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

Gekwalificeerde verlener van vertrouwensdiensten

(*Qualified Trust Service Provider*, QTSP)

Gebruikshandleiding voor procedures van gekwalificeerde elektronische ondertekening op afstand in de bank- en financiële sector

Documentcode: MO_REMBAN
OID: 1.3.76.21.1.50.110
Opgesteld door: Antonio Raia
Goedgekeurd door: Franco Tafini
Datum van afgifte: 01/07/2019
Versie: 04

Getekend door Antonio Raia
IN.TE.S.A. S.p.A.

An IBM Company
intesa
DIGITAL
BUSINESS SOLUTIONS

VERSIES

Versie nr.: 04		***Datum van herziening:***	***01/07/2019***
Beschrijving van de wijzigingen:	Wijziging van informatie over onderneming en logo Actualiseringen van definities en toepasselijke wet- en regelgeving Actualisering van visuele weergave Opname van ondertekeningsprocedure voor *Prospects* (I.2.3)		
Redenen:	Actualiseringen wet- en regelgeving: Verordening (EU) 910/2014 (eIDAS), Italiaans wetgevend besluit 179/2016 (AVG) Organisatorische wijzigingen TSP Procedure voor acquisitie van nieuwe klanten		
Versie nr.: 03		***Datum van herziening:***	***13/06/2012***
Beschrijving van de wijzigingen:	Uitbreiding van de handleiding voor toepassing op zowel de financiële sector (betalingsinstellingen) als de banksector		
Redenen:	Update		
Versie nr.: 02		***Datum van herziening:***	***02/04/2012***
Beschrijving van de wijzigingen:	B.4.2. - Introductie van een identificatiesysteem van de houder (*due diligence*) dat niet de fysieke aanwezigheid hiervan vereist. C.5. - Introductie van identificatiesysteemmethoden van de houder (*due diligence*). F.1.3. - Opname standaardbeperking op het gebruik. G. - Opname van e-mailberichten als methode voor het bevestigen van succesvolle transacties.		
Redenen:	Update		
Versie nr.: 01		***Datum van herziening:***	***01/11/2011***
Beschrijving van de wijzigingen:	geen		
Redenen:	eerste versie		

Samenvatting

Toepasselijke wetgeving

Geconsolideerde wetgeving - Italiaans presidentieel besluit 445/00 en volgende wijzigingen en aanvullingen	Italiaans presidentieel besluit nr. 445/00 van 28 december 2000. "*Geconsolideerde wet- en regelgevende voorschriften inzake administratieve documentatie*". Hierna ook kortweg: TU *[Testo Unico* – eenvormige tekst] genoemd.
Italiaanse wet op digitale administratie - Italiaans wetgevend besluit 85/05 en volgende wijzigingen en aanvullingen	Italiaans wetgevend besluit nr. 82 van 7 maart 2005. "*Wet op digitale administratie*". Hierna ook kortweg CAD [*Codice dell'amministrazione Digitale*] genoemd.
Besluit van de Italiaanse minister-president van 22/02/2013 *Nieuwe Technische normen* en volgende wijzigingen en aanvullingen	Besluit van de Italiaanse minister-president van 22 februari 2013. *"Tecnische normen voor het genereren, toepassen en verifiëren van geavanceerde, gekwalificeerde en digitale elektronische handtekeningen, overeenkomstig artikel 20, lid 3, artikel 24, lid 4, artikel 28, lid 3, artikel 32, lid 3 onder b), artikel 35, lid 2, artikel 36, lid 2 en artikel 71" (van de CAD, ed.).* Hierna ook kortweg *DPCM [Decreto del Presidente Del Consiglio Dei Ministri]* genoemd.
Verordening (EU) nr. 910/2014 (eIDAS) en volgende wijzigingen en aanvullingen	Verordening (EU) nr. 910/2014 van het Europees Parlement en de Raad van 23 juli 2014, betreffende elektronische identificatie en vertrouwensdiensten voor elektronische transacties in de interne markt en tot intrekking van Richtlijn 1999/93/EG. Hierna ook kortweg eIDAS-verordening genoemd.
AVG Algemene Verordening Gegevensbescherming en volgende wijzigingen en aanvullingen	Verordening (EU) 2016/679 betreffende de bescherming van natuurlijke personen in verband met de verwerking van persoonsgegevens en betreffende het vrije verkeer van die gegevens, en tot intrekking van Richtlijn 95/46/EG (algemene verordening gegevensbescherming). Hierna ook kortweg AVG genoemd.
BEPALING NR. 147/2019 en volgende wijzigingen en aanvullingen	Richtsnoeren bevattende "Technische normen en aanbevelingen inzake het genereren van gekwalificeerde elektronische certificaten, gekwalificeerde elektronische handtekeningen en stempels en gekwalificeerde elektronische tijdstempels. Hierna ook kortweg de BEPALING genoemd.

Definities en afkortingen

AgID	*Agenzia per l'Italia Digitale* (Agentschap voor Digitaal Italië, voorheen CNIPA en DigitPA) – *www.agid.gov.it*. Toezichthoudende autoriteit, in overeenstemming met Ver. (EU) 910/2014 (eIDAS). Hierna ook kortweg het AgID genoemd.
QTSP Gekwalificeerde verlener van vertrouwensdiensten Geaccrediteerde certificeringsinstantie	*Gekwalificeerde verlener van vertrouwensdiensten* (Qualified Trust Service Provider). Natuurlijke of rechtspersoon, die een of meer gekwalificeerde vertrouwensdiensten verleent. Voorheen *Geaccrediteerde certificeringsinstantie*, overeenkomstig de CAD. In dit document wordt hiermee verwezen naar QTSP In.Te.S.A. S.p.A.
Gekwalificeerde vertrouwensdienst	Een door een QTSP verleende elektronische dienst, die bestaat uit de elementen beschreven in artikel 3, leden 16 en 17 van Ver. (EU) 910/2014 (eIDAS). In dit document wordt hiermee verwezen naar QTSP In.Te.S.A. S.p.A., die diensten van gekwalificeerde elektronische ondertekening en elektronische tijdstempels en andere daarmee verband houdende diensten verleent.
Gekwalificeerd certificaat voor elektronische handtekening	Elektronisch attest, dat de validatiegegevens van een elektronische handtekening aan een natuurlijke persoon verbindt en ten minste de naam of het pseudoniem van die persoon bevestigt. Dit wordt afgegeven door een gekwalificeerd verlener van vertrouwensdiensten en voldoet aan de in bijlage I van de Verordening (EU) 910/2014 (eIDAS) vastgelegde vereisten.

Privésleutel	Het element in het asymmetrische sleutelpaar, dat door de houder wordt gebruikt om elektronische documenten digitaal te ondertekenen.
Publieke sleutel	Het element in het asymmetrische sleutelpaar, dat bedoeld is om openbaar te worden gemaakt en wordt gebruikt om de op het elektronische document aangebrachte digitale handtekening te verifiëren.
CRL	Certificate Revocation List, een lijst van alle ingetrokken of opgeschorte certificaten, die door de uitgevende certificeringsinstantie niet langer als geldig worden beschouwd.
OCSP	Online Certificate Status Protocol: dienst voor de verificatie van de geldigheidsstatus van het certificaat, volgens het OCSP.
Elektronisch document	Elektronisch document, houdende de weergave van handelingen, feiten of juridisch relevante gegevens.
GEH – Gekwalificeerde Elektronische Handtekening *DH – Digitale Handtekening*	Elektronische handtekening, aangemaakt door een voor het voortbrengen van gekwalificeerde elektronische handtekeningen bedoeld apparaat en gebaseerd op een gekwalificeerd certificaat voor elektronische handtekeningen. In Italië komt deze overeen met de *Firma Digitale* [digitale handtekening], als volgt gedefinieerd in artikel 1, lid 1, onder s) van de CAD: een gekwalificeerde elektronische handtekening op basis van een systeem van cryptografische sleutels – een publieke sleutel en een privésleutel, die met elkaar verbonden zijn – dat de houder, met behulp van de privésleutel, en de ontvanger, met behulp van de publieke sleutel, in staat stelt de oorsprong en de integriteit van een elektronisch document of een reeks elektronische documenten aan te tonen en te verifiëren.
Handtekening op afstand	Een specifieke procedure voor gekwalificeerde elektronische handtekeningen of digitale handtekeningen, gegenereerd op een HSM, die onder het toezicht en beheer staat van de geaccrediteerde certificeringsinstantie, waardoor de exclusieve controle van de privésleutels door de houders wordt gewaarborgd.
HSM - Hardware Security Module	Apparaten voor het aanmaken van gekwalificeerde elektronische handtekeningen, indien zij voldoen aan de vereisten van bijlage II van Ver. (EU) 910/2014. Ook wel *ondertekenapparaten* genoemd.
Gekwalificeerde elektronische tijdstempel	*Gekwalificeerde elektronische tijdstempel*-gegevens in elektronische vorm die andere gegevens in elektronische vorm aan een bepaald tijdstip verbinden en het bewijs vormen dat deze laatste gegevens op dat moment bestonden. Het voldoet aan de eisen van artikel 42 van de eIDAS-verordening.
CA – Certificeringsinstantie	Autoriteit die de elektronische handtekeningcertificaten uitgeeft.
RA - Registratieautoriteit	Registratieautoriteit: door de QTSP benoemde entiteit, verantwoordelijk voor de registratie en verificatie van de door de QTSP vereiste informatie (met name de identiteit van de houder) voor de uitgifte van het gekwalificeerde certificaat.
Certificatenlijst	De combinatie van een of meer elektronische bestanden, die in het bezit zijn van de certificeringsinstantie en die alle afgegeven certificaten bevatten.
Aanvrager	De natuurlijke persoon die het certificaat aanvraagt.
Houder	De natuurlijke persoon aan wie het certificaat is afgegeven en die bevoegd is het te gebruiken voor doeleinden van het aanbrengen van zijn/haar handtekening.
Klant *Prospect*	Dit is de klant (of potentiële klant*, prospect* genoemd) van de bank/financiële instelling.
Tijdreferentie	Informatie over de datum en het tijdstip, gekoppeld aan een of meer elektronische documenten.
TSI – Tijdstempelinstantie	Autoriteit die de elektronische tijdstempels uitgeeft.

A. Inleiding

Dit document is de door de QTSP In.Te.S.A. S.p.A. opgestelde *Gebruikshandleiding voor procedures van gekwalificeerde elektronische ondertekening op afstand in de bank- en financiële sector* (hierna de *gebruikshandleiding* genoemd).

De inhoud van deze gebruikshandleiding voldoet aan de eisen die zijn vastgelegd in de technische normen die zijn opgenomen in het *besluit van de Italiaanse minister-president van 22 februari 2013* (hierna "DPCM" genoemd) en *Italiaans wetgevend besluit nr. 82 van 7 maart 2005,* dat de "*wet op digitale administratie*" bevat,

zoals later gewijzigd en aangevuld (hierna *CAD* genoemd), en voldoet aan *Verordening (EU) 910/2014* (hierna *eIDAS-verordening* genoemd).

Voor alle zaken die niet uitdrukkelijk in deze handleiding zijn opgenomen, wordt verwezen naar de huidige en toekomstige regelgeving inzake de specifieke omstandigheden.

In dit document worden de normen en operationele procedures van de *QTSP In.Te.S.A. S.p.A.* uiteengezet (hierna, *QTSP INTESA, Certificeringsinstantie* of kortweg *INTESA* genoemd) voor de afgifte van gekwalificeerde certificaten, het aanmaken en verifiëren van gekwalificeerde elektronische handtekeningen en de procedures van de tijdstempeldienst, overeenkomstig de huidige regelgeving binnen een context van bank- of financiële projecten.

In het kader van dergelijke projecten zullen de banken of financiële instellingen, als aanbieders van diensten op het gebied van thuisbankieren en diensten binnen de filialen, ook optreden als lokale registratieautoriteiten (hierna *LRAs* genoemd) namens QTSP INTESA. De voornoemde banken of financiële instellingen zullen hierna worden aangeduid als *bank* of *betalingsinstelling* (of kortweg *bank/instelling*).

In dit verband zijn de gekwalificeerde certificaathouders beperkt tot de personen die zijn geïdentificeerd door de bank/instelling, die op grond van een specifieke overeenkomst met QTSP INTESA bevoegd is om op te treden als registratieautoriteit.

Er wordt derhalve op gewezen dat alle ondertekeningsprocessen van documenten die onder deze gebruikshandleiding vallen, uitsluitend zullen worden uitgevoerd in het kader van bancaire of financiële toepassingen.

De activiteiten die in deze gebruikshandleiding zijn beschreven, worden uitgevoerd in overeenstemming met Ver. 910/2014 (eIDAS).

A.1. Intellectuele eigendom

Deze handleiding is de exclusieve eigendom van In.Te.S.A. S.p.A., die alle intellectuele eigendomsrechten ervan bezit.

De in dit document beschreven informatie met betrekking tot de uitvoering van QTSP-activiteiten is onderworpen aan intellectuele eigendomsrechten.

A.2. Geldigheid

De inhoud van dit document is van toepassing op QTSP INTESA (d.w.z. op zijn logistieke en technische infrastructuur en zijn personeel), op houders van certificaten die door laatstgenoemde zijn afgegeven en op degenen die dergelijke certificaten gebruiken om de authenticiteit en integriteit te controleren van documenten die zijn ondertekend met behulp van een gekwalificeerde elektronische handtekening, waarbij ook gebruik is gemaakt van de gekwalificeerde tijdstempels die door QTSP INTESA zijn afgegeven, en op de bank/betalingsinstelling in hun hoedanigheid van lokale registratieautoriteit.

Artikel 5, lid 4, van het DPCM regelt het gebruik van de sleutels en de bijbehorende certificaten, en stelt dat de sleutels voor ondertekening en verificatie en de bijbehorende diensten in de volgende categorieën kunnen worden onderverdeeld:

a) ondertekensleutels, gebruikt voor het aanmaken en verifiëren van handtekeningen die zijn aangebracht op of geassocieerd met documenten;
b) certificeringssleutels, gebruikt voor het aanmaken en verifiëren van handtekeningen die zijn aangebracht op gekwalificeerde certificaten, voor het verschaffen van informatie over de geldigheid van het certificaat of voor het ondertekenen van certificaten met betrekking tot elektronische tijdstempelsleutels;
c) tijdstempelsleutels, gebruikt voor het aanmaken en verifiëren van tijdstempels.

B. Algemene informatie

Het doel van dit document is om in algemene termen de procedures en normen te beschrijven die de afgifte van gekwalificeerde certificaten door QTSP INTESA regelen.

De bovengenoemde normen en procedures zijn gebaseerd op de huidige geldende regelgeving; dankzij de naleving van het voorgaande is INTESA opgenomen in de lijst van geaccrediteerde certificeringsinstanties.

In overeenstemming met de bovengenoemde regelgeving, zijn er dus meerdere entiteiten betrokken bij het

proces, zoals verderop in dit document wordt aangegeven.

B.1. Identificatiegegevens van de gebruikshandleidingsversie

Dit document is versie *04* van de *gebruikshandleiding voor procedures van gekwalificeerde elektronische ondertekening op afstand in de bank- en financiële sector,* uitgegeven overeenkomstig artikel 40 van het DPCM.

De objectidentifier van dit document is **1.3.76.21.1.50.110**.

De gebruikshandleiding is gepubliceerd en kan elektronisch worden geraadpleegd:

- op de QTSP website, *https://www.intesa.it/e-trustcom/*
- op de AgID website, *www.agid.gov.it*
- op de officiële website van de bank/instelling.

Opmerking: geactualiseerde versies van deze gebruikshandleiding kunnen alleen worden gepubliceerd met voorafgaande toestemming van het AgID [Agentschap voor Digitaal Italië].

B.2. Identificatiegegevens QTSP – Gekwalificeerde verlener van vertrouwensdiensten

De onderneming In.Te.S.A. S.p.A. is de QTSP (Qualified Trust Service Provider). De identificatiegegevens worden hieronder verstrekt.

Bedrijfsnaam	**In.Te.S.A. S.p.A.**
Statutaire zetels	**Strada Pianezza, 289** **10151 Turijn**
Wettelijke vertegenwoordiger	**Afgevaardigd bestuurder**
Handelsregister Turijn	**Registratienummer 1692/87**
BTW-nr.	**05262890014**
Telefoonnummer (centrale)	**+39.011.19216.111**
Website	**www.intesa.it**
E-mailadres	**marketing@intesa.it**
Adres certificatenlijst (URL)	**ldap://x500.e-trustcom.intesa.it**
ISO Objectidentifier (OID)	**1.3.76.21.1**

De volgende personeelsleden zijn verantwoordelijk voor de certificeringsactiviteiten, overeenkomstig artikel 38 van het DCPM:

a) Beveiligingsmanager.
b) Servicemanager tijdstempel en certificering.
c) Technisch systeembeheerder.
d) Manager logistiek en technische diensten.
e) Inspectie- en auditmanager.

De bovengenoemde personen maken allemaal deel uit van de QTSP INTESA-organisatie.

B.3. Verantwoordelijkheid voor de gebruikshandleiding

In overeenstemming met artikel 40, lid 3, onder c) van het DCPM is de certificeringsinstantie INTESA verantwoordelijk voor deze handleiding en houdt zij toezicht op de opstelling en publicatie ervan.

INTESA ontvangt graag opmerkingen en verzoeken om verduidelijking via de volgende kanalen:

via e-mail aan:	*marketing@intesa.it*
telefonisch op:	+39 011.192.16.111
via de Helpdesk service	voor oproepen binnen Italië: 800.80.50.93
	voor oproepen buiten Italië: +39 02.871.193.396

B.4. De bij de processen betrokken entiteiten

Binnen de QTSP-organisatie zijn er speciale entiteiten aangesteld om een deel van het proces uit te voeren dat verband houdt met de afgifte van certificaten.

Deze entiteiten werken in overeenstemming met de door de QTSP vastgestelde voorschriften en processen en vervullen de delen van de aan hen toegewezen taken.

B.4.1. Certificeringsinstantie (CA)

Overeenkomstig de bepalingen van het DPCM, de CAD en de eIDAS-verordening, voert INTESA de activiteiten van gekwalificeerde verlener van vertrouwensdiensten uit. Dergelijke activiteiten omvatten gekwalificeerde vertrouwensdiensten waarbij elektronische handtekeningen, elektronische zegels en elektronische tijdstempels worden gegenereerd, geverifieerd en gecertificeerd.

De identificatiegegevens van QTSP INTESA zijn opgenomen in het vorige punt *B.2*.

B.4.2. Lokale registratieautoriteit (LRA)

Voor het specifieke type dienst (gekwalificeerde elektronische ondertekening op afstand voor bancaire en financiële toepassingen) dat in deze gebruikshandleiding wordt beschreven, delegeert QTSP INTESA de taken van registratieautoriteit aan de bank/instelling die van de dienst gebruikmaakt.

De LRA verbindt zich ertoe de volgende taken uit te voeren:

- identificatie van de houder;
- registratie van de houder.

Bij de uitoefening van de rol van registratieautoriteit dient de bank/instelling toezicht te houden op de identificatieactiviteiten om ervoor te zorgen dat deze worden uitgevoerd in overeenstemming met de geldende wetgeving en de bepalingen van deze handleiding.

Met name kan de bank/instelling, in overeenstemming met de anti-witwasvoorschriften, de houder identificeren (*due diligence*), ook wanneer deze niet persoonlijk aanwezig in een filiaal is.

In dit geval dient de bank/instelling:

- de identiteit van de houder vast te stellen aan de hand van documenten, gegevens of aanvullende informatie zoals openbare documenten, gewaarmerkte onderhandse akten, certificaten die worden gebruikt om een gekwalificeerde elektronische handtekening te genereren in verband met elektronische documenten of op basis van de verklaring van een Italiaanse consulaire autoriteit;
- aanvullende maatregelen te nemen voor de verificatie van de verstrekte documenten, waaronder bijvoorbeeld een bevestigingsverklaring van een onder de richtlijn vallende krediet- of financiële instelling;
- documenten te gebruiken om te bewijzen dat de opdracht afkomstig is van een rekening op naam van de klant.

C. Verplichtingen

C.1. Verplichtingen van de gekwalificeerde verlener van vertrouwensdiensten (QTSP)

Bij de uitvoering van zijn functie, handelt de gekwalificeerde verlener van vertrouwensdiensten (ook de *Geaccrediteerde certificeringsinstantie* genoemd) in overeenstemming met de voorschriften van:

- Italiaans wetgevend besluit nr. 82 van 7 maart 2005 en latere wijzigingen.
- Besluit van de Italiaanse minister-president van 22 februari 2013.
- Verordening (EU) 2016/679 (AVG)
- Verordening (EU) 910/2014 (eIDAS)

De QTSP:

- voert alle passende organisatorische en technische maatregelen uit om schade aan anderen te

voorkomen;

- voldoet aan de technische normen van het DPCM en latere wijzigingen en aanvullingen;
- waarborgt dat zijn kwaliteitssysteem voldoet aan de normen ISO 9001;
- waarborgt dat het apparaat voor het aanmaken van handtekeningen (HSM) voldoet aan de veiligheidseisen als bedoeld in artikel 29 van de eIDAS-verordening;
- geeft het gekwalificeerde certificaat af en maakt het openbaar, tenzij anders vermeld door de houder, overeenkomstig artikel 32 van de CAD;
- verstrekt de aanvragers duidelijke en expliciete informatie over het certificeringsproces, de technische vereisten om hiertoe toegang te krijgen, de kenmerken van de handtekeningen die op basis van de certificeringsdienst zijn afgegeven en de beperkingen op het gebruik ervan;
- leeft de veiligheidsmaatregelen na met betrekking tot de verwerking van persoonsgegevens (AVG);
- is geen bewaarplaats van de gegevens die worden gebruikt voor het aanmaken van de handtekening van de houder;
- trekt het elektronische certificaat in of schort het op wanneer de houder of de belanghebbende derde daarom verzoekt;
- garandeert een nauwkeurige specificatie van de datum en het tijdstip van afgifte, intrekking en opschorting van elektronische certificaten;
- houdt alle informatie met betrekking tot het gekwalificeerde certificaat gedurende 20 (twintig) jaar bij, ook elektronisch, met name met het oog op het verstrekken van een bewijs van certificering in geval van gerechtelijke procedures;
- waarborgt dat de (voor de QTSP exclusieve) identificatiecode die aan elke houder is toegekend, uniek is onder zijn gebruikers;
- verstrekt alle informatie die nuttig kan zijn voor personen die een aanvraag indienen voor het gebruik van de certificatiedienst op een duurzame drager. Deze informatie omvat: de precieze voorwaarden voor het gebruik van het certificaat, met inbegrip van eventuele beperkingen op het gebruik ervan, het bestaan van een optionele accreditatieregeling en de klachten- en geschillenbeslechtingsprocedures. Deze informatie, die elektronisch kan worden verzonden, moet in eenvoudige en duidelijke taal worden geschreven en moet worden verstrekt voordat de overeenkomst tussen de aanvrager en de QTSP tot stand komt;
- gebruikt betrouwbare systemen om de certificatenlijst zodanig te beheren dat alleen bevoegde personen gegevens kunnen invoeren en wijzigingen kunnen aanbrengen, dat de authenticiteit van de informatie kan worden gecontroleerd, dat de certificaten alleen met toestemming van de houder van het certificaat publiek kunnen worden geraadpleegd en dat de operator eventuele gebeurtenissen die de veiligheidseisen in het gedrang kunnen brengen, kan identificeren;
- registreert de afgifte van gekwalificeerde certificaten in het controlelogboek, met vermelding van de datum en het tijdstip van afgifte.

In overeenstemming met artikel 14 van het DPCM beveelt de certificeringsinstantie minstens één systeem aan dat de verificatie van digitale handtekeningen mogelijk maakt.

De QTSP:

- genereert een gekwalificeerd certificaat voor elk van de geavanceerde elektronische handtekeningensleutels die AgID gebruikt om de openbare lijst van certificeringsinstanties te ondertekenen, en publiceert deze in haar eigen certificatenlijst in overeenstemming met artikel 42 van het DPCM;
- beveelt een systeem voor de verificatie van elektronische handtekeningen aan, zoals bedoeld in artikel 10 van het DPCM;
- houdt een kopie bij van de door AgID ondertekende lijst van certificaten die verbonden zijn aan de in artikel 43 van het DPCM bedoelde certificeringssleutels en publiceert deze elektronisch overeenkomstig artikel 42, lid 3, van het DPCM.

C.2. Verplichtingen van de houder

De houder die een gekwalificeerd certificaat aanvraagt voor de in deze gebruikshandleiding beschreven

diensten is een klant van de bank of de betalingsinstelling die als registratieautoriteit optreedt.

De houder ontvangt een gekwalificeerd certificaat voor de elektronische ondertekening op afstand, dat kan worden gebruikt voor het ondertekenen van contracten en documenten met betrekking tot producten en/of diensten die door de bank/instelling worden aangeboden volgens de in punt . beschreven methoden.

De houder is verplicht de informatie die nodig is voor het gebruik van zijn particuliere ondertekensleutel op passende wijze op te slaan en geschikte organisatorische en technische maatregelen te nemen om schade aan anderen te voorkomen (CAD, artikel 32, lid 1).

De houder van de sleutel is ook verplicht om:

- alle door de QTSP gevraagde informatie te verstrekken en de juistheid ervan te garanderen onder zijn/haar eigen verantwoordelijkheid;
- de certificeringsaanvraag in te dienen volgens de in deze handleiding aangegeven methoden;
- de QTSP, ook via de lokale registratieautoriteiten, op de hoogte te brengen van wijzigingen in de informatie die tijdens de registratie wordt verstrekt: persoonlijke gegevens, adres, telefoonnummers, e-mailadressen, enz;
- de informatie waarmee de privésleutel wordt geactiveerd, met de grootst mogelijke zorg en zorgvuldigheid op te slaan;
- het verlies of de diefstal van de codes en/of apparaten die nodig zijn voor toegang tot de ondertekensleutels onmiddellijk te melden aan de bevoegde autoriteiten en aan de bank/instelling; de bank/instelling zal ervoor zorgen dat het certificaat onmiddellijk wordt ingetrokken;
- eventuele verzoeken tot intrekking of opschorting van het digitale certificaat te verzenden volgens de instructies in deze gebruiksaanwijzing.

C.3. Verplichtingen van de gebruikers van certificaten

Met de gebruiker (*Relying Party*) wordt iedere persoon bedoeld die een digitaal ondertekend document ontvangt en voor de controle van de geldigheid ervan gebruik maakt van het gekwalificeerde certificaat dat door de houder is gebruikt om dat document te ondertekenen.

De controle van de digitale handtekening en de daaropvolgende extractie van de ondertekende objecten kan worden uitgevoerd met behulp van elke software die in staat is om overeenkomstig de eIDAS-verordening ondertekende bestanden te verwerken.

Personen die een gekwalificeerd certificaat gebruiken om de geldigheid van een digitaal ondertekend document te verifiëren, zijn verplicht om:

- de geldigheid van het certificaat dat de publieke sleutel bevat van de houder die het bericht heeft ondertekend, te verifiëren overeenkomstig de op het moment van afgifte geldende normen;
- de geldigheid van het certificaat te verifiëren met behulp van het OCSP-protocol of door toegang te krijgen tot de intrekkingslijsten;
- de geldigheid van het certificeringspad te verifiëren, op basis van de openbare lijst van QTSPs;
- te controleren of er beperkingen zijn op het gebruik van het door de houder gebruikte certificaat.

C.4. Verplichtingen van de belanghebbende derde

De bank of betalingsinstelling is de belanghebbende derde voor de in deze gebruikshandleiding beschreven diensten. Als zodanig moet de bank/instelling, handelend als belanghebbende derde:

- nagaan of de klant aan alle noodzakelijke vereisten voldoet en de klant machtigen om een gekwalificeerd certificaat voor digitale handtekeningen op afstand aan te vragen;
- de houder voorzien van ondersteunende diensten;
- de QTSP op de hoogte stellen van eventuele aanvullende beperkingen op het gebruik van het gekwalificeerd certificaat voor digitale handtekeningen, andere dan die welke zijn voorzien in punt *F.1.1*.

Als zodanig kan de bank/instelling, in haar hoedanigheid van belanghebbende derde, de QTSP in kennis stellen van eventuele beperkingen op het gebruik van het certificaat, en van eventuele vertegenwoordigingsbevoegdheden, en is zij verplicht om alle wijzigingen met betrekking tot deze beperkingen

te melden. Hieronder vallen bijvoorbeeld:

- wijzigingen van of intrekking van de vertegenwoordigingsbevoegdheden;
- veranderingen met betrekking tot interne rollen en functies;
- beëindiging van de arbeidsbetrekking.

Verzoeken van de belanghebbende derde aan de LRA om een certificaat in te trekken of op te schorten moeten onmiddellijk worden doorgestuurd naar de certificeringsinstantie, wanneer de houder niet langer voldoet aan de eisen op basis waarvan de elektronische handtekening is afgegeven.

C.5. Verplichtingen van externe registratieautoriteiten (LRA)

Om redenen die verband houden met het verlenen van de dienst, maakt QTSP INTESA gebruik van aanvullende partijen in het hele land (hierna externe RA's of LRA's - lokale registratieautoriteiten) voor de uitvoering van een aantal van de taken van haar registratieafdeling.

QTSP In.Te.S.A. S.p.A. delegeert de taken van de registratieautoriteit aan de bank of de betalingsinstelling zoals overeengekomen in een specifieke *lastgevingsovereenkomst*, die door beide partijen is ondertekend.

Meer in het bijzonder voeren externe RA's de volgende taken uit:

- positieve identificatie van de persoon die de certificering aanvraagt (hierna de certificaathouder);
- registratie van de aanvrager/houder;
- de houder voorzien van de apparaten en/of codes waarmee hij/zij toegang krijgt tot zijn/haar ondertekensleutel in overeenstemming met de artikelen 8 en 10, lid 2, van het DPCM;
- het verzenden van documentatie ondertekend door de RA-afdeling van QTSP INTESA, tenzij anders overeengekomen in de lastgevingsovereenkomst.

In de lastgevingsovereenkomst zijn de verplichtingen die bindend zijn voor de door QTSP INTESA als LRA aangewezen bank/instelling uitdrukkelijk vastgelegd; de naleving hiervan moet door de QTSP worden gecontroleerd.

Meer in het bijzonder zijn de LRA's verplicht het volgende te doen:

- ervoor te zorgen dat de identificatieactiviteiten worden uitgevoerd in overeenstemming met de lokale regelgeving (de CAD, en volgende wijzigingen, het DPCM, de eIDAS-verordening en de anti-witwasregelgeving);
- de tijdens het identificatieproces verkregen persoonsgegevens te gebruiken en te verwerken in overeenstemming met de AVG;
- het tijdens het identificatie- en registratieproces verzamelde materiaal ter beschikking te stellen van QTSP INTESA.

De identificatiedienst (*due diligence*) kan op drie verschillende manieren worden uitgevoerd, zoals hieronder beschreven:

- *Standaard*: de aanvrager wordt geïdentificeerd in een filiaal van de bank of betalingsinstelling;
- *On demand*: wanneer een nieuwe rekening-courant wordt geopend, kan de aanvrager vragen dat er contact met hem/haar wordt opgenomen door een persoonlijk financieel adviseur die een afspraak zal maken om de klant bij te staan bij alle procedures voor het openen van een rekening-courant. In dit stadium zal de klant (nadat hij/zij naar behoren is geïdentificeerd en geregistreerd) hulp krijgen bij het aanvragen van een gekwalificeerd certificaat voor elektronische handtekeningen;
- *Online*: indien de aanvrager de methode van directe inschrijving selecteert en reeds een rekening-courant bij een nationale bank heeft, kan hij/zij voor wettelijke doeleinden worden geïdentificeerd met behulp van de volgende methoden:
  - via een SEPA-procedure (of SDD - SEPA Direct Debit);
  - door het uitvoeren van een overschrijving van de bestaande rekening-courant bij de voormelde bank.

De LRA of de bank of betalingsinstelling zal bij het gebruik van de voormelde methoden alle wettelijk verplichte informatie ontvangen op een absoluut veilige manier en met volledige inachtneming van de privacyvereisten.

D. Aansprakelijkheid en beperkingen van schadevergoeding

D.1. Aansprakelijkheid van de QTSP - Beperkingen van schadevergoeding

QTSP INTESA is jegens de houders aansprakelijk voor de naleving van alle verplichtingen die voortvloeien uit de uitvoering van de activiteiten die zijn voorzien in het DPCM, de AVG, de CAD en de eIDAS-verordening (en volgende wijzigingen en aanvullingen), zoals beschreven in punt *C.1.Verplichtingen van de gekwalificeerde verlener van vertrouwensdiensten (QTSP)*.

Behalve in gevallen van opzettelijk wangedrag of nalatigheid (artikel 13, eIDAS-verordening), kan INTESA niet aansprakelijk worden gesteld voor gevolgen die voortvloeien uit het gebruik van de certificaten anders dan dat voorzien in artikel 5 van het DPCM, en in het bijzonder het niet naleven van de houder en de belanghebbende derde van deze gebruikshandleiding en/of de geldende regelgeving.

INTESA is evenmin aansprakelijk voor gevolgen die voortvloeien uit omstandigheden die niet aan haar zijn toe te schrijven, met inbegrip van, maar niet beperkt tot: natuurrampen, storingen in de dienstverlening en/of technische en logistieke storingen die buiten haar controle vallen, interventies door autoriteiten, rellen of oorlogshandelingen die ook of alleen gevolgen hebben voor entiteiten waarvan INTESA gebruik maakt voor het verlenen van haar certificeringsdiensten.

QTSP INTESA kan niet aansprakelijk worden gesteld voor schade als gevolg van oneigenlijk gebruik van het gekwalificeerde certificaat voor digitale ondertekening op afstand, met betrekking tot de beperking van het gebruik ervan zoals aangegeven in punt *F.1.1*.

De houder moet, na het lezen van deze handleiding, alle passende speciale *due diligence*-maatregelen nemen om schade aan derden in verband met oneigenlijk gebruik van het door de geaccrediteerde certificeringsinstantie verstrekte materiaal te voorkomen. In het bijzonder moeten de OTP-apparaten en geheime codes die nodig zijn om toegang te krijgen tot de ondertekensleutels, met de nodige zorgvuldigheid worden opgeslagen.

D.2. Verzekering

QTSP INTESA heeft verzekeringspolissen afgesloten om risico's in verband met de activiteiten en schade aan derden te dekken, waarvan de inhoud voldoet aan de eisen voor het uitoefenen van de beroepsactiviteiten in kwestie.

AgID heeft een specifieke verklaring over het bestaan van een dergelijke polis ontvangen.

E. Tarieven

De dienst wordt door de bank of betalingsinstelling aan haar klanten verleend. De kosten voor afgifte, vernieuwing, intrekking of opschorting van het gekwalificeerde certificaat zijn vermeld in de overeenkomsten die tussen de klant en de bank/instelling worden gesloten.

F. Methoden voor de identificatie en registratie van de gebruikers

F.1. Identificatie van de gebruiker

De QTSP moet de identiteit van elke aanvrager met zekerheid vaststellen, wanneer deze voor het eerst een gekwalificeerd certificaat aanvraagt.

De voornoemde taak is gedelegeerd aan de bank/instelling die, in haar hoedanigheid van LRA en in overeenstemming met de bepalingen van de huidige anti-witwasregelgeving, de houder zal identificeren en registreren.

In het geval van verlengingsaanvragen terwijl het gekwalificeerde certificaat nog geldig is, hoeft de activiteit niet te worden herhaald: de houder is verantwoordelijk voor de kennisgeving aan de QTSP via de bank/instelling van eventuele wijzigingen in zijn/haar registratiegegevens.

De registratiegegevens die nodig zijn om de dienst waarop dit document betrekking heeft uit te voeren, omvatten:

- naam en achternaam;

- geboortedatum;
- geboorteplaats of buitenlands geboorteland;
- fiscaal identiteitsnummer (of gelijkwaardig);
- woonadres;
- adres waarnaar schriftelijke berichten moeten worden gestuurd;
- mobiel telefoonnummer;
- e-mailadres;
- type en nummer van het verstrekte identificatiedocument;
- naam van de autoriteit die het identificatiedocument heeft afgegeven, datum en plaats van afgifte en vervaldatum.

Zodra het registratieproces is voltooid, kan aan de houder een One Time Password-apparaat worden verstrekt op basis van bruikleen; dit apparaat heeft een scherm en kan numerieke codes voor eenmalig gebruik aanmaken (ook bekend als OTP-codes of kortweg OTPs).

Als alternatief voor een fysiek OTP-token kan de bank of de betaalinstelling de houder instructies geven voor het activeren van een software-authenticatiesysteem voor mobiele apparaten (als de houder hierover beschikt en deze methode verkiest boven het ontvangen van een fysiek token op bruikleenbasis). Met dit softwaresysteem kan een eenmalig wachtwoord worden gegenereerd op het mobiele apparaat van de houder, dat vervolgens kan worden gebruikt als authenticatiemiddel voor de systemen voor ondertekening op afstand.

Naast het OTP krijgt de houder alle nodige informatie en een persoonlijk identificatienummer (PIN) om een veilige toegang tot de dienst voor ondertekening op afstand van de bank/instelling te waarborgen.

Dezelfde PIN-code kan worden gebruikt als noodcode (bijvoorbeeld in het geval dat het OTP-token of het mobiele apparaat verloren gaat en/of kwijtgeraakt is) om het hem/haar toegewezen gekwalificeerde certificaat met spoed op te schorten (punt *H.2.2*).

De houder kan vervolgens de PIN-code wijzigen of actualiseren tijdens het gebruik van de door de bank/ betalingsinstelling verleende diensten.

In deze fase zal de houder ook informatie krijgen over hoe hij het verstrekte mobiele nummer op elk moment kan wijzigen.

Bovendien moet de houder tijdens de inschrijving bij de bank/instelling, of later, door in te loggen op de door de bank/instelling verleende internetbankieren-dienst, en in elk geval vóór de aanvraag van een gekwalificeerd certificaat:

- de QTSP INTESA-gebruikshandleiding lezen;
- de bank of betalingsinstelling toestemming geven om zijn/haar persoonsgegevens te verwerken voor doeleinden die verband houden met de afgifte van een gekwalificeerd certificaat voor elektronische handtekeningen.

De voormelde registratiedocumenten van de houder worden gedurende 20 (twintig) jaar na het verstrijken van het certificaat bewaard.

F.1.1. Beperkingen op het gebruik

Het gekwalificeerde certificaat voor elektronische handtekeningen, afgegeven in verband met de diensten beschreven in deze handleiding en aangeboden door de bank/instelling, is altijd onderworpen aan beperkingen op het gebruik ervan.

De standaardformule is als volgt:

Dit certificaat mag alleen worden gebruikt in transacties met naam van de bank/instelling.

Er kunnen bepaalde gebruiksbeperkingen met de bank of betaalinstelling worden overeengekomen.
INTESA is niet aansprakelijk voor schade die voortvloeit uit het gebruik van een gekwalificeerd certificaat op een wijze die niet overeenstemt met de daaraan verbonden beperkingen, of die voortvloeit uit de niet-naleving van dergelijke beperkingen.

F.1.2. Beroepstitels of -kwalificaties

Indien de beroepskwalificaties in het gekwalificeerde certificaat (bv. lidmaatschap van een beroepsvereniging) moeten worden gespecificeerd, moet de aanvrager passende documentatie indienen om aan te tonen dat hij/zij daadwerkelijk in het bezit is van dergelijke kwalificaties.

Een elektronische kopie van deze documenten wordt gedurende 20 (twintig) jaar na het verstrijken van de geldigheidsduur van het certificaat bewaard.

De documentatie die wordt verstrekt ter ondersteuning van verzoeken om beroepstitels of -kwalificaties in een gekwalificeerd certificaat op te nemen, mag niet later gedateerd zijn dan 10 (tien) dagen vóór de indiening van het verzoek tot afgifte van het certificaat.

INTESA kan niet aansprakelijk worden gesteld voor schade die voortvloeit uit het oneigenlijke gebruik van een gekwalificeerd certificaat met informatie over beroepskwalificaties.

In geval van zelfcertificering aanvaardt INTESA geen enkele aansprakelijkheid, behalve in geval van opzettelijk wangedrag of nalatigheid (eIDAS-verordening, artikel 13), voor het opnemen van eventuele informatie inzake de zelfcertificering in het certificaat door de houder.

F.1.3. Vertegenwoordigingsbevoegdheden

Bij verzoeken om in het gekwalificeerde certificaat de vertegenwoordigingsbevoegdheid te specificeren (bv. dat de houder tot een organisatie behoort en zijn/haar functie daarin, de bevoegdheid om in naam en voor rekening van een klant op te treden, enz.), dient de aanvrager passende documentatie in te dienen waaruit blijkt dat hij/zij werkelijk over deze vertegenwoordigingsbevoegdheden beschikt.

In geval van vertegenwoordigingsbevoegdheden voor natuurlijke personen, moet de aanvrager een gewaarmerkt afschrift van de door een notaris opgestelde en door de vertegenwoordigde persoon ondertekende machtiging of volmacht indienen, naast een verklaring van instemming van de vertegenwoordigde persoon met betrekking tot opname van die rol in het certificaat.

In geval van verzoeken om in het certificaat aan te geven dat de houder de bevoegdheid heeft om organisaties of privaatrechtelijke entiteiten te vertegenwoordigen, moet de houder documentatie indienen waaruit blijkt welke functie hij/zij in het certificaat wil opnemen, evenals een verklaring van de betreffende organisatie of entiteit, waarmee de QTSP wordt gemachtigd om deze functie in het certificaat op te nemen. Dit laatste document mag niet meer dan 20 (twintig) dagen vóór de datum van aanvraag van het gekwalificeerde certificaat zijn afgegeven.

Voor opname in het gekwalificeerde certificaat van informatie over openbare ambten of vertegenwoordigingsbevoegdheden met betrekking tot overheidsinstanties of organisaties, zijn specifieke overeenkomsten met deze entiteiten van toepassing. Op basis van dergelijke overeenkomsten, kan de rol van de houder binnen de overheidsinstantie of -organisatie nader worden aangegeven.

Alle ingediende documentatie wordt gedurende 20 (twintig) jaar bewaard.

INTESA kan niet aansprakelijk worden gesteld voor schade die voortvloeit uit het oneigenlijke gebruik van een gekwalificeerd certificaat met informatie over vertegenwoordigingsbevoegdheden.

F.1.4. Gebruik van pseudoniemen

Onder bepaalde omstandigheden kan de houder verzoeken om een pseudoniem op het certificaat te vermelden, in plaats van zijn of haar werkelijke gegevens.

De gegevens van de werkelijke identiteit van de gebruiker worden gedurende 20 (twintig) jaar opgeslagen.

F.2. Registratie van gebruikers die een certificaat aanvragen

Zodra het identificatieproces is voltooid, worden de gegevens van de houder opgenomen in de bestanden van de certificeringsinstantie.

Dit proces kan worden uitgevoerd met behulp van een softwareprogramma dat rechtstreeks toegankelijk is via de applicaties van de bank of betalingsinstelling.

G. Het aanmaken van certificerings-, tijdstempel- en ondertekensleutels

G.1. Het aanmaken van certificeringssleutels

Sleutels worden aangemaakt op ondertekenapparaten in aanwezigheid van de certificeringsmanager, zoals voorzien in artikel 7 van het DPCM.

Deze handelingen worden voorafgegaan door de initialisatie van de ondertekenapparaten voor het systeem dat de certificaten aanmaakt om de certificaten van de houders te ondertekenen en die voor het tijdstempelsysteem.

Deze handelingen worden uitgevoerd in een dual control-modus om illegale activiteiten te voorkomen.

Zodra een sleutelpaar voor certificering is aangemaakt, kunnen de transacties alleen worden uitgevoerd met specifieke autorisatieapparaten (USB-tokens): uitgebreide toegang tot HSM's kan alleen worden verkregen met behulp van de sleutels die in de hierboven genoemde autorisatieapparaten zijn opgenomen.

Om de veiligheid te verhogen, worden dergelijke sleutels verdeeld over meerdere apparaten, met behulp van een logica van het type “n-van-m”; als zodanig kunnen bewerkingen met de betrokken bevoegdheden alleen worden uitgevoerd in de gelijktijdige aanwezigheid van ten minste *n* van *m* delen van de sleutel. Deze worden in afzonderlijke, speciale kluizen bewaard.

De certificeringssleutels hebben een lengte van minstens 2048 bits.

G.2. Het aanmaken van sleutels voor het tijdstempelsysteem

Sleutels voor tijdstempels worden in overeenstemming met de voorschriften van artikel 49 van het DPCM aangemaakt. De sleutels voor het tijdstempelsysteem hebben een lengte van minstens 2048 bits.

G.3. Het aanmaken van ondertekensleutels

Zodra het registratieproces – tijdens welke de gegevens van de houder worden opgeslagen in de bestanden van de certificeringsinstantie – is voltooid, kan de ondertekensleutel worden aangemaakt.

De houder kan het aanmaakproces van de sleutel starten en het bijbehorende handtekeningcertificaat aanvragen via een van de methoden die zijn beschreven in punt *I. Werkprocedures voor het ondertekenen van documenten*.

De sleutelparen voor ondertekening worden gegenereerd op veilige ondertekenapparaten (HSM - Hardware Security Module), die voldoen aan de specificaties van bijlage II van de eIDAS-verordening.

De ondertekensleutels hebben een lengte van minstens 2048 bits.

H. Procedures voor de afgifte van certificaten

H.1. Procedures voor de afgifte van certificeringscertificaten

Na het aanmaken van de certificeringssleutels, beschreven in punt *G.1*, worden publieke sleutelcertificaten gegenereerd in overeenstemming met de bepalingen van het DPCM, ondertekend met de betreffende privésleutels en geregistreerd in de certificatenlijst volgens de voorziene methoden.

De certificeringssleutelcertificaten worden naar AgID gestuurd met behulp van het in artikel 12, lid 1, DPCM bedoelde communicatiesysteem.

De certificeringsinstantie genereert een gekwalificeerd certificaat voor elk van de gekwalificeerde elektronische ondertekensleutels die door AgID worden gebruikt om de publieke lijst van certificeringsinstanties te ondertekenen, en publiceert deze in haar certificatenlijst. De certificeringsinstantie moet vervolgens een kopie van de door de afdeling ondertekende lijst van de certificaten met betrekking tot de certificeringssleutels bewaren en deze elektronisch ter beschikking stellen (artikel 42, lid 1 en lid 3, van het DPCM).

H.2. Procedures voor de afgifte van ondertekencertificaten

Het systeem van INTESA voor de afgifte van certificaten is in overeenstemming met artikel 33 van het DPCM.

Na de generatie van het sleutelpaar, beschreven in punt *G.3*, wordt een aanvraag gegenereerd voor een

nieuw certificaat in PKCS#10-formaat, dat automatisch het bezit van de privésleutel bewijst en controleert of het sleutelpaar goed werkt.

Zodra de sleutels zijn gegenereerd, wordt onmiddellijk een certificaataanvraag vanaf de applicatie van de bank/instelling naar de certificeringsinstantie van de QTSP gestuurd.

Het genereren van het certificaat wordt geregistreerd in het controlelogboek (DPCM, artikel 18, lid 4).

H.2.1. De in de ondertekencertificaten bevatte informatie

INTESA-certificaten, die in overeenstemming met deze handleiding worden afgegeven, zijn gekwalificeerde certificaten overeenkomstig EU-verordening nr. 910/2014 (eIDAS) en derhalve zijn hun interoperabiliteit en erkenning op EU-niveau gegarandeerd.

Het gekwalificeerde certificaat identificeert ondubbelzinnig de CA die het heeft afgegeven en bevat de gegevens die nodig zijn om de digitale handtekening te verifiëren.

Elk gekwalificeerd certificaat voor elektronische handtekeningen voldoet aan de eIDAS-verordening en de AgID- BEPALING nr. 147/2019 (*Richtsnoeren bevattende technische normen en aanbevelingen inzake het genereren van certificaten*).

Alle gekwalificeerde certificaten die worden afgegeven als onderdeel van de diensten die in dit handboek worden beschreven, bevatten ten minste één beperking op het gebruik ervan (punt *F.1.1*).

H.2.2. Noodcode

In overeenstemming met de bepalingen van artikel 21 van het DPCM garandeert de certificeringsinstantie dat er een *noodcode* wordt verstrekt die kan worden gebruikt om de ***dringende opschorting*** van het certificaat aan te vragen.

Voor de in deze gebruikshandleiding beschreven toepassingen dient de tijdens de registratie aan de houder verstrekte pincode als noodcode.

I. Werkprocedures voor het ondertekenen van documenten

QTSP INTESA stelt via de diensten van de bank of de betalingsinstelling de houder de middelen ter beschikking om gekwalificeerde elektronische handtekeningen te genereren in overeenstemming met de bepalingen van de geldende regelgeving.

Voor het specifieke type dienst in kwestie is het niet nodig dat er een handtekeningapplicatie wordt geïnstalleerd op de personal computer van de houder. In plaats daarvan is de ondertekeningsfunctie toegankelijk via de dienst voor thuisbankieren die door de bank of betalingsinstelling wordt aangeboden, of kan persoonlijk bij een filiaal van de bank of betalingsinstelling plaatsvinden.

Gekwalificeerde elektronische handtekeningen die met behulp van deze methoden worden aangebracht, zijn volledig in overeenstemming met de bepalingen van artikel 4, lid 2, van het DPCM inzake de gebruikte algoritmen.

Bovendien zullen deze documenten, zoals bepaald in artikel 4, lid 3, van het DPCM, geen macro-instructies of uitvoerbare codes bevatten die functies zouden kunnen activeren die, zonder dat de houder dat merkt, records, feiten en gegevens in de ondertekende documenten zouden kunnen bewerken.

Hieronder worden twee verschillende authenticatiemethoden beschreven die, in overeenstemming met de huidige regelgeving, de geregistreerde houders in staat stellen om eerst ondertekensleutels te genereren en een gekwalificeerd certificaat aan te vragen, en deze vervolgens te gebruiken om transacties met gekwalificeerde elektronische handtekeningen uit te voeren.

Succesvolle ondertekeningstransacties worden bevestigd via sms. Als de houder een smartphone heeft geconfigureerd om berichten te lezen, kan hij/zij vragen om een bevestiging per e-mail (in plaats van per sms) te ontvangen.

I.1. Authenticatie van het type “Call Drop"

Deze authenticatiemethode vereist dat de gebruiker, die al eerder is geïdentificeerd, vanaf zijn of haar mobiele telefoon belt (vanaf het nummer dat tijdens het identificatieproces is opgegeven) naar een specifiek telefoonnummer dat door de dienst is opgegeven, om te bevestigen dat hij/zij een document wil

ondertekenen.

Na ontvangst van een dergelijke oproep zal worden gecontroleerd of het nummer dat voor de oproep wordt gebruikt (Call Identifier) overeenkomt met het nummer dat tijdens de registratie met de gebruiker is geassocieerd en, als de nummers overeenkomen, zal de gekwalificeerde elektronische handtekeningtransactie worden geautoriseerd.

Wanneer de houder dus een document wenst te ondertekenen door middel van toegang tot het portaal van de bank/instelling, zal hij/zij gebruik maken van een authenticatiesysteem op basis van twee factoren, waarbij een PIN-code (die alleen de gebruiker kent) en een telefoonnummer (gekoppeld aan de SIM-kaart, die alleen de gebruiker bezit) worden ingevoerd.

Dit type authenticatie wordt ook wel “Call Drop” genoemd, omdat wanneer de houder belt om de authenticatie uit te voeren, hij/zij niet hoeft te spreken en de oproep na enkele seconden wordt afgebroken.

De oproep van de houder wordt niet beantwoord en er worden dus geen gesprekskosten in rekening gebracht.

Deze methode is uiterst praktisch en kosteneffectief, omdat er geen fysiek authenticatie-apparaat nodig is. Ook is de methode zeer gebruiksvriendelijk.

We zullen hieronder zien dat deze authenticatiemethode met name wordt aanbevolen voor situaties waarin de houder vanaf “onbemande stations” werkt (bijvoorbeeld bij toegang tot de diensten van de bank of betalingsinstelling voor thuisbankieren vanaf zijn/haar PC). Deze methode is echter niet bijzonder praktisch wanneer de houder persoonlijk contact heeft met een externe operator, bijvoorbeeld in een station dat bemand is door een medewerker van de bank of de betalingsinstelling.

Voor deze laatste situaties is een oplossing ontwikkeld die gebaseerd is op een dynamisch beheer van de op te roepen telefoonnummers om het authenticatieproces vanuit “bemande stations” af te ronden.

I.1.1. Procedure voor ondertekening vanaf onbemande stations (thuisbankieren)

Na ontvangst van de vereiste codes tijdens het identificatieproces kan de houder overgaan tot het aanvragen van een digitaal certificaat en het ondertekenen van documenten volgens de hieronder beschreven methoden.

1. Allereerst dient de houder in te loggen op de bank- of financiële applicatie met behulp van zijn/haar persoonlijke toegangscodes voor de applicatie;
2. Vervolgens moet hij/zij het te ondertekenen document selecteren en verifiëren;
3. Daarna moet hij/zij zijn/haar PIN-code invoeren;
4. Nadat de PIN is gevalideerd, op een vooraf ingesteld tijdstip (niet meer dan een minuut eerder) en vanaf het geregistreerde mobiele nummer, moet de houder het telefoonnummer bellen dat als video op het scherm verschijnt, om te bevestigen dat hij/zij het document wil ondertekenen;
5. Zodra het systeem detecteert dat het nummer dat voor de oproep wordt gebruikt overeenkomt met dat van de houder, voert het de ondertekeningstransactie uit en stuurt het een bevestiging dat de handeling met succes is voltooid;
6. Als de toegewezen tijd verstrijkt zonder dat het systeem een oproep ontvangt op het in punt 4 bedoelde nummer, wordt de handeling als ongeldig beschouwd en wordt het document niet ondertekend.

Indien meer dan één document moet worden ondertekend, moet de houder de stappen 2 t/m 5 voor elk document herhalen.

I.1.2. Procedure voor ondertekening vanaf bemande stations (persoonlijk bij een bank of financiële instelling)

Na een gekwalificeerd certificaat te hebben verkregen, kan de houder overgaan tot het ondertekenen van documenten.

Zoals eerder gezegd, kan het zijn dat de houder bij het ondertekenen in aanwezigheid van een medewerker van een bank of financiële instelling geen persoonlijke en vertrouwelijke codes, zoals PIN-codes, kan invoeren.

Om deze reden is een alternatieve oplossing ontwikkeld, om maximale veiligheid te waarborgen:

1. de gebruiker gaat naar het filiaal van een bank-/financiële instelling (bemand station) en wordt door het personeel (bijvoorbeeld de bankbediende) met behulp van standaardmethoden geïdentificeerd;

2. na het lezen van het te ondertekenen document kan de houder beginnen met het ondertekeningsproces;
3. nu krijgt de houder een scherm te zien met een telefoonnummer (willekeurig gekozen uit een uitgebreide set beschikbare nummers) en wordt een timer geactiveerd;
4. de houder moet op een vooraf ingesteld tijdstip (en niet meer dan een minuut eerder) het nummer bellen dat op het scherm verschijnt (vanaf het geregistreerde mobiele nummer) om te bevestigen dat hij/zij het document wil ondertekenen;
5. als het systeem detecteert dat de oproep geldig is, zal het overgaan tot het ondertekenen van het document en stuurt het een sms-bericht om te bevestigen dat de transactie met succes is afgerond;
6. als de toegewezen tijd verstrijkt zonder dat het systeem een oproep ontvangt naar het nummer dat is opgegeven in punt 3, wordt de operatie geannuleerd.

Indien meer dan één document moet worden ondertekend, moet de houder de stappen 2 t/m 5 voor elk document herhalen.

I.2. Mobiele OTP-authenticatie

Als alternatief voor de “Call Drop”-authenticatiemethode is er een tweede authenticatiemethode die “Mobiele OTP” wordt genoemd.

Om deze methode te gebruiken, moet de houder beschikken over een van de smartphones die door de bank/instelling als geschikt voor de dienst zijn bevonden.

Na bevestiging hiervan ontvangt de houder tijdens de identificatiefase van het registratieproces bij de bank/instelling het adres van een specifieke pagina op de website van de bank of betalingsinstelling om een applicatie genaamd “Mobiele OTP” te downloaden op zijn/haar smartphone, evenals een pincode.

De procedure voor het uitvoeren van dit tweede type authenticatie op bemande en onbemande stations wordt hieronder beschreven.

I.2.1. Procedure voor ondertekening vanaf onbemande stations (thuisbankieren)

Na een gekwalificeerd certificaat te hebben ontvangen, kan de houder een document ondertekenen door de volgende stappen te volgen:

1. allereerst dient de houder in te loggen op de bank- of financiële applicatie met behulp van zijn/haar persoonlijke toegangscodes voor de applicatie;
2. vervolgens moet hij/zij het te ondertekenen document selecteren en verifiëren;
3. daarna moet hij/zij zijn/haar PIN-code invoeren;
4. vervolgens moet hij/zij de eerder op de smartphone gedownloade applicatie opstarten en ontvangt hij/zij een mobiele OTP die na de PIN-code moet worden ingevoerd;
   na verificatie van de ingevoerde PIN en mobiele OTP gaat het systeem over tot de ondertekening en stuurt het een bevestiging dat de operatie met succes is afgerond.

Indien meer dan één document moet worden ondertekend, moet de houder de stappen 2 t/m 5 voor elk document herhalen.

I.2.2. Procedure voor ondertekening vanaf bemande stations (persoonlijk bij een bank of financiële instelling)

Ook in dit geval is een oplossing ontwikkeld om te voorkomen dat de houder vertrouwelijke codes moet invoeren – die mogelijk worden hergebruikt om hem/haar te bestelen – ten overstaan van personeel van de bank of betalingsinstelling.

Na ontvangst van een gekwalificeerd certificaat kan de houder een document als volgt ondertekenen:

1. de gebruiker gaat naar het filiaal van een bank/betalingsinstelling (bemande post) en wordt door het personeel (bijvoorbeeld de bankbediende) met behulp van standaardmethoden geïdentificeerd;
2. bij het ondertekenen van het document krijgt de gebruiker een specifieke monitor te zien die met een webcam is uitgerust;
3. zodra het te ondertekenen document op de monitor is geverifieerd en de houder door wil gaan met de ondertekeningstransactie, moet hij/zij een OTP via zijn/haar smartphone genereren, die ook als

barcode zal worden weergegeven;

4. nu moet de houder zijn of haar smartphone voor de webcam houden, zodat de in stap 3 gegenereerde OTP kan worden gelezen en het feitelijke ondertekeningsproces kan beginnen;
5. zodra het document is ondertekend, zal het systeem de houder onmiddellijk per sms op de hoogte brengen.

Om meerdere documenten te ondertekenen moeten de stappen 2 t/m 5 worden herhaald.

I.2.3. Ondertekeningsprocedure voor potentiële klanten (*Prospects*)

De stappen om een gekwalificeerd certificaat voor handtekeningen op afstand te ontvangen kunnen ook worden uitgevoerd door potentiële klanten (*Prospects*) tijdens het Onboarding (*klantenwerving*)-proces.

Het proces is compatibel met alle belangrijkste browsers (Chrome, Firefox, Edge, Safari) en de meest recente versies van Android en Apple mobiele apparaten.

Potentiële klanten dienen als volgt te werk te gaan:

1. aan het begin van het proces wordt de *Prospect* gevraagd om zijn of haar persoonlijke gegevens in te voeren, zodat hij/zij positief kan worden geïdentificeerd na het privacybeleid van QTSP INTESA te hebben ondertekend;
2. de bankinstelling stuurt een sms met een OTP (*One Time Password*) dat voor een beperkte tijd geldig is. De *Prospect* moet die code invoeren om te bewijzen dat hij/zij toegang heeft tot het mobiele apparaat dat bij het invoeren van zijn/haar gegevens is opgegeven;
3. na voltooiing van het in het vorige punt bedoelde verificatieproces dient de *Prospect* de identiteitsdocumenten bij de bankinstelling in te dienen. De persoonsgegevens moeten door de *Prospect* worden ingevoerd of via OCR uit de documenten worden verkregen;
4. zodra het registratieproces is voltooid, stuurt de bank de contractuele documentatie naar de *Prospect*, die deze kan ondertekenen met behulp van een gekwalificeerd certificaat voor digitale handtekeningen op afstand, afgegeven door de QTSP INTESA;
5. zoals beschreven in verband met internetbankieren, zal de *Prospect* documentatie ontvangen om een certificaat aan te vragen bij de QTSP INTESA;
6. de *Prospect* moet de relevante vakjes op het document aanvinken om te bevestigen dat hij/zij het document heeft gelezen, en het elektronisch ondertekenen door een OTP in te voeren die per sms is ontvangen van QTSP INTESA;
7. als de verificatie van het van QTSP INTESA ontvangen OTP positief is, kan een gekwalificeerd certificaat worden afgegeven. In tegengesteld geval moet een nieuw OTP worden aangevraagd;
8. in ieder geval moet bij het genereren van het certificaat een pincode worden ingevoerd, die bij elk gebruik van het handtekeningcertificaat wordt opgevraagd;
9. certificaten die op deze manier worden afgegeven, kunnen alleen worden gebruikt om het contractvoorstel te ondertekenen. Zij kunnen niet worden gebruikt voor andere documenten totdat de bank de controles heeft uitgevoerd die nodig zijn om een rekening-courant te openen;
10. indien het resultaat van de door de bank uitgevoerde controles positief is, wordt de rekening-courant geopend en kan de *Prospect* gebruik maken van het certificaat dat is afgegeven voor transacties met de bank, in overeenstemming met de beperkingen op het gebruik ervan;
    als de bank daarentegen het verzoek om een rekening-courant te openen afwijst, wordt het certificaat ingetrokken en kan het niet langer worden gebruikt;
11. in beide gevallen zal de *Prospect* worden geïnformeerd over het resultaat van de controles en, in voorkomend geval, over de intrekking van het certificaat.

I.3. Authenticatie met een OTP-token

Ten slotte kan de authenticatie worden uitgevoerd met behulp van een fysiek OTP-token (zeer gebruikelijk in de bancaire en financiële sector).

Fysieke OTP-tokens worden momenteel alleen gebruikt op onbemande stations (normaal gesproken vanaf een thuisbankierstation).

De houder gebruikt zijn/haar persoonlijke codes om in te loggen op de bancaire of financiële applicatie, en

begint de ondertekeningsprocedure door zijn/haar PIN en OTP-code in te voeren die in de tussentijd is aangemaakt en op het scherm van het token wordt weergegeven.

J. Werkprocedures voor de controle van handtekeningen

Documenten die met behulp van bovengenoemde methoden zijn ondertekend, zijn uitsluitend in pdf-formaat: dit ondertekeningsformaat wordt als passend beschouwd voor gebruik in bancaire en financiële toepassingen.

Ondertekende documenten kunnen eenvoudig worden geverifieerd met behulp van Acrobat Reader DC-software, die alle soorten gekwalificeerde elektronische handtekeningen in pdf-formaat kan verifiëren die in de Europese Unie in overeenstemming met de eIDAS-verordening zijn geproduceerd.

Acrobat Reader DC kan gratis worden gedownload van de website: *https://www.adobe.com/it/*.

K. Procedure voor de intrekking en opschorting van certificaten

Overeenkomstig de eIDAS-verordening is informatie over de status van het certificaat beschikbaar via het OCSP-protocol op de URL die op het certificaat zelf is vermeld.

De intrekking en opschorting van certificaten kan worden geformaliseerd door ze op te nemen in de CRL-lijst (artikel 22 van het DPCM). Het CRL-profiel voldoet aan de RFC 3280-norm. Deze lijst, ondertekend door de certificeringsinstantie die het certificaat afgeeft, wordt met vooraf vastgestelde intervallen geactualiseerd in overeenstemming met de geldende regelgeving.

De CRL-lijst is ook beschikbaar in de certificatenlijst.

Wanneer de intrekking of opschorting plaatsvindt op verzoek van de CA of derde partij (artikelen 23, 25, 27 en 29 van het DPCM), stelt de bevoegde autoriteit de houder in kennis van het verzoek en van het tijdstip waarop het verzoek van kracht wordt.

De datum en het tijdstip waarop de intrekking in werking moet treden, moeten in het verzoek worden vermeld (artikel 24, lid 1, DPCM).

K.1. Intrekking van certificaten

Een certificaat kan worden ingetrokken op verzoek van de houder, de belanghebbende derde of de certificeringsinstantie (d.w.z. de QTSP).

Ingetrokken certificaten kunnen in geen geval opnieuw worden geactiveerd.

K.1.1. Intrekking op verzoek van de houder

De houder kan om intrekking verzoeken door zich te wenden tot een specifieke sectie van de onlinediensten van de bank of betalingsinstelling, of door rechtstreeks contact op te nemen met de klantenservice van de bank of betalingsinstelling.

Na kennisgeving door de bank/instelling, die in de tussentijd de toegangscodes van de houder heeft geblokkeerd, zal de QTSP het certificaat onmiddellijk intrekken.

K.1.2. Intrekking op verzoek van de belanghebbende derde

In haar hoedanigheid van belanghebbende derde kan de bank of betalingsinstelling om intrekking van het certificaat verzoeken.

De QTSP zal, na vaststelling van de geldigheid van het verzoek, de betrokken houders op de hoogte stellen van de intrekking via de met de houder overeengekomen kanalen op het moment van registratie, zoals later door de houder geactualiseerd en gemeld aan de QTSP, onder andere via de LRA's (punt *C.2. Verplichtingen van de houder*).

K.1.3. Intrekking op verzoek van de certificeringsinstantie

Behoudens in gerechtvaardigde dringende gevallen, stellen de certificeringsinstanties die een gekwalificeerd certificaat wensen in te trekken, de bank/instelling (belanghebbende derde partij) hiervan per e-mail op de hoogte en stellen zij de houder hiervan tegelijkertijd op de hoogte op het e-mailadres dat bij de aanvraag van

het certificaat is opgegeven, of op zijn/haar huisadres, met vermelding van de redenen voor de intrekking en de datum en het tijdstip waarop deze in werking zal treden.

K.1.4. Intrekking van certificaten met betrekking tot certificeringssleutels

In het geval dat:

- de certificeringssleutel gesaboteerd is,
- de betrokken activiteit wordt beëindigd,

zal de CA de corresponderende certificeringscertificaten en de met die certificeringssleutel ondertekende certificaten intrekken.

De CA zal AgID en de houders binnen 24 uur op de hoogte brengen van de intrekking.

K.2. Opschorting van certificaten

Met betrekking tot de opschorting en het melden hiervan, zijn de in punt *K.1.* beschreven methoden van toepassing.

Certificaten worden opgeschort wanneer nader onderzoek is vereist om te bepalen of een certificaat moet worden ingetrokken (bijvoorbeeld in geval van een vermoeden van verlies/diefstal van het OTP-token, of in afwachting van nadere informatie om vast te stellen dat de houder de activiteiten waarvoor het certificaat is afgegeven, heeft beëindigd, enz.).

Een verzoek tot opschorting kan worden ingediend door elk van de in de artikelen 27, 28 en 29 van het DPCM genoemde entiteiten (certificeringsinstantie, houder, belanghebbende derde).

Indien de houder niet reageert, wordt het certificaat automatisch ingetrokken na een opschortingsperiode van 90 (negentig) dagen of, in ieder geval, op de vervaldatum van het certificaat.

De datum van inwerkingtreding van de intrekking valt in ieder geval samen met de datum van inwerkingtreding van de opschorting.

K.2.1. Opschorting op verzoek van de houder

De houder kan om opschorting verzoeken door zich te wenden tot een specifieke sectie van de onlinediensten van de bank of betalingsinstelling, of door rechtstreeks contact op te nemen met de klantenservice van de bank of betalingsinstelling.

De certificeringsinstantie zal het certificaat opschorten en de houder hiervan op de hoogte stellen via de specifieke kanalen die deel uitmaken van de diensten van de bank of betalingsinstelling.

De houder kan vervolgens verzoeken om reactivering van het certificaat volgens de door de bank of betalingsinstelling vastgestelde methoden.

Bij gebrek aan verdere kennisgevingen, worden de opgeschorte certificaten automatisch ingetrokken aan het einde van de opschortingsperiode en zal de datum van intrekking samenvallen met de opschortingsdatum.

K.2.2. Opschorting op verzoek van de belanghebbende derde

In haar hoedanigheid van belanghebbende derde kan de bank of betalingsinstelling om opschorting van het certificaat verzoeken.

De certificeringsinstantie zal, na vaststelling van de geldigheid van het verzoek, het certificaat onverwijld opschorten en de betrokken houders per e-mail of via de in het kader van de dienstverlening van de bank of betalingsinstelling ter beschikking gestelde communicatiekanalen op de hoogte stellen van de opschorting.

K.2.3. Opschorting op verzoek van de certificeringsinstantie

Behoudens in gevallen van gerechtvaardigde en aangetoonde urgentie, kan de certificeringsinstantie het certificaat opschorten, waarvan zij de houder vooraf in kennis stelt via het bij de inschrijving opgegeven e-mailadres of huisadres, met opgave van de redenen voor de opschorting en de datum en het tijdstip waarop deze in werking treedt.

De certificeringsinstantie zal een soortgelijke kennisgeving aan de belanghebbende derde sturen.

L. Methode voor het vervangen van sleutels

L.1. Vervanging van gekwalificeerde certificaten en sleutels van de houder

Gekwalificeerde certificaten voor elektronische handtekeningen die door de certificeringsinstantie zijn afgegeven in de context die in deze gebruiksaanwijzing is aangegeven, zijn 36 (zesendertig) maanden geldig vanaf de datum van afgifte.

Aan het einde van die periode moet een nieuw sleutelpaar worden aangemaakt en moet een nieuw certificaat worden afgegeven.

De procedure voor het afgeven van een nieuw certificaat is in dit geval vergelijkbaar met de procedure die wordt gevolgd voor het afgeven van het eerste certificaat, met uitzondering van de procedure voor de identificatie van de houder, die niet hoeft te worden herhaald.

L.2. Vervanging van certificeringssleutels

L.2.1. Noodvervanging van certificeringssleutels

De procedure die moet worden gevolgd wanneer het ondertekeningsapparaat (HSM) met de certificeringssleutels (CA en TSCA) uitvalt, of wanneer zich een ramp voordoet in het hoofdbedieningscentrum, wordt behandeld in de sectie *P Procedure voor het beheer van rampen*.

L.2.2. Geplande vervanging van certificeringssleutels

Binnen de door de huidige regelgeving vereiste termijn en vóór het verstrijken van het certificaat dat betrekking heeft op de certificeringssleutelparen (CA en TSCA) die door de systemen worden gebruikt om ondertekencertificaten en TSA-certificaten te ondertekenen, zal de certificeringsinstantie de in artikel 30 van het DPCM bedoelde stappen uitvoeren.

L.3. Sleutels voor tijdstempelsysteem (TSA)

Overeenkomstig de bepalingen van artikel 49, lid 2, van het DPCM worden deze binnen 90 (negentig) dagen na de datum van afgifte vervangen om het aantal tijdstempels dat met hetzelfde TSA-sleutelpaar wordt gegenereerd, te beperken. Op dat moment wordt ook een certificaat voor het nieuwe sleutelpaar afgegeven, zonder dat het certificaat voor het vervangen sleutelpaar wordt ingetrokken.

M. Certificatenlijst

M.1. Procedures voor het beheer van de certificatenlijst

INTESA publiceert de volgende informatie in de certificatenlijst:

1. Certificaten van de ondertekensleutel en tijdstempels.
2. Certificaten van de certificeringssleutels (CA en TSCA).
3. Certificaten die worden uitgegeven na vervanging van certificeringssleutels.
4. Certificaten voor AgID-ondertekensleutels (DPCM, artikel 42, lid 1).
5. Lijsten van intrekkingen en opschortingen (CRL).

Transacties met betrekking tot de certificatenlijst worden uitsluitend uitgevoerd door bevoegde personen, waarvan er voldoende aanwezig zijn om het voorkomen van illegale activiteiten door een beperkt aantal personeelsleden te waarborgen.

De certificeringsinstantie houdt een moederkopie bij van de certificatenlijst die van buitenaf ontoegankelijk is: deze actualiseert de operationele kopie in real time en is toegankelijk voor gebruikers via het LDAP-protocol.

Er wordt systematisch gecontroleerd of de moederkopie overeenkomt met de operationele kopie.

M.2. Logische toegang tot de certificatenlijst

De moederkopie van de lijst bevindt zich binnen een beperkt netwerk dat is beschermd door geschikte apparatuur. Daarom heeft alleen de server die de certificaten afgeeft toegang tot de moederkopie van de lijst, teneinde de afgegeven certificaten en de CRL te registreren.

Operationele kopieën zijn toegankelijk via ***ldap://x500.e-trustcom.intesa.it*** met behulp van het LDAP-protocol.

De certificeringsinstantie biedt ook toegang tot de CRLs via het http-protocol, op de URL die in het CDP-veld (CRL Distribution Point) van het certificaat is aangegeven.

M.3. De ruimte waar zich de certificeringslijst bevindt – fysieke toegang

Personeel dat bevoegd is om de certificatenlijst rechtstreeks te beheren, heeft alleen toegang tot de gebouwen waar het systeem is geïnstalleerd en kan de relevante bewerkingen uitvoeren in de dual control-modus om illegale activiteiten te voorkomen.

De systeembeheerders, netwerkbeheerders, onderhoudstechnici, enz., kunnen de ruimte waar het systeem is geïnstalleerd alleen betreden en daar werken in aanwezigheid van medewerkers die bevoegd zijn om de certificatenlijst te beheren op de manier die eerder is beschreven voor bevoegde operatoren.

N. Procedures voor de bescherming van persoonsgegevens

De veiligheidsmaatregelen voor de bescherming van persoonsgegevens voldoen aan de eisen van Verordening (EU) nr. 679/2016 (AVG) en latere wijzigingen en aanvullingen.

O. Procedures voor het beheer van back-ups

De digitale archieven waarvan een back-up wordt gemaakt, zijn de volgende:

- CERTIFICATENLIJST, een digitaal archief dat het in punt M vermelde materiaal bevat.
- OPERATONELE INFORMATIE, een digitaal archief waarin alle informatie die van de houder is ontvangen op het moment van registratie en aanvraag van een certificaat wordt opgeslagen, evenals eventuele intrekkings- en opschortingsverzoeken, samen met de bijbehorende documentatie.
- CONTROLELOGBOEK, een archief bestaande uit de set van records die automatisch worden aangemaakt door de systemen die geïnstalleerd zijn als onderdeel van de QTSP-certificeringsdienst (artikel 36 van het DPCM).
- DIGITAAL TIJDSTEMPELARCHIEF, bevat de tijdstempels die door het tijdstempelsysteem worden aangemaakt (artikel 53, lid 1, van het DPCM).
- OPERATIONEEL REGISTER VAN TIJDSTEMPELGEBEURTENISSEN, een register waar gebeurtenissen met betrekking tot tijdstempelactiviteiten automatisch worden opgeslagen. Eventuele storingen of sabotagepogingen die de goede werking van het tijdstempelsysteem kunnen beïnvloeden, worden hier geregistreerd (artikel 52 van het DPCM).

De archivering van alle hierboven genoemde back-ups wordt uitgevoerd overeenkomstig de bepalingen van de huidige regelgeving.

P. Procedures voor het beheer van rampen

De QTSP INTESA beschikt over een rampenbeheerplan, waarin de volgende stappen zijn voorzien:

- beheer van de noodperiode: tijdens deze fase is de continuïteit van de toegang tot de CRL gegarandeerd; er kunnen zich vertragingen voordoen bij de afgifte ervan, omdat de back-upserver van de CA (die zich op de back-uplocatie bevindt) moet worden geactiveerd;
- beheer van de overgangsperiode: tijdens deze fase is de afgifte van certificaten gegarandeerd, evenals de activering van aanvullende oplossingen voor rampen;
- terugkeer naar de standaard bedrijfsmodus: op de oorspronkelijke locatie of op een alternatieve, maar permanente locatie.

Replica's van de operationele kopie van de certificatenlijst worden over verschillende locaties verdeeld, wat

betekent dat in geval van een dienstonderbreking op een van de locaties de inhoud van de certificatenlijst nog steeds toegankelijk is en up-to-date zal zijn tot het moment van de onderbreking.

Ten behoeve van het beheer van de noodsituatie wordt de replicatie van de certificatenlijst en van de gegevens van het certificatensysteem op de back-uplocatie uitgevoerd. Binnen 24 uur zal getraind personeel de functie voor afgifte van CRLs herstellen. Het bovengenoemde personeel wordt niet alleen getraind in het beheer van de SW- en HW-systemen, maar ook in het omgaan met noodsituaties.

Een papieren versie van het noodplan wordt bewaard op alle locaties die betrokken zijn bij het beheer van rampen.

Q. Procedure voor het toepassen en definiëren van tijdreferenties

Alle apparaten die in het PKI-systeem van de certificeringsinstantie zijn opgenomen, worden gesynchroniseerd met het I.N.RI.M. - *Istituto Nazionale di Ricerca Metrologica* (Nationaal Instituut voor Metrologisch Onderzoek) in Turijn, voorheen het Galileo Ferraris *Istituto Elettrotecnico Nazionale* (Nationaal Elektrotechnisch Instituut).

Deze functie wordt uitgevoerd door specifieke software die op elke server is geïnstalleerd en die via het Network Time Protocol verbinding maakt met de geconfigureerde servers op afstand.

Het Network Time Protocol (NTP) is een van de meest nauwkeurige en flexibele manieren om informatie over tijd en datum op het internet te verkrijgen. Het synchroniseert voortdurend alle computers die via lokale, metropolitane of zelfs wereldwijde netwerken (internet) met elkaar verbonden zijn, door middel van een hiërarchische piramidestructuur.

I.N.RI.M. biedt een synchronisatiedienst voor computersystemen die met het internet zijn verbonden, op basis van twee primaire NTP-servers die in het Laboratorium Tijd- en Frequentiestandaard zijn geïnstalleerd. Ze worden gesynchroniseerd via een tijd- en datumcodegenerator door cesiumbundel-atoomklokken, die ook worden gebruikt om de Italiaanse nationale tijdschaal UTC (IT) te genereren. Het tijdsinterval tussen de NTP-servers van I.N.RI.M. en de Italiaanse nationale tijdschaal wordt bewaakt en is meestal lager dan een paar milliseconden. De synchronisatieprecisie is afhankelijk van het type netwerk en de afstand tussen de NTP-server en het te synchroniseren systeem; de typische afwijkingswaarden zijn minder dan een milliseconde voor systemen die tot hetzelfde netwerk behoren en kunnen enkele honderden milliseconden bereiken voor netwerken op afstand.

De software die op de site van de certificeringsinstantie is geïnstalleerd, maakt op regelmatige tijdstippen verbinding met de server op afstand en corrigeert, na het verkrijgen van de huidige tijd, de klok op de lokale machine met behulp van verfijnde algoritmen.

De tijdreferenties die door de applicaties worden toegepast zijn strings in datumformaat (DD/MM/JJJJ uu:mm:ss) en zijn nauwkeurig tot op de dichtstbijzijnde seconde. Ze geven de lokale tijd weer in overeenstemming met de machineconfiguratie. Deze referenties voldoen aan artikel 51 van het DPCM.

Elk record in het controlelogboek bevat een tijdreferentie die is aangemaakt zoals hierboven is beschreven en bindend is voor derden (artikel 41 van het DPCM).

Q.1. Procedure voor het aanvragen en verifiëren van tijdstempels

De certificeringsinstantie brengt een tijdstempel (gekwalificeerd elektronisch tijdstempel volgens de eIDAS-verordening) aan op alle documenten die door de houder zijn ondertekend in het kader van de diensten die in deze gebruikshandleiding worden beschreven.

Het aanbrengen van deze tijdstempel is een integraal onderdeel van het ondertekeningsproces en vereist geen specifieke actie van de houder.

R. Lead time en RACI-tabel voor de afgifte van certificaten

De onderstaande tabel verwijst naar de “proces-lead times” voor het beheer van aanvragen voor de afgifte; intrekking, opschorting en heractivering van de certificaten.

Persoon	Aanvraag	Betrokken partij	Actie van betrokken partij	Betrokken partij	Actie van betrokken partij
Gebruiker, Aanvrager, Houder van certificaat	*Verzoek tot afgifte certificaat aan LRA*	*Bank/instelling (optredend als) lokale RA*	*Geeft opdracht tot publicatie van certificaat aan CA na verificatie van identiteit*	*Certificeringsinstantie*	*Verwerking certificeringsverzoek*
Gebruiker, Aanvrager, Houder van certificaat	*Verzoek tot intrekking certificaat aan RA of LRA*	*Intesa (optredend als) registratieautoriteit (RA) of bank / instelling (optredend als LRA)*	*Geeft opdracht tot intrekking van certificaat aan CA na verificatie van identiteit*	*Certificeringsinstantie*	*Verwerking intrekkingsverzoek*
Gebruiker, Aanvrager, Houder van certificaat	*Verzoek tot opschorting certificaat aan RA of LRA*	*Intesa (optredend als) registratieautoriteit (RA) of bank / instelling (optredend als LRA)*	*Geeft opdracht tot opschorting van certificaat aan CA na verificatie van identiteit*	*Certificeringsinstantie*	*Verwerking opschortingsverzoek*
Gebruiker, Aanvrager, Houder van certificaat	*Verzoek tot heractivering certificaat aan RA of LRA*	*Intesa (optredend als) registratieautoriteit (RA) of bank / instelling (optredend als LRA)*	*Geeft opdracht tot heractivering van certificaat aan CA na verificatie van identiteit*	*Certificeringsinstantie*	*Verwerking heractiveringsverzoek*

De onderstaande RACI-tabel geeft de verantwoordelijkheden weer van de partijen die betrokken zijn bij het beheer van de verzoeken tot afgifte, intrekking, opschorting en heractivering van certificaten.

Betrokken persoon	Verantwoordelijk	Eindverantwoordelijk	Geraadpleegd	Geïnformeerd
Registratieautoriteit	***X***			
Lokale registratieautoriteit	***X***			
Certificeringsinstantie		***X***		
Gebruiker van certificaat, Aanvrager, Houder			***X***	***X***

S. Technisch referentiemateriaal

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	Recommendation ITU-R TF.460-6, Annex 1 – Time Scales.
RFC5905	Network Time Protocol (NTP 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	Recommendation ITU-R TF.460-6, Annex 1 – Time Scales.
RFC5905	Network Time Protocol (NTP Protocol)

------- EINDE DOCUMENT -------