wird der potenzielle Kunde zur Eingabe der eigenen personenbezogenen Daten aufgefordert, um, nach Unterzeichnung der Mitteilung zum Datenschutz des QTSP INTESA, die anschließende eindeutige Identifizierung zu ermöglichen;
2. Die Bank / das Institut versendet ein SMS mit einem OTP (One Time Password) mit befristeter Gültigkeit: Der potenzielle Kunde muss diesen Code eingeben, um die tatsächliche Verfügbarkeit des bei der Eingabe seiner Daten angegebenen mobilen Geräts zu verifizieren;
3. Nach der Prüfung übermittelt der potenzielle Kunde dann seine Ausweispapiere an die Bank / das Institut: Die persönlichen Daten werden vom potenziellen Kunden eingegeben oder durch ein OCR-System aus den Ausweispapieren ausgelesen;
4. Nach Abschluss der Registrierung sendet die Bank dem potenziellen Kunden die Vertragsunterlagen zu, die der potenzielle Kunde mit einem vom QTSP INTESA ausgegebenen Qualifizierten Zertifikat für die E-Signatur (FDR) unterzeichnen kann.
5. Ähnlich wie beim für das Internetbanking beschriebenen Verfahren werden dem potenziellen Kunden die Unterlagen für die Beantragung des Zertifikats vom QTSP INTESA vorgelegt.
6. Die Einsichtnahme dieser Unterlagen muss unbedingt durch Setzen eines Hakens in das Kästchen des Dokuments und das Einfügen der elektronischen Signatur durch die Eingabe des per SMS vom QTSP INTESA erhaltenen OTP unterzeichnet werden.
7. Bei einer Bestätigung des vom QTSP INTESA übermittelten OTP kann das qualifizierte Zertifikat eingegeben werden, andernfalls ist ein neue OTP anzufordern.
8. Bei der Generierung des Zertifikats ist in jedem Fall die Eingabe einer PIN unerlässlich; diese Nummer wird dann bei jeder Verwendung des Zertifikats für die Signatur abgefragt.
9. Das soeben ausgegebene Zertifikat kann in jedem Fall nur für die Unterzeichnung des Antrags auf Abschluss eines Vertrags, jedoch kein anderes Dokument, verwendet werden, solange die Bank nicht die notwendigen vorbereitenden Prüfungen für die Eröffnung eines Kontos abgeschlossen hat.
10. Werden die Prüfungen der Bank erfolgreich abgeschlossen und das Konto aktiviert, kann der potenzielle Kunde das ausgegebene Zertifikat im Rahmen der geltenden Nutzungsbeschränkungen in den Beziehungen zur Bank benutzen.
    Falls jedoch die Bank dem Antrag auf Eröffnung eines Kontos nicht stattgeben sollte, würde das Zertifikat widerrufen und wäre nicht weiter verwendbar.
11. In beiden vorgenannten Fällen wird der potenzielle Kunde in jedem Fall über den Ausgang der Überprüfungen und einen eventuellen Widerruf des Zertifikats informiert.

I.3. Authentifizierung mit Token OTP

Schließlich kann eine Authentifizierung durchgeführt werden, die an die Nutzung physischer Token OTP gebunden ist (die in der Bank-und Finanzwelt weit verbreitet sind).

Heute ist die Nutzung dieser Token OTP nur für Zugriffe an unbemannten Arbeitsstationen (in der Regel ein externer Homebanking-Rechner) vorgesehen.

Der Inhaber stellt mit seinen persönlichen Codes für den Zugriff auf die App und den Start des Unterzeichnungsverfahrens eine Verbindung zur Bank- oder Finanz-App her und gibt die PIN und den OTP-Code ein, den er in der Zwischenzeit generiert und auf dem Token-Display angezeigt hat.

J. Verfahrensabläufe für die Überprüfung der Unterschrift

Die mit den oben beschriebenen Methoden unterzeichneten Dokumente sind ausschließlich Dokumente im PDF-Format: Dieses Unterzeichnungsformat gilt im Bereich von Bank- oder Finanzanwendungen als einfach zu verwenden.

Die Überprüfung der unterzeichneten Unterlagen kann ohne weiteres mit der Software *Acrobat Reader DC* durchgeführt werden, einer Anwendung, die alle Arten von qualifizierten elektronischen Signaturen im Format PDF, die von der EU im Einklang mit der eIDAS-Verordnung erzeugt werden, überprüfen kann.

Acrobat Reader DC kann kostenlos auf der folgenden Website von Adobe heruntergeladen werden: *https://www.adobe.com/it/*

K. Methode für Widerruf oder Aussetzung der Zertifikate

Im Einklang mit der eIDAS-Verordnung sind die Informationen betreffend des Zertifikat-Status per OCSP-Protokoll unter der auf dem Zertifikat angeführten URL abrufbar.

Der Widerruf und die Aussetzung der Zertifikate können auch durch ihre Aufnahme in die Liste widerrufener Zertifikate („Certificate Revocation List“, CRL) (Artikel 22 des DPCM) bestätigt werden. Das Profil der CRL ist konform mit dem Standard RFC 3280. Diese von der Certification Authority, die das Zertifikat ausstellt, unterzeichnete Liste wird in vorgegebenen Zeitabständen und im Einklang mit den geltenden Rechtsvorschriften aktualisiert.

Die CRL ist auch im Zertifikate-Register verfügbar.

In den Fällen, in denen der Widerruf oder die Aussetzung auf Initiative des Zertifizierungsdiensteanbieters oder des beteiligten Dritten (Artikel 23, 25, 27 und 29 des DPCM) erfolgt, benachrichtigt der Zertifizierungsdiensteanbieter den Inhaber über den Antrag sowie den Zeitpunkt Inkrafttretens der angeforderten Maßnahme.

Bei der Beantragung werden das Datum und die Uhrzeit für den Zeitpunkt benannt, ab dem das Zertifikat als widerrufen gilt (Artikel 24 Absatz 1, DPCM).

K.1. Widerruf der Zertifikate

Ein Zertifikat kann auf Antrag des Inhabers, des beteiligten Dritten oder der Certification Authority (d. h. dem QTSP - Zertifizierungsdiensteanbieter) widerrufen werden.

Ein widerrufenes Zertifikat darf in keiner Weise reaktiviert werden.

K.1.1. Widerruf auf Antrag des Inhabers

Der Inhaber kann den Widerruf beantragen, indem er auf einen bestimmten im Rahmen der Dienste der Bank oder des Zahlungsinstituts bereitgestellten Bereich zugreift oder sich mit dem Kundendienst der Bank oder des Zahlungsinstituts in Verbindung setzt.

Der von der Bank / dem Institut benachrichtigte QTSP, der in der Zwischenzeit die Zugangscodes des Inhabers gesperrt hat, wird das Zertifikat unverzüglich widerrufen.

K.1.2. Widerruf auf Antrag des beteiligten Dritten

Die Bank oder das Zahlungsinstitut, als beteiligte Dritte, können den Widerruf eines Zertifikats beantragen.

Nach Überprüfung der Richtigkeit des Antrags benachrichtigt der QTSP die betroffenen Inhaber auf den zum

Zeitpunkt der Registrierung mit dem Inhaber vereinbarten oder im Folgenden aktualisierten und dem QTSP, auch über die LRA, vom Inhaber mitgeteilten Kommunikationswegen über den Widerruf (Abschnitt *C.2. Pflichten des Inhabers*).

K.1.3. Widerruf auf Antrag des Zertifizierungsdiensteanbieters

Der Zertifizierungsdiensteanbieter, der den Widerruf des Qualifizierten Zertifikats beabsichtigt, benachrichtigt darüber die Bank /das Institut (beteiligte Dritte) im Vorhinein per E-Mail (außer in Fällen mit begründeter Dringlichkeit) und informiert gleichzeitig den Inhaber unter der bei der Beantragung des Zertifikats angegebenen E-Mail-Adresse oder unter seiner Wohnanschrift, wobei er die Gründe des Widerrufs sowie das Datum und die Uhrzeit für den Zeitpunkt der Wirksamkeit des Widerrufs angibt.

K.1.4. Widerruf der Zertifikate im Zusammenhang mit Zertifizierungsschlüsseln

Im Fall:

- einer Gefährdung der Zertifizierungsschlüssel sowie
- einer Einstellung der Betriebstätigkeit

widerruft der Zertifizierungsdiensteanbieter die entsprechenden Zertifikate und die mit dem gleichen Zertifizierungsschlüssel unterzeichneten Unterzeichnungszertifikate.

Innerhalb der 24 Stunden benachrichtigt der Zertifizierungsdiensteanbieter die Agentur für das Digitale Italien sowie die Inhaber von dem Widerruf.

K.2. Aussetzung der Zertifikate

Für die Methoden für die Aussetzung und Benachrichtigung über Aussetzungen gelten die Angaben zu den Methoden für Widerrufe in Abschnitt *K.1*.

Die Aussetzung eines Zertifikats ist vorgesehen, falls eine zusätzliche Untersuchung durchgeführt werden muss, um festzustellen, ob der Widerruf des Zertifikats tatsächlich notwendig ist (z. B. wenn der Verlust / Diebstahl des Token OTP befürchtet wird oder überprüft wird, ob der Inhaber wirklich die Tätigkeit, für die das Zertifikat ausgegeben worden war, eingestellt hat, usw.).

Der Antrag auf Aussetzung kann von allen im DPCM in den Artikeln 27, 28 und 29 genannten Parteien erstellt werden (Zertifizierungsdiensteanbieter, Inhaber, beteiligter Dritter).

Erfolgt keine Mitteilung durch den Inhaber, wird das Zertifikat automatisch nach einer Aussetzungsdauer von 90 (neunzig) Tagen oder in jedem Fall spätestens am Ablaufdatum des Zertifikats widerrufen.

Der Zeitpunkt des Inkrafttretens des Widerrufs entspricht in jedem Fall dem Tag des Beginns der Aussetzung.

K.2.1. Aussetzung auf Antrag des Inhabers

Der Inhaber kann die Aussetzung des Zertifikats beantragen, indem er auf einen bestimmten im Rahmen der Dienste der Bank oder des Zahlungsinstituts bereitgestellten Bereich zugreift oder sich mit dem Kundendienst der Bank oder des Zahlungsinstituts in Verbindung setzt.

Der Zertifizierungsdiensteanbieter sorgt für die Aussetzung, welche dem Inhaber über die speziellen im Rahmen der Dienste der Bank oder des Zahlungsinstituts verfügbaren Funktionen kommuniziert wird.

Später kann der Inhaber die Wiederaktivierung des Zertifikats mit den von der Bank oder dem Zahlungsinstitut bereitgestellten Methoden beantragen.

Erfolgen keine weiteren Mitteilungen, wird das Zertifikat automatisch am Ende der Aussetzungsdauer widerrufen und das Widerrufsdatum entspricht dem Tag des Beginns der Aussetzung.

K.2.2. Aussetzung auf Antrag des beteiligten Dritten

Die Bank oder das Zahlungsinstitut, als beteiligte Dritte, können die Aussetzung eines Zertifikats beantragen.

Nach Überprüfung der Richtigkeit des Antrags setzt der Zertifizierungsdiensteanbieter das Zertifikat unverzüglich

aus und benachrichtigt die betroffenen Inhaber über die Aussetzung per E-Mail oder die angebotenen Dienste der Bank oder des Zahlungsinstituts.

K.2.3. Aussetzung auf Antrag des Zertifizierungsdiensteanbieters

Der Zertifizierungsdiensteanbieter kann, außer in Fällen begründeter Dringlichkeit, das Zertifikat aussetzen, indem er den Inhaber im Vorhinein unter der bei der Beantragung des Zertifikats angegebenen E-Mail-Adresse oder unter seiner Wohnanschrift informiert und dabei die Gründe der Aussetzung sowie das Datum und die Uhrzeit für den Zeitpunkt der Wirksamkeit des Aussetzung angibt.

Der Zertifizierungsdiensteanbieter schickt eine vergleichbare Mitteilung auch an den beteiligten Dritten.

L. Methode für die Ersetzung der Schlüssel

L.1. Ersetzung der qualifizierten Zertifikate und Schlüssel des Inhabers

Vom Zertifizierungsdiensteanbieter in dem in diesem Verfahrenshandbuch genannten Kontext ausgegebene qualifizierte Zertifikate mit elektronischer Signatur haben eine Gültigkeit von 36 (sechsunddreißig) Monaten ab ihrem Ausgabedatum.

Am Ende des vorgenannten Zeitraums muss gleichzeitig mit der Ausgabe eines neuen Zertifikats ein neues Signaturschlüssel-Paar generiert werden.

In diesem Fall wird für die Ausgabe des neuen Zertifikats ein ähnliches Verfahren wie das für die erste Ausgabe befolgt, allerdings ist eine Wiederholung der Identifizierung des Inhabers nicht notwendig.

L.2. Ersetzung der Schlüssel des Zertifizierungsdiensteanbieters

L.2.1. Ersetzung im Notfall der Zertifizierungsschlüssel

Das im Fall von Defekten der Signaturerstellungsheinheit (HSM), die die Zertifizierungsschlüssel (CA und TSCA) enthält, oder einer Katastrophe am Hauptsitz angewandte Verfahren wird im Abschnitt *Verwaltungsverfahren für Katastrophenereignisse* beschrieben.

L.2.2. Programmierte Ersetzung der Zertifizierungsschlüssel

Innerhalb der durch die geltenden Rechtsvorschriften vorgeschriebenen Frist geht der Zertifizierungsdiensteanbieter vor dem Ablauf des Zertifikats für die Zertifizierungsschlüssel-Paare (CA und TSCA), die von den Systemen für die Ausgabe der Unterzeichnungszertifikate und der TSA-Zertifikate verwendet werden, gemäß den Bestimmungen von Artikel 30 des DPCM vor.

L.3. Schlüssel des Zeitstempel-Systems (TSA)

Im Einklang mit den Bestimmungen von Artikel 49, Absatz 2 des DPCM werden die Schlüssel des Zeitstempel-Systems innerhalb von 90 (neunzig) Tagen ab ihrem Ausgabedatum ersetzt, um die Anzahl der mit demselben Zertifizierungsschlüssel-Paar generierten Zeitstempel zu beschränken. Gleichzeitig wird ein Zertifikat für das neue Schlüssel-Paar ausgegeben (ohne das vorherige, dem ersetzten Schlüssel-Paar zugehörige, zu widerrufen).

M. Zertifikate-Register

M.1. Methode für die Verwaltung des Zertifikate-Registers

Im Zertifikate-Register veröffentlicht INTESA:

1. Die Signaturschlüssel und die Schlüssel für das Zeitstempel-System.
2. Die Zertifikate der Zertifizierungsschlüssel (CA und TSCA).

3. Die in Folge des Auswechselns der Zertifizierungsschlüssel ausgegebenen Zertifikate.
4. Zertifikate für die Signaturschlüssel der Agentur für das Digitale Italien (DPCM Artikel42, Absatz 1).
5. Die Zertifikatssperrlisten (CRL).

Vorgänge betreffend das Zertifikate-Register werden nur von Personen durchgeführt, die für diese autorisiert wurden; diese sind in einer ausreichenden Anzahl vorhanden, die geeignet ist, rechtswidrige Handlungen durch eine begrenzte Zahl von Mitarbeitern zu verhindern.

Der Zertifizierungsdiensteanbieter bewahrt eine Referenzkopie des Zertifikate-Registers auf, die von außerhalb nicht zugänglich ist; diese Kopie aktualisiert in Echtzeit die operative Kopie, auf die die Benutzer mit LDAP-Protokoll Zugriff haben.

Die Übereinstimmung zwischen Referenzkopie und operativer Kopie wird systematisch überprüft.

M.2. Logischer Zugang zum Zertifikate-Register

Die Referenzkopie befindet sich in einem speziellen, durch entsprechende Vorrichtungen geschützten Netz und ist daher für andere nur über den Server für die Ausgabe der Zertifikate zugänglich, der hier die ausgegebenen Zertifikate und die CRL registriert.

Der Zugriff auf die operativen Kopien ist mit LDAP-Protokoll möglich unter der Adresse ***ldap://x500.e-trustcom.intesa.it*** .

Der Zertifizierungsdiensteanbieter gewährt auch über das http-Protokoll Zugriff auf die CRL, unter der URL, die im Zertifikat im Feld CDP (CRL Distribution Point) angegeben ist.

M.3. Physischer Zugang zu den Räumen der Systeme der Zertifikate-Register

Die für die direkte Verwaltung des Zertifikate-Registers berechtigten Mitarbeiter haben Zugang zu dem Raum, in dem das System installiert ist, und können mit dem Register nur mit Kontrollen nach dem Vier-Augen-Prinzip arbeiten, um gesetzwidrige Vorgänge zu verhindern.

Die für die Systemverwaltung, Netzverwaltung, Wartung usw. zuständigen Mitarbeiter haben Zugang zu dem Raum, in dem das System installiert ist und können dort nur in Anwesenheit der für die Verwaltung des Zertifikate-Registers berechtigten Mitarbeiter auf die für die zugelassenen Mitarbeiter dargelegte Weise arbeiten.

N. Schutzmethode für personenbezogene Daten

Die Sicherheitsmaßnahmen für den Schutz der personenbezogenen Daten entsprechen den Maßnahmen, die durch die Europäische Verordnung 679/2016 (DSGVO), mit späteren Änderungen und Ergänzungen, vorgesehen sind.

O. Verwaltungsverfahren für Sicherheitskopien

Die elektronischen Archive, für die es Sicherheitskopien geben muss, sind die folgenden:

- ZERTIFIKATE-REGISTER, digitales Archiv mit dem unter Abschnitt M genannten Inhalt.
- OPERATIVE INFORMATIONEN - digitales Archiv, in dem alle vom Inhaber bei der Registrierung und der Beantragung der Zertifizierung erhaltenen Informationen sowie die Anträge auf Widerruf und Aussetzung zusammen mit den zugehörigen Unterlagen gespeichert sind.
- PRÜFUNGSBUCH - Archiv, das alle automatisch von den beim Zertifizierungsdienst des QTSP installierten Systemen durchgeführten Registrierungen enthält (Artikel 36 des DPCM).
- DIGITALES ZEITSTEMPEL-ARCHIV - enthält die vom Zeitstempel-System generierten Zeitstempel (Artikel 53, Absatz 1 des DPCM).
- OPERATIVES REGISTER DER ZEITSTEMPEL-EREIGNISSE - Register, in dem automatisch diejenigen Ereignisse in

Verbindung mit der Ausgabe von Zeitstempeln gespeichert werden, für die die Registrierung von Anomalien oder Versuchen von Manipulation vorgesehen ist, welche die Funktionsfähigkeit des Zeitstempel-Systems gefährden könnten (Artikel 52 des DPCM).

Die Aufbewahrung aller beschriebenen Sicherheitskopien erfolgt im Einklang mit den einschlägigen geltenden Rechtsvorschriften.

P. Verwaltungsverfahren für Katastrophenereignisse

Der QTSP INTESA verfügt über einen Notfallplan für das Katastrophenmanagement mit folgenden Phasen:

- Notfallmanagement: In dieser Phase wird die Kontinuität des Zugriffs auf die CRL gewährleistet; bei ihrer Ausgabe kann es zu Verzögerungen aufgrund der Notwendigkeit kommen, den Backup-Server der CA am Backup-Standort zu aktivieren;
- Übergangsverwaltung: In dieser Phase wird die Ausgabe der Zertifikate und die Wiederherstellung weiterer Desaster-Recovery-Lösungen gewährleistet;
- Rückkehr zum normalen Betrieb: auf derselben originalen Seite oder einer alternativen Seite, aber endgültig.

Es sei darauf hingewiesen, dass das Vorhandensein von Kopien der operativen Kopie des Zertifikate-Registers an mehreren verschiedenen Stellen bei einer Betriebsunterbrechung einer der Niederlassungen den Zugang zum Inhalt des bis zum Moment der Unterbrechung aktualisierten Inhaltes des Zertifikate-Registers ermöglicht.

Für das Notfallmanagement sind Kopien der Backup-Seite des Zertifikate-Registers, der Daten des Systems für die Ausgabe der Zertifikate sowie das Eingreifen innerhalb von 24 Stunden von Personal vorgesehen, das zur Aktivierung der Funktionen für die Ausgabe der CRL befähigt ist. Dieses Personal wird dementsprechend für die Verwaltung der Soft- und Hardware sowie den Umgang mit Notsituationen geschult.

In allen an der Verwaltung von Katastrophenereignissen beteiligten Niederlassungen ist eine gedruckte Kopie des Notfallplans hinterlegt.

Q. Methode für die Einfügung und Definition des Zeitstempels

Alle Computer der Public Key Infrastructure (PKI) des Zertifizierungsdiensteanbieters sind mit dem *I.N.RI.M. - Istituto Nazionale di Ricerca Metrologica* (Nationales Metrologisches Institut) in Turin (früher *Istituto Elettrotecnico Nazionale Galileo Ferraris*) synchronisiert. Die Synchronisation wird durch eine spezielle Software ermöglicht, die auf jedem Server installiert ist und sich über das NTP (Network Time Protocol) mit dem konfigurierten Remote-Server verbindet.

Das Network Time Protocol (NTP) ist eine der genausten und flexibelsten Methoden, um im Internet Zeit- und Datumsangaben zu übermitteln. Dieses Protokoll ermöglicht die Synchronisation von Computern, die über lokale Netzwerke, Stadtnetze oder sogar globale Netze (Internet) verbunden sind, durch Nutzung einer pyramidenförmigen hierarchischen Struktur.

Das I.N.RI.M stellt einen Synchronisationsdienst für mit dem Internet verbundene IT-Systeme bereit, das auf zwei primären NTP-Servern basiert, die im Labor für Standard-Zeit und -Frequenz installiert sind. Sie werden über einen Zeit- und Datumscodegenerator mit Caesium-Atomuhren synchronisiert, der auch für die Generierung der italienischen Zeit UTC(IT) verwendet werden. Die Zeitdifferenz zwischen den NTP-Servern des I.N.RI.M und der nationalen deutschen Uhrzeit wird kontrolliert und beträgt im Normalfall weniger als einige Millisekunden. Die erreichbare Synchronisationspräzision hängt ab von der Art des Netzwerks und dem Abstand zwischen dem NTP-Server und dem Rechner, der synchronisiert werden soll; bei Systemen, die dem gleichen Netzwerk angehören, liegen die Zeitdifferenzwerte typischerweise unter einer Millisekunde, während sie bei Remote-Netzwerken einige Hundert Millisekunden erreichen können.

Die beim Zertifizierungsdiensteanbieter installierte Software stellt in regelmäßigen Zeitintervallen eine Verbindung zum Remote-Server her, ruft die aktuelle Zeit ab und korrigiert dann die Uhr des lokalen PCs mittels komplexer Algorithmen.

Die von den Anwendungen verwendeten Zeitbezüge sind Zeichenfolgen im Datumsformat (TT/MM/JJJJ SS:MM:SS) mit einer Genauigkeit bis auf die Sekunde, die je nach Konfiguration des PCs die Ortszeit anzeigen.

Diese Bezüge sind konform mit Artikel 51 des DPCM.

Jede im Kontrollbuch verzeichnete Registrierung enthält einen Zeitbezug der, da er mit der hier beschriebenen Methode generiert wurde, für Dritte verbindlich ist (Artikel 41 des DPCM).

Q.1. Methode für die Beantragung und Überprüfung der Zeitstempel

Der Zertifizierungsdiensteanbieter versieht alle vom Inhaber im Rahmen der in diesem Verfahrenshandbuch beschriebenen Unterlagen mit einem Zeitstempel (*qualifizierter Zeitstempel zur elektronischen Validierung* gemäß eIDAS-Verordnung).

Das Einfügen des Zeitstempels ist in das Unterzeichnungsverfahren integriert und erfordert keine spezifische Maßnahme seitens des Inhabers.

R. Lead Time und Raci-Tabelle für die Erstellung der Zertifikate

Die folgende Tabelle enthält Angaben zur „Prozessvorlaufzeit“ für die Abwicklung von Anfragen auf Ausgabe, Widerruf, Aussetzung und Reaktivierung von Zertifikaten.

Person	Anfrage	Beteiligte Einrichtung	Maßnahme der beteiligten Einrichtung	Beteiligte Einrichtung	Maßnahme der beteiligten Einrichtung
Benutzer, Antragsteller, Zertifizierter Inhaber	*Anfrage auf Zertifikatsausgabe über LRA*	*Bank / Institut (als) Local RA*	*Erteilt Anordnung für Veröffentlichung des Zertifikats über CA, nach vorheriger Identitätsprüfung*	*Certification Authority (CA)*	*Bearbeitung der Anfrage auf Ausgabe*
Benutzer, Antragsteller, Zertifizierter Inhaber	*Anfrage auf Zertifikatswiderruf über RA oder LRA*	*Intesa (als) Registration Authority (RA) oder Bank /Institut (als LRA)*	*Erteilt Anordnung für Widerruf des Zertifikats über CA, nach vorheriger Identitätsprüfung*	*Certification Authority (CA)*	*Bearbeitung der Anfrage auf Widerruf*
Benutzer, Antragsteller, Zertifizierter Inhaber	*Anfrage auf Zertifikatsaussetzung über RA oder LRA*	*Intesa (als) Registration Authority (RA) oder Bank /Institut (als LRA)*	*Erteilt Anordnung für Aussetzung des Zertifikats über CA, nach vorheriger Identitätsprüfung*	*Certification Authority (CA)*	*Bearbeitung der Anfrage auf Aussetzung*
Benutzer, Antragsteller, Zertifizierter Inhaber	*Anfrage auf Zertifikats-reaktivierung über RA oder LRA*	*Intesa (als) Registration Authority (RA) oder Bank /Institut (als LRA)*	*Erteilt Anordnung für Reaktivierung des Zertifikats über CA, nach vorheriger Identitätsprüfung*	*Certification Authority (CA)*	*Bearbeitung der Anfrage auf Reaktivierung*

Die folgende Tabelle RACI enthält Angaben zu den Zuständigkeiten in Verbindung mit den von den Anfragen auf Ausgabe, Widerruf, Aussetzung und Reaktivierung von Zertifikaten betroffenen Einrichtungen.

Betroffene Person	Verantwortlich	Rechenschafts-pflichtig	Konsultiert	Informiert
Registration Authority	***X***			
Local Registration Authority	***X***			
Zertifizierungsdienste-anbieter (CA)		***X***		
Anwender, Antragsteller, Zertifikatsinhaber			***X***	***X***

S. Technische Referenzen

ETSI-319.401	ETSI EN 319 401 v2.1.1 - Electronic Signatures and Infrastructures (ESI); General Policy Requirements for Trust Service Providers
ETSI-319.411-1	ETSI EN 319 411-1 V1.1.1 - Electronic Signatures and Infrastructures (ESI); Policy and security requirements for Trust Service Providers issuing certificates; Part 1: General requirements
ETSI-319.411-2	ETSI EN 319 411-2 V2.1.0 - Electronic Signatures and Infrastructures (ESI); Policy and security requirements for Trust Service Providers issuing certificates; Part 2: Requirements for trust service providers issuing EU qualified certificates
ETSI-319.411-3	ETSI EN 319 411-3 V1.1.1 - Electronic Signatures and Infrastructures (ESI); Policy and security requirements for Trust Service Providers issuing certificates; Part 3: Policy requirements for Certification Authorities issuing public key certificates
ETSI-319.412-1	ETSI EN 319 412-1 V1.1.1 - Electronic Signatures and Infrastructures (ESI); Certificate Profiles; Part 1: Overview and common data structures
ETSI-319.412-2	ETSI EN 319 412-2 V2.1.1 - Electronic Signatures and Infrastructures (ESI); Certificate Profiles; Part 2: Certificate profile for certificates issued to natural persons
ETSI-319.412-5	ETSI EN 319 412-5 V2.1.1 - Electronic Signatures and Infrastructures (ESI); Certificate Profiles; Part 5: QCStatements
Rec ITU-R	Recommandation ITU-R TF.460-6, Annex 1 – Time Scales.
RFC5905	Network Time Protocol
ETSI-319.421	ETSI EN 319 421 v1.1.1 - Electronic Signatures and Infrastructures (ESI); Policy and Security Requirements for Trust Service Providers issuing Time-Stamps
ETSI-319.422	ETSI EN 319 422 v1.1.1 - Electronic Signatures and Infrastructures (ESI); Time-stamping protocol and time-stamp token profiles
Rec ITU-R	Recommandation ITU-R TF.460-6, Annex 1 – Time Scales.
RFC5905	Network Time Protocol

------- ENDE DES DOKUMENTS ------