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

Prestataire de services de confiance qualifié

Manuel opérationnel portant sur les procédures de signature électronique qualifiée à distance dans les secteurs bancaire et financier

Code du document : MO_REMBAN

OID : 1.3.76.21.1.50.110

Rédigé par : Antonio Raia

Approuvé par : Franco Tafini

Date d'émission : 01/07/2019

Version : 04

Signé par Antonio Raia
IN.TE.S.A. S.p.A.

VERSIONS

Version nº : 04		***Date de révision :***	***01/07/2019***
Description des modifications :	Changement du logo et des informations concernant l'entreprise Mise à jour des définitions et des règlementations applicables Mise à jour de la disposition graphique Inclusion of signing procedure for Prospect (I.2.3)		
Motifs :	Refonte des règlements : Règlement (EU) 910/2014 (eIDAS), Décret législatif italien 179/2016 (RGPD) Modifications organisationnelles du TSP Procédure pour l'acquisition de nouveaux clients		
Version nº : 03		***Date de révision :***	***13/06/2012***
Description des modifications :	Extension du manuel aux secteurs financier (Instituts de paiement) et banquier		
Motifs :	Mise à jour		
Version nº : 02		***Date de révision :***	***02/04/2012***
Description des modifications :	B.4.2. - Introduction du système de reconnaissance de l'identité du titulaire (vérification adéquate) ne requérant pas sa présence physique. C.5. - Introduction des méthodes du système de reconnaissance de l'identité du titulaire (vérification adéquate). F.1.3. – Insertion de la limite d'utilisation habituelle. G. – Insertion des modes de communication électronique des confirmations opérationnelles		
Motifs :	Mise à jour		
Version nº : 01		***Date de révision :***	***01/11/2011***
Description des modifications :	aucune		
Motifs :	première version		

Sommaire

Références règlementaires

Texte Unique – Décret du président de la République 445/00 et ses modifications ultérieures	Décret du président de la République italienne nº 445 du 28 Décembre 2000. *« Texte unique des dispositions législatives et règlementaires en matière de documentation administrative »*. *Appelé ci-après plus simplement TU [Texte Unique]*.
Code de l'Administration numérique – Décret législatif italien nº 82/05 et ses modifications et ajouts ultérieurs	Décret législatif italien nº 82 du 7 mars 2005. « *Codice dell'amministrazione Digitale* » *(Code de l'Administration Numérique). Appelé ci-après plus simplement* CAD.
Décret du premier ministre italien 22/02/2013 *Nouvelles règles techniques* et ses modifications et ajouts ultérieurs	Décret du président du Conseil des ministres italien du 22 février 2013. *« Règles techniques en matière de génération, application et vérification des signatures électroniques avancées, qualifiées et numériques, en vertu des articles 20, paragr. 3, 24 paragr. 4, 28 paragr. 3, 32 par. 3 point b), 35 paragr. 2, 36 paragr. 2, et 71 » (du CAD, ed.).* Ci-après appelé également *DPCM [Décret du Président du Conseil des Ministres]*.
Règlement (EU) nº 910/2014 (eIDAS) et ses modifications et ajouts ultérieurs	Règlement (EU) nº 910/2014 du Parlement européen et du Conseil du 23 juillet 2014, sur l'identification électronique et les services de confiance pour les transactions électroniques au sein du marché intérieur et abrogeant la directive 1999/93/CE. Appelé ci-après simplement Règ. eIDAS.
RGPD Règlement général sur la protection des données et ses modifications et ajouts ultérieurs	Règlement (EU) 2016/679 du Parlement européen et du Conseil du 27 avril 2016 relatif à la protection des personnes physiques à l'égard du traitement des données à caractère personnel et à la libre circulation de ces données, et abrogeant la directive 95/46/CE (règlement général sur la protection des données). Appelé ci-après plus simplement RGPD.
RÉSOLUTION Nº 147/2019 et ses modifications et ajouts ultérieurs	Lignes directrices portant « Règles techniques et recommandations liées à la génération des certificats électroniques qualifiés, signatures et cachets électroniques qualifiés et horodatages électroniques qualifiés. » Appelé ci-après plus simplement RÉSOLUTION.

Définitions et Acronymes

AgID	*Agenzia per l'Italia Digitale* (Agence pour l'Italie Numérique, anciennement CNIPA et DigitPA) - www.agid.gov.it. Organisme de surveillance en vertu du règlement EU 910/2014 (eIDAS). Appelé ci-après simplement l'Agence.
QTSP Qualified Trust Service Provider (Prestataire de services de confiance qualifié). Accredited Certification Authority (Autorité de certification accréditée)	*Prestataire de services de confiance qualifié*. Personne physique ou morale qui fournit un ou plusieurs services de confiance qualifiés. Anciennement *Autorité de certification accréditée*, conformément au CAD. Dans le cadre du présent document, il s'agit du QTSP In.Te.S.A. S.p.A.
Service de confiance qualifié	Service électronique fourni par un prestataire comprenant les éléments visés à l'art. 3, point 16) et point 17) du règlement EU 910/2014 (eIDAS). Dans le cadre de ce document, il s'agit du prestataire In.Te.S.A. S.p.A. mettant à disposition les services qualifiés de signature électronique, de validation temporaire électronique et tout autre service lié.

Certificat qualifié de signature électronique	Attestation électronique associant les données de validation d'une signature électronique à une personne physique et confirmant au minimum le nom ou le pseudonyme de cette personne. Elle est délivrée par un prestataire de services de confiance qualifié et remplit les exigences visées à l'annexe I du Règlement (EU) 910/2014 (eIDAS).
Clé privée	L'élément de la paire de clés asymétriques, utilisé par le titulaire, à l'aide duquel la signature numérique est apposée sur les documents informatiques.
Clé publique	L'élément de la paire de clés asymétriques destiné à être rendu public permettant la vérification de la signature numérique du document informatique.
CRL	*Certificate Révocation List*, liste des certificats révoqués, où figurent les certificats révoqués ou suspendus, que l'autorité de certification, à l'origine de leur délivrance, ne considère plus comme valides.
OCSP	*Online Certificate Status Protocol* (Protocole de vérification de certificat en ligne) : service de vérification du statut de validité du certificat, selon le protocole OCSP.
Document informatique	Le document électronique où figure la représentation des actes, faits ou données ayant une pertinence juridique
QES -Signature électronique qualifiée *DS - Signature Numérique*	Signature électronique créée par un dispositif de création de signature électronique qualifiée reposant sur un certificat qualifié pour les signatures électroniques. Elle coïncide, en Italie, avec la *Signature numérique [Digital Signature]* définie à l'art.1, paragr. 1, point s) du CAD : une signature électronique qualifiée reposant sur un système de clés cryptographiques, l'une publique et l'autre privée, reliées l'une à l'autre – permettant au titulaire via la clé privée et au destinataire, à l'aide de la clé publique, de prouver et de vérifier l'origine et l'intégrité d'un document informatique ou d'un ensemble de documents informatiques.
Signature à distance	Une procédure spéciale de signature électronique qualifiée ou de signature numérique, générée sur HSM encadrée et gérée sous la responsabilité de l'autorité de certification accréditée, qui permet de garantir le contrôle exclusif des clés privées de la part de leurs titulaires.
HSM - Hardware Security Module	Dispositifs pour la création de la signature électronique qualifiée, lorsqu'ils remplissent les conditions visées à l'annexe II du Reg. (EU) 910/2014. Appelés également *Dispositifs de Signature*.
Qualified Electronic Time Stamp (horodatage)	*Horodatage électronique qualifié* Données au format électronique qui associent d'autres données au format électronique à une date et heure données, afin de prouver que ces dernières existaient à ce moment précis. Elles remplissent les exigences de l'art. 42 du règlement eIDAS.
CA – Certification Authority (Autorité de certification)	Autorité qui délivre les certificats pour la signature électronique.
RA – Registration Authority (Autorité d'enregistrement)	*Autorité en charge de l'enregistrement* : entité, nommée par le QTSP, en charge de l'enregistrement et de la vérification des informations (notamment de l'identité du titulaire) requises par le QTSP afin de délivrer le certificat qualifié.
Registre des certificats	L'ensemble d'un ou de plusieurs fichiers informatiques, conservé par l'autorité de certification, contenant tous les certificats délivrés.
Demandeur	La personne physique qui demande le certificat.
Titulaire	La personne physique pour laquelle le certificat qualifié est délivré, autorisée à l'utiliser afin d'apposer sa signature numérique.
Client *Prospect*	Le client (ou client potentiel appelé *Prospect*) de la banque ou de l'institut financier.
Référence temporelle	Information contenant la date et l'heure, associée à un ou plusieurs documents informatiques.

TSA - Time Stamping Authority (autorité en charge de l'horodatage)	Autorité délivrant les horodatages électroniques.

A.Introduction

Le présent document constitue le *Manuel opérationnel portant sur les procédures de signature électronique qualifiée à distance dans les secteurs bancaire et financier* (ci-après, le *Manuel opérationnel* ou simplement *MO*) préparé par le QTSP In.Te.S.A. S.p.A.

Le contenu du présent manuel respecte les prescriptions des règles techniques figurant dans le *Décret du président du Conseil des ministres du 22 février 2013* (ci-après *DPCM*) et le *Décret législatif italien n° 82 du 07 mars 2005,* comprenant le *« Codice di Amministrazione Digitale » (*Code d'administration numérique) ci-après « *CAD* » et ses modifications et ajouts ultérieurs et est conforme au *Règlement (EU) 910/2014* (ci-après, Règ. *eIDAS*).

Pour toutes les matières non traitées explicitement dans ce manuel *opérationnel*, on se réfèrera aux règlements en vigueur et ultérieurs régissant les cas concrets.

Ce document décrit les règles et les procédures opérationnelles du prestataire de services de confiance qualifié *In.Te.S.A. S.p.A.* (ci-après, *QTSP INTESA, Autorité de certification* ou simplement *INTESA*) pour la délivrance des certificats qualifiés, la génération et la vérification de la signature électronique qualifiée et les procédures liées au service de validation temporelle, conformément à la règlementation en vigueur, lorsque cette dernière est gérée dans le cadre de projets bancaires ou financiers.

Pour ce type de projets, les entités bancaires ou financières, délivrant des services de banque à domicile et d'applications au guichet, feront également office d'autorités d'enregistrement locales (ci-après *Local Registration Authority*, LRA) pour le compte du QTSP INTESA. Ces entités bancaires ou financières seront ensuite appelées *Banque ou Institut de paiement* (ou simplement *Banque ou Institut*).

À cet égard, seules les personnes identifiées par ladite banque ou l'institut qui, en vertu d'un accord spécial avec le QTSP INTESA, est autorisé à agir en tant qu'autorité d'enregistrement, pourront être titulaires d'un certificat qualifié.

On souligne ainsi que l'ensemble des processus de signature de documents faisant l'objet du présent manuel opérationnel sera mis en œuvre exclusivement dans le cadre des applications bancaires ou financières.

Les activités décrites dans le présent manuel opérationnel sont réalisées dans le respect du règlement EU 910/2014 (eIDAS).

A.1. Propriété intellectuelle

Le présent manuel opérationnel relève de la propriété exclusive de In.Te.S.A. S.p.A., qui en détient tous les droits intellectuels.

Les informations décrites dans ce document concernant la réalisation des activités du QTSP sont couvertes par les droits en matière de propriété intellectuelle.

A.2. Validité

Le contenu de ce document s'applique au QTSP INTESA (à savoir à ses infrastructures logistiques et techniques et à son personnel), aux titulaires des certificats délivrés par ce dernier et à tous ceux qui utilisent ces certificats afin de vérifier l'authenticité et l'intégrité des documents sur lesquels une signature électronique qualifiée est apposée, y compris par le biais d'horodatages qualifiés délivrés par le QTSP INTESA, et à la banque ou à l'institut de paiement en tant qu'autorité d'enregistrement locale.

L'art. 5, paragraphe 4 du DPCM régit l'utilisation des clés et des certificats correspondants, et prévoit la répartition des clés de signature et de vérification ainsi que des services correspondants selon les catégories suivantes :

a) Clés de signature utilisées pour générer et vérifier les signatures apposées ou associées aux documents ;
b) Clés CA, utilisées pour générer et vérifier les signatures apposées sur les certificats qualifiés, fournir des informations concernant l'état de validité du certificat ou signer des certificats liés aux clés d'horodatage électronique ;
c) Clés d'horodatage, utilisées pour générer et vérifier les horodatages.

B. Informations générales

Ce document a pour objectif de définir, dans les grandes lignes, les procédures et les règles régissant la délivrance des certificats qualifiés par le QTSP INTESA.

Les règles et les procédures mentionnées ci-dessus reposent sur le respect des règlementations applicables en vigueur, qui permet à INTESA de figurer parmi les autorités de certification habilitées.

Ainsi, conformément aux règlementations mentionnées ci-dessus, de nombreuses entités, seront impliquées dans le processus, comme indiqué plus en détails dans ce document.

B.1. Données d'identification de la version du manuel opérationnel

Le présent document représente la version *04* du *Manuel opérationnel portant sur les procédures de signature électronique qualifiée à distance dans le domaine bancaire et financier,* délivré conformément à l'art. 40 du DPCM.

L'identificateur d'objet de ce document est **1.3.76.21.1.50.110**.

Le présent manuel est public et disponible à la consultation électronique :

- À l'adresse internet du prestataire, *https://www.intesa.it/e-trustcom/*
- À l'adresse internet de l'AgID, *www.agid.gov.it*
- Sur le site officiel de la banque ou de l'institut.

Remarque : la publication de versions actualisées du présent manuel opérationnel ne pourra avoir lieu sans l'autorisation de l'AgID [Agence pour l'Italie Numérique].

B.2. Données d'identification du Prestataire de services de confiance qualifié

La société ***In.Te.S.A. S.p.A.*** constitue le QTSP (*Qualified Trust Service Provider*, Prestataire de services de confiance qualifié). Les informations permettant son identification sont reportées ci-dessous.

Nom de la société	**In.Te.S.A. S.p.A.**
Adresse du siège légal	**Strada Pianezza, 289 10151 Turin**
Représentant légal	**Administrateur délégué**
Registre du commerce de Turin	**N° d'inscription 1692/87**
N° de TVA	**05262890014**
N° de téléphone (standard)	**+39.011.19216.111**
Site internet	**www.intesa.it**
Adresse électronique	**marketing@intesa.it**
Adresse (URL) du registre des certificats	**ldap://x500.e-trustcom.intesa.it**
Identificateur d'objet ISO (OID)	**1.3.76.21.1**

Le personnel en charge des activités de certification est réparti comme suit, conformément à l'art. 38 du DPCM :

a) Responsable de la sécurité.

b) Responsable du service de certification et d'horodatage.
c) Responsable du fonctionnement technique des services.
d) Responsable des services technique et logistique.
e) Responsable des inspections et audits.

Les figures professionnelles mentionnées ci-dessus appartiennent toutes à l'organisation du QTSP INTESA.

B.3. Responsabilité du manuel opérationnel

Conformément à l'art. 40, paragr. 3 point c) du DPCM, l'autorité de certification INTESA est responsable de ce manuel opérationnel et veille à sa préparation et à sa publication.

Afin de recueillir les éventuelles observations et demandes d'éclaircissements, INTESA met à disposition les moyens de communication suivants :

une adresse électronique : e-trustcom@intesa.it *marketing@intesa.it*

un numéro de téléphone : +39 011.192.16.111

un service d'assistance pour les appels depuis l'Italie : 800.80.50.93

pour les appels depuis l'étranger : +39 02.871.193.396

B.4. Entités impliquées dans les processus

Au sein de la structure du QTSP, plusieurs entités prenant part aux processus liés à la délivrance des certificats ont été identifiées.

Ces entités exercent dans le respect des règles et des procédures mises en œuvre par le QTSP et s'acquittent des tâches relevant de leur compétence.

B.4.1. Autorité de Certification (CA)

Conformément aux dispositions du DPCM, du CAD et du règlement eIDAS, INTESA exerce l'activité de prestataire de services de confiance qualifié. Cette activité recouvre les services de confiance qualifiés comprenant la création, la vérification et la validation de signatures électroniques, cachets électroniques ou validations temporaires électroniques (horodatage).

Les données d'identification concernant le QTSP INTESA sont fournies au paragraphe *B.2* précédent.

B.4.2. Autorité Locale d'Enregistrement (LRA)

Pour la mise en œuvre du type de service particulier proposé (signature électronique qualifiée à distance pour des applications bancaires et financières) décrit dans ce manuel opérationnel, le QTSP INTESA délègue les fonctions d'autorité d'enregistrement à la banque ou à l'institut qui aura acquis le service.

La LRA s'engage à réaliser les activités suivantes :

- Identification du titulaire ;
- Enregistrement du titulaire.

Durant l'exercice de ses fonctions d'Autorité en charge de l'enregistrement, la banque ou l'institut veillera à ce que l'activité de reconnaissance se déroule dans le respect de la règlementation en vigueur et des dispositions du présent manuel opérationnel.

En particulier, conformément à la norme en matière de lutte contre le recyclage, la banque ou l'institut pourra identifier le titulaire (vérification adéquate), y compris lorsque ce dernier ne se présente pas physiquement à l'agence.

Dans ce cas, la banque ou l'institut doit :

- S'assurer de l'identité à l'aide de documents, données ou informations complémentaires tels que les actes authentiques, actes sous seing privés authentifiés, certificats utilisés pour générer une signature électronique qualifiée associée à des documents informatiques ou bien à l'aide d'une déclaration du

consulat italien ;

- Appliquer des mesures complémentaires de vérification des documents présentés, telles qu'une attestation de confirmation d'un institut de crédit ou financier soumis à la directive ;
- Utiliser les documents prouvant que la délégation vient d'un compte au nom du client.

C. Obligations

C.1. Obligations du prestataire de services de confiance qualifié (QTSP)

Lors de l'exercice de son activité, le prestataire de services de confiance qualifié (ci-après *Autorité de certification accréditée*) respecte les dispositions du :

- Décret législatif n° 82 du 7 mars 2005 et ses modifications ultérieures.
- Décret du président du conseil des ministres du 22 février 2013.
- Règlement (EU) 2016/679 (RGPD)
- Règlement (EU) 910/2014 (eIDAS)

En particulier, le QTSP :

- Adopte toutes les mesures organisationnelles et techniques nécessaires afin d'éviter tout dommage à autrui ;
- Se conforme aux règles techniques indiquées dans le DPCM et ses modifications et ajouts ultérieurs ;
- Garantit la conformité de son système de qualité aux normes ISO 9001 ;
- Assure que le dispositif pour la génération des signatures (HSM) remplit les conditions de sécurité prévues par l'art. 29 du règlement eIDAS ;
- Délivre et publie le certificat qualifié, sauf indication contraire du titulaire, conformément à l'art.32 du CAD ;
- Fournit aux demandeurs, de façon claire et explicite, des informations sur la procédure de certification, les exigences techniques nécessaires pour y accéder, les caractéristiques et limites d'utilisation des signatures délivrées avec le service de certification ;
- Se conforme aux mesures de sécurité en matière de traitement des données à caractère personnel (RGPD) ;
- Ne constitue pas un dépôt des données pour la création de la signature du titulaire ;
- Publie la révocation ou la suspension du certificat électronique en cas de demande de la part du titulaire ou du tiers concerné ;
- Détermine avec précision la date et l'heure de délivrance, de révocation et de suspension des certificats électroniques ;
- Conserve un enregistrement, y compris électronique, de toutes les informations concernant le certificat qualifié sur une durée de 20 (vingt) ans, afin notamment de fournir la preuve de la certification dans l'éventualité de procédures judiciaires ;
- Assure que le code d'identification (de propriété exclusive du QTSP) attribué à chaque titulaire est univoque parmi ses utilisateurs ;
- Fournit, sur des moyens de communication durables, toutes les informations utiles aux personnes requérant le service de certification. Ces informations comprennent : les termes et conditions précises d'utilisation du certificat, incluant toute limitation d'utilisation, l'existence d'un système d'accréditation facultatif et les procédures de réclamation et de résolution des litiges. Ces informations, pouvant être transmises par voie électronique, doivent être rédigées dans un langage clair et compréhensible avant l'accord entre la personne demandant le service et le QTSP ;
- Utilise des systèmes fiables pour la gestion du registre des certificats de façon à garantir que seules les personnes autorisées peuvent saisir et modifier les données, que l'authenticité des informations peut être vérifiée, que le public ne peut consulter les certificats que dans les cas autorisés par le titulaire du certificat et que l'opérateur peut percevoir tout événement compromettant les exigences de sécurité ;

- Enregistre les certificats qualifiés délivrés dans le journal d'audit en indiquant la date et l'heure de délivrance.

Dans le respect de l'art. 14 du DPCM, l'autorité de Certification fournit ou indique au moins un système permettant de vérifier les signatures numériques.

En outre, le QTSP :

- génère un certificat qualifié pour chacune des clés d'une signature électronique avancée utilisées par l'AgID pour signer la liste publique des autorités de certification, et le publie dans son registre des certificats en vertu de l'art. 42 du DPCM ;
- indique un système de vérification de la signature électronique, visé par l'art. 10 du DPCM ;
- garde une copie de la liste, signée par l'AGID, des certificats associés aux clés de certification visées à l'art. 43 du DPCM, et la met à disposition du public par voie télématique comme prévu par l'art. 42, paragr. 3, du DPCM.

C.2. Obligations du titulaire

Le titulaire demandant un certificat qualifié pour les services décrits dans le présent manuel opérationnel est un client de la banque ou de l'institut de paiement, qui fait office d'autorité d'enregistrement.

Le titulaire recevra un certificat qualifié pour la signature électronique qualifiée à distance, qui lui permettra d'apposer sa signature pour conclure des contrats ou souscrire des documents liés aux produits et/ou aux services offerts par la banque ou l'institut selon les modalités décrites au paragr.

Le titulaire est tenu de conserver les informations nécessaires pour l'utilisation de sa clé privée de signature de façon adéquate et d'adopter toutes les mesures organisationnelles et techniques appropriées afin d'éviter tout dommage à autrui (CAD, art. 32, paragr. 1).

Le titulaire de la clé doit en outre :

- fournir toutes les informations requises par le QTSP, et garantir leur exactitude sous sa responsabilité ;
- envoyer la demande de certification selon les modalités indiquées dans ce manuel opérationnel;
- informer le QTSP, y compris par l'intermédiaire de la LRA, de toute variation des informations fournies au moment de l'enregistrement : données personnelles, résidence, contacts téléphoniques, adresse électronique, etc. ;
- conserver avec le plus grand soin les informations concernant l'habilitation à l'utilisation de la clé privée ;
- en cas de perte ou de vol des codes et/ou des dispositifs indiqués pour accéder aux clés personnelles de signature, informer immédiatement les autorités compétentes ainsi que la banque ou l'institut qui veillera à la révocation immédiate du certificat ;
- envoyer les demandes éventuelles de révocation ou de suspension du certificat qualifié conformément aux indications du présent manuel opérationnel.

C.3. Obligations des utilisateurs des certificats

L'utilisateur (*Relying Party*) est la personne qui reçoit un document portant une signature numérique et qui, afin d'en vérifier la validité, utilise le certificat qualifié utilisé par le titulaire pour signer ledit document.

La vérification de la signature numérique puis l'extraction des objets signés peut être réalisée avec n'importe quel logiciel capable d'élaborer des fichiers signés conformément au règlement eIDAS.

Les personnes qui utilisent un certificat qualifié pour vérifier la validité d'un document portant une signature numérique doivent :

- vérifier la validité d'un certificat contenant la clé publique du titulaire signataire du message, selon les indications des normes en vigueur au moment de sa délivrance ;
- vérifier le statut de validité du certificat à l'aide du protocole OCSP ou en consultant les listes de révocation ;

- vérifier la validité du parcours de certification, reposant sur la liste publique des QTSP ;
- vérifier l'existence d'éventuelles limites d'utilisation du certificat utilisé par le titulaire.

C.4. Obligations de la tierce partie concernée

Dans le cadre des services décrits par le présent manuel, la banque ou l'institut de paiement représente la tierce partie concernée et met en œuvre les activités suivantes :

- elle vérifie que le client remplit toutes les conditions nécessaires et l'autorise à demander la délivrance du certificat qualifié pour la signature numérique à distance.
- elle assiste le titulaire
- elle indique au QTSP les éventuelles limites d'utilisation ultérieures du certificat qualifié pour la signature numérique en plus de celles prévues au paragr. *F.1.1*.

La banque ou l'institut, en sa qualité de tierce partie concernée, pourra indiquer au QTSP les éventuelles limites d'utilisation du certificat, les pouvoirs de représentation potentiels et communiquer toute variation les concernant.
Celles-ci peuvent concerner, à titre d'exemple :

- la variation ou la cessation des pouvoirs de représentation ;
- la variation de rôles et de qualifications internes ;
- la cessation du rapport d'embauche.

La demande de révocation ou de suspension de la part de la tierce partie concernée envoyée à la LRA devra être immédiatement envoyée à la CA lorsque le titulaire cesse de remplir les conditions à l'origine de la délivrance du certificat qualifié pour la signature électronique.

C.5. Obligations des autorités d'enregistrement externes (LRA)

Pour des raisons liées à la fourniture du service, le QTSP INTESA a recours à d'autres entités présentes sur l'ensemble du territoire national (appelées ci-après RA externes ou LRA – *Local Registration Authorities*, autorités d'enregistrement locales) pour mettre en œuvre une partie des activités du bureau d'enregistrement.

Le QTSP In.Te.S.A. S.p.A. délègue l'exercice de la fonction d'autorité d'enregistrement à la banque ou à l'institut de paiement via un *Contrat de mandat* spécifique, signé par les deux parties.

En particulier, les RA externes mettent en œuvre les activités suivantes :

- identification sûre de la personne demandant la certification (ci-après le titulaire du certificat) ;
- enregistrement du demandeur ou du titulaire ;
- remise au titulaire des dispositifs et/ou des codes lui permettant d'accéder à sa clé de signature, dans le respect des articles 8 et 10 paragr. 2 du DPCM ;
- envoi de la documentation signée au département RA du QTSP INTESA, sous réserve d'accords ultérieurs figurant dans le contrat de mandat.

Le contrat de mandat établit explicitement les obligations prévues pour la banque ou l'institut nommé en tant que LRA par le QTSP INTESA, dont le respect est surveillé par ce dernier.

En particulier, il est demandé aux LRA de :

- veiller à ce que les activités d'identification se déroulent dans le respect des règlementations en vigueur (le CAD et ses modifications et ajouts ultérieurs, le DPCM, le règlement eIDAS et les règlementations en matière d'anti-recyclage) ;
- utiliser et traiter les données à caractère personnel obtenues au moment de la reconnaissance conformément au RGPD ;
- mettre à disposition du QTSP INTESA le matériel collecté durant la phase d'identification et d'enregistrement.

Le service d'identification (*due diligence*) pourra être géré de trois manières différentes, décrites ci-après :

- *habituelle* : le demandeur est identifié auprès d'une filiale de la banque ou de l'institut de paiement ;
- *sur demande* : à l'ouverture d'un nouveau compte courant, le requérant pourra demander à être contacté par un conseiller financier personnel qui, après avoir convenu d'un rendez-vous, assistera le client durant toutes les procédures concernant l'ouverture d'un compte courant. Au cours de cette phase, le client sera guidé (après avoir été identifié et enregistré), y compris pour la demande d'un certificat de signature électronique qualifiée ;
- *en ligne* : si le demandeur opte pour la modalité d'adhésion directe et possède déjà un compte courant dans une banque présente sur le territoire national, il pourra, pour être identifié aux termes de la loi, utiliser les méthodes suivantes :
  - utiliser une procédure SEPA (ou SDD – prélèvement SEPA);
  - disposer un virement depuis le compte courant ouvert dans la banque précitée.

Grâce aux procédures mentionnées ci-dessus, la LRA de la banque ou de l'institut de paiement recevra toutes les informations prévues par la loi, en toute sécurité et dans le respect le plus strict de la confidentialité.

D. Responsabilité et restrictions aux indemnisations

D.1. Responsabilité du QTSP – Restrictions aux indemnisations

Le QTSP INTESA est responsable vis-à-vis des titulaires de la conformité à toutes les obligations dérivant de l'accomplissement des activités prévues par le DPCM, le RGPD, le CAD et le règlement eIDAS (et ses modifications et ajouts ultérieurs) comme décrit au paragr. *C.1.Obligations du prestataire de services de confiance qualifié (QTSP)*.

Sous réserve des cas de conduite malveillante ou de négligence (Art. 13, règlement eIDAS), INTESA n'est pas responsable des conséquences dérivant d'une utilisation des certificats autre que celle prévue par l'art. 5 du DPCM, et notamment pour le non-respect des indications du présent manuel opérationnel et/ou de la règlementation en vigueur de la part du titulaire et de la tierce partie concernée.

De même, INTESA ne sera pas retenue responsable des conséquences dérivant de circonstances non attribuables à cette dernière, telles que, de manière non exhaustive : les calamités naturelles, les mauvais services ou fonctionnements techniques et logistiques indépendants de son contrôle, les interventions des autorités, les révoltes ou actes de guerre affectant également ou uniquement les entités dont INTESA se sert pour la prestation de ses services de certification.

Le QTSP INTESA ne sera pas retenu responsable des dommages dérivant d'une utilisation non conforme du certificat qualifié pour la signature numérique à distance, en relation avec la restriction de son utilisation comme spécifié au paragr. *F.1.1*.

Après avoir consulté le présent manuel opérationnel, le titulaire doit mettre en œuvre toutes les mesures de prudence nécessaires afin d'éviter les dommages à autrui liés à une mauvaise utilisation du matériel fourni par l'autorité de certification accréditée. En particulier, les dispositifs OTP et les codes secrets requis pour accéder aux clés de signature doivent être conservés avec le plus grand soin.

D.2. Assurance

Le QTSP INTESA bénéficie de contrats d'assurance pour la couverture des risques liés à l'activité et des dommages provoqués à des tiers, dont le contenu est conforme aux exigences nécessaires pour l'exercice de l'activité professionnelle en question.

L'AgID a reçu une déclaration spécifique concernant l'existence dudit contrat.

E. Tarifs

La banque ou l'institut bancaire fournit le service à ses clients. Les frais pour la délivrance, le renouvellement, la révocation et la suspension du certificat qualifié seront indiqués dans les contrats stipulés entre le client et la

banque ou l'institut.

F. Méthodes d'identification et enregistrement des utilisateurs

F.1. Identification des utilisateurs

Le QTSP doit vérifier avec certitude l'identité du demandeur lors de sa première demande de délivrance du certificat qualifié.

Cette opération est confiée à la banque ou à l'institut qui, en sa qualité de LRA et conformément aux dispositions de la règlementation en vigueur en matière d'anti-recyclage, identifiera et enregistrera le titulaire.

En ce qui concerne les renouvellements ultérieurs, s'ils ont lieu lorsque le certificat qualifié est encore valide, cette activité ne devra pas être répétée : le titulaire veillera à communiquer au QTSP par l'intermédiaire de la banque ou de l'institut les changements éventuels concernant ses données d'enregistrement.

Les données d'enregistrement requises pour la mise en place du service faisant l'objet du présent document comprennent :

- Prénom et nom ;
- Date de naissance ;
- Ville ou pays étranger de naissance ;
- Code fiscal (ou équivalent) ;
- Adresse de résidence ;
- Domicile où seront envoyées les communications papier ;
- Numéro de téléphone mobile ;
- Adresse électronique ;
- Type et numéro du document d'identité présenté ;
- Autorité ayant délivré le document et date et lieu de délivrance et d'expiration.

Au terme de cette étape d'enregistrement, le titulaire pourra recevoir un dispositif de mot de passe à usage unique prêt à l'emploi ; ce dispositif est doté d'un écran et peut générer des codes numériques à usage unique (appelés ci-après codes OTP ou simplement OTP).

En guise d'alternative au jeton OTP physique, la banque ou l'institut de paiement pourra indiquer aux titulaires comment activer un système d'authentification de logiciels pour dispositifs mobiles (si le titulaire en possède un et juge cette modalité plus pratique par rapport à l'utilisation d'un jeton d'authentification physique). Ce système logiciel permettra de générer un mot de passe à usage unique sur le dispositif mobile du titulaire et pourra ainsi être utilisé comme outil d'authentification des systèmes de signature à distance.

En plus de l'OTP, le titulaire recevra toutes les informations nécessaires ainsi qu'un numéro d'identification personnel (*Personal Identification Number*, PIN) afin de garantir un accès sécurisé au service de signature à distance que la banque ou l'institut bancaire mettra à sa disposition.

Ledit code PIN pourra être utilisé en tant que code d'urgence (en cas par exemple d'égarement ou de perte du jeton OTP ou du mobile) afin de pouvoir suspendre immédiatement le certificat qualifié à son nom (paragr. *H.2.2*).

Le titulaire pourra ensuite modifier ou mettre à jour le code PIN en utilisant les services fournis par la banque ou l'institut.

Durant cette phase, le titulaire recevra également les informations nécessaires lui permettant de changer à tout moment le numéro de portable fourni précédemment.

En outre le titulaire devra, directement au guichet de la banque ou de l'institut, ou bien dans un deuxième temps, en se connectant au service de la banque en ligne mis à disposition par la banque ou l'institut, mais en tous cas avant la demande de délivrance d'un certificat qualifié :

- consulter le manuel opérationnel du QTSP INTESA ;

- autoriser la banque ou l'institut de paiement au traitement de ses données à caractère personnel pour les fins liées à la délivrance d'un certificat qualifié pour la signature électronique.

La documentation indiquée ci-dessus, concernant l'enregistrement des titulaires doit être conservée pendant 20 (vingt) ans à compter de l'expiration du certificat.

F.1.1. Limites d'utilisation

Le certificat qualifié pour les signatures électroniques, délivré dans le cadre des services décrits dans le présent manuel et offerts par la banque ou l'institut est toujours soumis à des limites d'utilisation.

La formule habituelle est la suivante :

L'utilisation du certificat est limitée aux relations avec Nom de la banque ou de l'institut.

This certificate may only be used in dealings with Bank / Institution Name.

Des limites d'utilisation particulières pourront être convenues avec la banque ou l'institut de paiement.
INTESA n'est pas responsable des dommages dérivant de l'utilisation d'un certificat qualifié en cas de non-respect des limites imposées pour son utilisation.

F.1.2. Titres et qualifications professionnelles

S'il est demandé de mentionner des qualifications professionnelles dans le certificat qualifié (comme l'appartenance à un ordre professionnel), le demandeur doit présenter une documentation adéquate afin de démontrer la possession de ladite qualification, ou toute documentation équivalente.

Une copie de cette documentation doit être conservée pendant 20 (vingt) ans à compter de la date d'expiration du certificat.

La documentation appuyant la demande d'insertion de titres ou de qualifications professionnelles dans le certificat qualifié ne pourra être antérieure à 10 (dix) jours avant la date de présentation de la demande de délivrance dudit certificat.

INTESA n'est pas responsable des dommages dérivant d'une mauvaise utilisation d'un certificat qualifié contenant des informations liées aux qualifications professionnelles.

En cas d'auto-certification, INTESA ne prend aucune responsabilité, sous réserve des cas de malveillance ou négligence (eIDAS Reg., Art. 13), pour la saisie éventuelle dans le certificat d'informations auto-certifiées par le titulaire.

F.1.3. Pouvoirs de représentation

Lorsque les pouvoirs de représentation (tel que l'appartenance du titulaire à une organisation et la fonction qu'il occupe, l'autorisation à exercer au nom et pour le compte d'un client, etc.) doivent figurer dans le certificat qualifié, le demandeur doit présenter une documentation adéquate prouvant l'existence desdits pouvoirs de représentation.

Pour la représentation de personnes physiques, le demandeur devra fournir une copie certifiée conforme du mandat ou une procuration notariée signée par la personne représentée, accompagnée de l'attestation d'autorisation de cette dernière autorisant l'inclusion de son rôle dans le certificat.

Si le certificat doit reporter l'indication d'un rôle lié à la représentation d'organisations ou d'entités de droit privé, le titulaire devra présenter un document prouvant le rôle qu'il souhaite inclure dans le certificat, accompagné d'une déclaration de l'organisation ou de l'entité en question, autorisant le QTSP à inscrire ce rôle spécifique dans le certificat. Ledit document ne devra pas être présenté plus de 20 (vingt) jours avant la date de demande de délivrance du certificat qualifié.

L'inclusion dans le certificat qualifié d'informations concernant l'exercice de fonctions publiques ou de pouvoirs de représentation liés à des entités ou à des organisations de droit public sera soumise à des accords spécifiques avec lesdites entités. En vertu de ces accords, il sera possible de préciser la fonction exercée par le titulaire au sein de l'entité ou de l'organisation publique.

La documentation fournie sera conservée pendant une durée de 20 (vingt) ans.

INTESA n'est pas responsable des dommages dérivant d'une mauvaise utilisation d'un certificat qualifié

comprenant des informations liées aux pouvoirs de représentation.

F.1.4. Utilisation de pseudonymes

Dans certains cas, le titulaire peut demander que le certificat reporte un pseudonyme au lieu de ses données réelles.

Les informations concernant la véritable identité de l'utilisateur seront conservées pendant 20 (vingt) ans.

F.2. Enregistrement des utilisateurs demandant la certification

Au terme de la phase d'identification, les données des titulaires sont ensuite enregistrées dans les fichiers de l'autorité de certification.

Cette opération pourra être réalisée à l'aide d'une application logicielle disponible directement depuis les applications institutionnelles de la banque ou de l'institut de paiement.

G. Génération des clés de certification, d'horodatage et de signature

G.1. Génération des clés de certification

La génération des clés au sein des dispositifs de signature se déroule en présence du responsable de certification, comme prévu par l'art. 7 du DPCM.

Cette opération a lieu après l'initialisation des dispositifs de signature pour le système de génération des certificats avec lesquels les certificats des titulaires et ceux du système d'horodatage sont signés.

Ces opérations sont soumises à un double contrôle afin d'éviter toute activité illégale.

Les actions suivant la génération des paires de clés de l'autorité de certification ne sont possibles qu'à l'aide de dispositifs d'autorisation particuliers (jetons USB) : l'accès privilégié aux HSM ne peut être réalisé qu'avec les clés présentes dans les dispositifs d'autorisation visés ci-dessus.

Pour plus de sécurité, ces clés sont réparties sur plusieurs dispositifs, selon une logique de type « n-de-m » ; de cette façon, seule la présence simultanée d'au moins *n* de *m* parties de la clé permettent de poursuivre les opérations avec les privilèges correspondants. Chacune d'entre elles doit donc être conservée dans un coffre-fort séparé.

La longueur des clés de certification doit être d'au moins 2 048 bits.

G.2. Génération des clés du système d'horodatage

La génération des clés d'horodatage a lieu conformément aux indications de l'art. 49 du DPCM. La longueur des clés du système d'horodatage doit être d'au moins 2 048 bits.

G.3. Génération des clés de signature

Au terme de la phase d'enregistrement, durant laquelle les données des titulaires sont mémorisées dans les fichiers de l'autorité de certification, la clé de signature peut être générée.

Le titulaire pourra lancer la procédure de génération des clés et demander le certificat de signature associé en utilisant l'une des méthodes décrites dans le paragr. *I. Procédures opérationnelles pour la signature de documents*.

Les paires de clés de signature sont créées sur des dispositifs sécurisés de signature (HSM – *Hardware Security Module*), conformes aux spécifications visées à l'*Annexe II* du règlement eIDAS.

La longueur des clés de signature doit être d'au moins 2 048 bits.

H. Procédures de délivrance des certificats

H.1. Procédures de délivrance des certificats de certification

Après la génération des clés de certification, décrite au paragr. *G.1*, les certificats des clés publiques sont créés, conformément aux dispositions du DPCM ; ils sont ensuite signés avec les clés privées correspondantes et enregistrés dans le registre des certificats selon les modalités prévues.

Les certificats des clés de certification sont envoyés à l'AgID via le système de communication visé à l'art.12, paragr. 1, du DPCM.

L'autorité de certification génère un certificat qualifié pour chacune des clés de signature électronique qualifiée utilisées par l'agence pour la signature de la liste publique des autorités de certification et le publie dans son propre registre des certificats. L'autorité de certification doit ensuite garder une copie de la liste, signée par le département, des certificats liés aux clés de certification qu'elle rend accessible par voie télématique (art. 42, paragr. 1 et paragr. 3, du DPCM).

H.2. Procédure de délivrance des certificats de signature

INTESA délivre les certificats avec un système conforme à l'art.33 du DPCM.

Au terme de la création de la paire de clés de signature, décrite au paragr. *G.3*, une demande de nouveau certificat est générée au format *PKCS#10*, qui prouve automatiquement la possession de la clé privée et la vérification du bon fonctionnement de la paire de clés.

Après la génération des clés, la demande de certification sera immédiatement envoyée par l'application de la banque ou de l'institut à l'autorité de certification du QTSP.

La génération des certificats est enregistrée dans le journal de contrôle (DPCM, Art.18, paragr. 4).

H.2.1. Informations figurant dans les certificats de signature

Les certificats INTESA, délivrés dans le cadre du présent manuel, sont des certificats qualifiés au sens du règlement EU n° 910/2014 (eIDAS) ce qui garantit leur interopérabilité et leur reconnaissance à l'échelle communautaire.

Le certificat qualifié définit avec exactitude l'autorité de certification l'ayant délivré et contient les données nécessaires pour la vérification de la signature numérique.

Chaque certificat qualifié pour la signature électronique est conforme au règlement eIDAS et à la résolution AgID N° 147/2019 (*Lignes directrices contenant les règles techniques et les recommandations concernant la génération de certificats*).

Tous les certificats qualifiés délivrés dans le cadre des services décrits dans le présent manuel comprennent au moins une limite d'utilisation (par. *F.1.1*).

H.2.2. Code d'urgence

Conformément aux dispositions de l'art. 21 du DPCM, l'autorité de certification garantit qu'un *code d'urgence* sera fourni afin de demander la ***suspension urgente*** du certificat.

En ce qui concerne les applications décrites par le présent manuel opérationnel, le PIN fourni au titulaire au moment de l'enregistrement sera considéré comme le code d'urgence.

I. Procédures opérationnelles pour la signature de documents

Le QTSP INTESA, par l'intermédiaire des services de la banque ou de l'institut de paiement, fournit aux titulaires les moyens nécessaires pour générer des signatures électroniques qualifiées, conformément aux dispositions de la règlementation en vigueur.

Le type particulier de service ne requiert pas la présence d'une application de signature sur son ordinateur. Les

fonctions de signature peuvent en revanche être accessibles depuis le service de banque à domicile fourni par la banque ou l'institut de paiement, ou en personne auprès de ces derniers.

Les signatures électroniques qualifiées pouvant être obtenues à l'aide de ces procédures seront totalement conformes aux dispositions de l'art. 4, paragr. 2 du DPCM en ce qui concerne les algorithmes utilisés.

En outre, conformément à l'art. 4, paragr.3, du DPCM, ces documents ne contiendront pas de macro-instructions ou de codes exécutables susceptibles d'activer des fonctions pouvant, à l'insu du signataire, modifier des actes, des faits et des données figurant dans les documents signés.

Deux différentes méthodes d'authentification sont décrites ci-après. Conformément à la règlementation en vigueur, ces dernières permettent au titulaire, après enregistrement, de générer des clés de signature et de demander un certificat qualifié dans un premier temps, puis de les utiliser pour l'apposition de signatures électroniques qualifiées.

La réussite des opérations de signature est confirmée par SMS si le titulaire possède un smartphone permettant la lecture des messages. En guise d'alternative il pourra également demander à recevoir la confirmation par courrier électronique.

I.1. Authentification de type « Call Drop »

Cette méthode d'authentification demande à l'utilisateur, préalablement identifié, de passer avec son téléphone mobile (depuis le numéro fourni au moment de l'identification) un appel à un numéro de téléphone donné, fourni dans le cadre du service, afin de confirmer sa volonté de signer un document.

À la réception dudit appel, la provenance du numéro de téléphone (*Call Identifier*) préalablement attribué à l'utilisateur en phase d'enregistrement est vérifiée. En cas de réponse positive, l'opération de signature électronique qualifiée est autorisée.

Ainsi, lorsque le titulaire souhaitera signer un document en accédant au portail de la banque ou de l'institut, il utilisera un système d'authentification à deux facteurs en saisissant un code PIN (que seul l'utilisateur connaît) et un numéro de téléphone (associé à la carte SIM, que seul l'utilisateur possède).

Ce type d'authentification est également appelé « Call Drop », car lorsque le titulaire passe un appel pour être authentifié, aucune conversation n'est activée et ledit appel se termine après quelques secondes.

L'appel du titulaire ne reçoit pas de réponse, aucun frais téléphonique ne lui est donc débité.

Cette méthode est extrêmement économique et pratique, étant donné qu'aucun dispositif physique d'authentification n'est requis. Elle est également très simple à utiliser.

Nous verrons par la suite que cette méthode d'authentification est particulièrement recommandée dans les situations où le titulaire exerce depuis des postes non surveillés (par exemple lorsqu'il se connecte aux services de la banque ou de l'institut de paiement avec son ordinateur à l'aide des services de banque à domicile). Elle est, en revanche, peu praticable en présence d'un opérateur externe, lorsque le titulaire doit opérer depuis un poste surveillé par un caissier de la banque ou de l'institut de paiement.

En ce qui concerne ces situations, une solution reposant sur une gestion dynamique des numéros de téléphones à appeler pour finaliser le processus d'authentification depuis des postes dits surveillés a été développée.

I.1.1. Procédures de signature depuis des postes non surveillés (banque à domicile)

Après avoir reçu les codes nécessaires lors de la phase d'identification, le titulaire pourra demander son certificat numérique et procéder à la signature d'un document selon les méthodes décrites ci-après.

1. Le titulaire se connecte tout d'abord à l'application bancaire ou financière à l'aide de ses codes personnels pour accéder à l'application ;
2. Il choisit et vérifie ensuite le document à signer ;
3. Il saisit son code PIN ;
4. Après la validation du PIN, dans un délai préétabli (n'excédant pas la première minute) et à l'aide du numéro de téléphone mobile vérifié précédemment, le titulaire doit appeler le numéro de téléphone qui apparaît à l'écran sous forme de vidéo, afin de confirmer sa volonté de signer le document ;

5. Le système, après avoir vérifié que le numéro utilisé pour passer l'appel coïncide avec celui associé au titulaire, procède à la signature et envoie une confirmation du succès de l'opération ;
6. Si, en revanche, la période prédéfinie s'écoule sans que le système ne reçoive d'appel au numéro indiqué au point 4, l'opération est considérée comme non valide et le document ne sera pas signé.

Dans l'éventualité de plusieurs documents à signer, le titulaire doit répéter, pour chacun d'entre eux, les étapes de 2 à 5.

I.1.2. Procédures de signature depuis des postes surveillés (en personne au guichet de la banque ou de l'institut)

Après avoir obtenu le certificat qualifié, le titulaire peut procéder à la signature des documents.

Comme indiqué précédemment, la signature en présence d'un employé de la banque ou de l'institut financier pourrait empêcher le titulaire de saisir ses codes personnels et confidentiels tels que des codes PIN.

Une solution alternative a donc été développée, afin de garantir la sécurité maximale :

1. L'utilisateur se présente au guichet d'une filiale de la banque ou de l'institut (poste surveillé) où il est reconnu par le personnel en charge (comme le caissier) selon les méthodes habituelles ;
2. Après lecture du document à signer, le titulaire peut lancer le processus de signature ;
3. Le titulaire verra alors un numéro de téléphone (choisi de façon aléatoire parmi un vaste éventail de numéros disponibles) s'afficher sous forme de vidéo et une minuterie s'activer simultanément ;
4. Dans un délai préétabli (et n'excédant pas la première minute), le titulaire doit appeler le numéro s'affichant à l'écran (en utilisant son téléphone mobile vérifié précédemment) afin de confirmer sa volonté de signer le document ;
5. À ce stade, si le système établit la validité de la personne passant l'appel, il procède à la signature du document et envoie un SMS confirmant le succès de l'opération ;
6. En revanche, si le temps alloué s'écoule sans que le système ne reçoive d'appel au numéro indiqué au point 3, l'opération sera annulée.

Dans l'éventualité de plusieurs documents à signer, le titulaire doit répéter, pour chacun d'entre eux, les étapes de 2 à 5.

I.2. Authentification de type OTP mobile

En guise d'alternative à l'authentification de type « Call Drop » une seconde méthode est disponible appelée « *OTP Mobile* ».

Pour mettre en œuvre cette méthode, le titulaire devra disposer de l'un des smartphones que la banque ou l'institut considère comme adéquat pour ce service.

Après cette vérification, au moment de son identification auprès de la banque ou de l'institut où l'enregistrement a eu lieu, une adresse spécifique sur le site de la banque ou de l'institut de paiement sera communiquée au titulaire d'où il pourra télécharger une application appelée « Mobile OTP » sur son smartphone, accompagnée d'un PIN.

La procédure pour la mise en œuvre de ce deuxième type d'authentification depuis des postes surveillés et non surveillés est décrite ci-après.

I.2.1. Procédures de signature depuis des postes non surveillés (Banque à domicile)

Après avoir reçu un certificat qualifié, le titulaire peut signer un document en complétant les étapes suivantes :

1. Le titulaire commence par se connecter à l'application bancaire ou financière à l'aide de ses codes personnels lui permettant d'accéder à l'application ;
2. Il sélectionne et vérifie ensuite le document à signer ;
3. Il saisit son code PIN ;

4. Il lance l'application préalablement téléchargée sur son smartphone, et recevra un OTP mobile qu'il devra saisir après le code PIN ;
5. Le système, après avoir vérifié les code PIN et OTP mobile, procèdera à la signature et confirmera le succès de l'opération.

Si la signature est requise pour plusieurs documents, le titulaire devra répéter les étapes de 2 à 5 pour chacun d'entre eux.

I.2.2. Procédures de signature depuis des postes surveillés (en personne au guichet de la banque ou de l'institut financier)

Dans ce cas également, une solution a été développée afin d'éviter au titulaire de devoir saisir ses codes confidentiels – qui pourraient être réutilisés de manière frauduleuse à ses dépens – face au personnel de la banque ou de l'institut de paiement.

Après avoir reçu son certificat qualifié, le titulaire peut signer un document de la façon suivante :

1. L'utilisateur se présente au guichet d'une filiale de la banque ou de l'institut de paiement (poste surveillé) où il est identifié par le personnel (par ex. le caissier) selon les méthodes habituelles ;
2. Au moment de signer le document, un écran spécifique doté d'une webcam s'active face à l'utilisateur ;
3. Après avoir vérifié à l'écran le document à signer et décidé de continuer, il génère depuis son smartphone un OTP qui s'affichera également sous forme de code barre ;
4. À ce stade, le titulaire peut, en positionnant son smartphone en face de la webcam, permettre la lecture de l'OTP généré à l'étape 3 et lancer la procédure de signature à proprement parler ;
5. Après la signature du document, le système informe immédiatement le titulaire en envoyant un SMS.

Pour la signature de plusieurs documents, les étapes de 2 à 5 doivent être répétées.

I.2.3. Procédures de signature pour les clients potentiels (*Prospects*)

La procédure pour la délivrance du certificat qualifié de signature à distance peut également être mise en œuvre par un client potentiel (*Prospect*) durant les activités d'« Onboarding » (acquisition du client).

Le processus est compatible avec l'ensemble des principaux navigateurs (Chrome, Firefox, Edge, Safari) et avec les versions plus récentes des dispositifs mobiles Android et Apple.

Les clients potentiels doivent procéder comme suit :

1. Au début du processus, le client devra saisir ses données personnelles afin de permettre une identification ultérieure certaine, après signature de la note d'information en matière de confidentialité du QTSP INTESA ;
2. L'institut bancaire enverra un SMS contenant un OTP (*One Time Password*) dont la validité est temporaire. Le client doit saisir ce code afin de prouver son accès au dispositif mobile spécifié au moment de la saisie des données ;
3. Au terme du processus de vérification visé au point précédent, le *Prospect* envoie ses documents d'identité à l'institut bancaire. Les données personnelles pourront être saisies par le client ou acquises à partir des documents via un logiciel d'OCR ;
4. Une fois le processus d'enregistrement achevé, la banque enverra les documents contractuels au *Prospect*, qui peut les signer en utilisant un certificat qualifié pour les signatures numériques à distance délivré par le QTSP INTESA ;
5. Comme décrit dans la procédure concernant la banque en ligne, la documentation de demande de certificat du QTSP INTESA sera présentée au client ;
6. Celui-ci devra cocher les cases pertinentes du document confirmant qu'il l'a bien lu, et apposer sa signature électronique en saisissant un OTP que le QTSP INTESA aura envoyé par SMS ;
7. Si l'OTP fourni par le QTSP INTESA est vérifié avec succès, un certificat qualifié peut être délivré. Sinon, un nouvel OTP devra être demandé ;
8. Un code PIN devra en tous cas être saisi au moment de la génération du certificat ; celui-ci sera requis

à chaque utilisation du certificat de signature ;

9. Le certificat délivré de cette façon ne pourra en tous cas servir qu'à signer la proposition contractuelle et aucun autre document tant que la banque n'aura pas complété les vérifications de rigueur précédant l'ouverture d'un compte courant ;
10. Si les vérifications de la banque sont concluantes, le compte courant sera ouvert et le *Prospect* pourra utiliser le certificat délivré dans le cadre de ses relations avec la banque, dans le respect des limites d'utilisation ;
    En revanche, si la banque rejette la demande d'ouverture d'un compte courant, le certificat sera révoqué et ne pourra plus être utilisé ;
11. Dans les deux cas, le *Prospect* sera en tous cas informé du résultat des vérifications et de la révocation éventuelle du certificat.

I.3. Authentification par jeton OTP

Enfin, l'authentification peut être réalisée à l'aide de jetons OTP physiques (très utilisés dans le monde bancaire et financier).

Les jetons physiques OTP ne sont actuellement utilisés que depuis des postes non surveillés (généralement depuis un poste à distance dans le cadre de la banque à domicile).

Le titulaire utilise ses codes personnels pour se connecter à l'application bancaire ou financière et lance la procédure de signature en saisissant ses codes PIN et OTP, générés entretemps, et affichés sur l'écran du jeton.

J. Procédures opérationnelles pour la vérification des signatures

Les documents signés à l'aide des méthodes décrites précédemment seront exclusivement au format PDF : ce format de signature est considéré en effet comme facilement utilisable dans le cadre des applications bancaires ou financières.

Les documents signés peuvent facilement être vérifiés en utilisant le logiciel Acrobat Reader DC, en mesure de contrôler tout type de signature électronique qualifiée au format PDF, produite à l'échelle communautaire dans le respect du règlement eIDAS.

Le logiciel Acrobat Reader DC peut être téléchargé gratuitement depuis le site d'Adobe : *https://www.adobe.com/it/*

K. Procédures de révocation et de suspension des certificats

Conformément au règlement eIDAS, les informations concernant le statut du certificat peuvent être obtenues via le protocole OCSP disponible depuis l'URL indiquée sur le certificat lui-même.

La révocation et la suspension des certificats peuvent être formalisées par leur inclusion dans la liste CRL (listes de révocation et de suspension) (art. 22 du DPCM). Le profil des CRL est conforme à la norme RFC 3280. Cette liste, signée par l'autorité de certification délivrant le certificat, est régulièrement actualisée, conformément aux règlements en vigueur.

La liste des CRL figure également dans le registre des certificats.

Lorsque la révocation ou la suspension est requise par l'autorité de certification ou la tierce partie (articles 23, 25, 27 et 29 du DPCM), l'autorité informe le titulaire de la demande et du moment où l'événement requis prend effet.

La date et l'heure de prise d'effet de la révocation doit être spécifiée dans la demande (art.24, paragr. 1, DPCM).

K.1. Révocation des certificats

Un certificat peut être révoqué sur demande du titulaire, de la tierce partie concernée ou de l'autorité de

certification (à savoir le QTSP).

Les certificats révoqués ne peuvent en aucun cas être réactivés.

K.1.1. Révocation sur demande du titulaire

Le titulaire peut demander la révocation en accédant à une section spécifique, disponible dans le cadre des services de la banque ou de l'institut de paiement ou bien en contactant directement le service clients de ces derniers.

Le QTSP, après avoir été informé par la banque ou par l'institut, qui entre temps aura également bloqué les codes d'accès du titulaire, procèdera à la révocation immédiate du certificat.

K.1.2. Révocation sur demande de la tierce partie

La banque ou l'institut de paiement, en sa qualité de tierce partie concernée, peut demander la révocation du certificat.

Le QTSP, après avoir vérifié la validité de la demande, communiquera la révocation aux titulaires concernés en utilisant les moyens de communication définis avec le titulaire au moment de l'enregistrement, mis à jour et transmis dans un deuxième temps par le titulaire au QTSP, y compris via les LRA (paragr. *C.2. Obligations du titulaire*).

K.1.3. Révocation sur demande de l'autorité de certification

À l'exception des cas d'urgence justifiée, lorsque l'autorité de certification souhaite révoquer le certificat qualifié, elle devra informer préalablement la banque ou l'institut (tierce partie concernée) par courrier électronique et simultanément le titulaire ; elle pourra pour cela utiliser l'adresse électronique fournie au moment de la demande de certificat ou l'adresse de résidence, et devra préciser les motifs de la révocation ainsi que la date et l'heure de prise d'effet de celle-ci.

K.1.4. Révocation des certificats liés aux clés de certification

Dans les cas :

- d'altération de la clé de certification,
- de cessation de l'activité,

l'autorité de certification procède à la révocation des certificats de certification correspondants ainsi que des certificats de signature signés avec la clé de certification.

L'autorité de certification informera l'AgID de la révocation dans les 24 heures.

K.2. Suspension des certificats.

En ce qui concerne les modes de suspension des certificats et la communication correspondante, les indications concernant les méthodes de révocation visées au paragr. *K.1* s'appliquent.

La suspension d'un certificat est prévue dans les situations où des enquêtes complémentaires sont nécessaires pour déterminer si un certificat doit être révoqué (par exemple en cas de soupçon de perte ou de vol du jeton OTP, ou dans l'attente d'informations ultérieures permettant de déterminer avec certitude que le titulaire a cessé d'exercer les activités pour lesquelles le certificat a été délivré, etc.).

La demande de suspension peut être présentée par n'importe quelle entité visée par les articles 27, 28 et 29 du DPCM (autorité de certification, titulaire, tierce partie concernée).

Faute de communication de la part du titulaire, le certificat sera automatiquement révoqué après une période de suspension de 90 (quatre-vingt-dix) jours ou, en tous cas, à la date d'expiration du certificat.

La date de prise d'effet de la révocation coïncidera, en tous cas, avec celle de la suspension.

K.2.1. Suspension sur demande du titulaire

Le titulaire peut demander la suspension du certificat en accédant à une section spécifique mise à disposition dans le cadre des services de la banque ou de l'institut de paiement ou bien en contactant directement le service clients de ces derniers.

L'autorité de certification suspendra le certificat et informera le titulaire à l'aide des fonctions prévues à cet effet par les services de la banque ou de l'institut de paiement.

Le titulaire pourra ensuite demander la réactivation du certificat selon les modalités fournies par la banque ou par l'institut de paiement.

Faute de communications ultérieures, le certificat suspendu sera automatiquement révoqué au terme de la période de suspension et la date de révocation coïncidera avec celle de prise d'effet de la suspension.

K.2.2. Suspension sur demande de la tierce partie

En sa qualité de tierce partie concernée, la banque ou l'institut de paiement peut demander la suspension du certificat.

L'autorité de certification, après avoir déterminé la validité de la demande, suspendra le certificat dans les plus brefs délais et informera les titulaires concernés par courrier électronique ou par communication via les services de la banque ou de l'institut de paiement.

K.2.3. Suspension sur demande de l'autorité de certification

Sous réserve des cas d'urgence justifiée, l'autorité de certification pourra suspendre le certificat, pour autant qu'elle en informe préalablement le titulaire à l'adresse électronique fournie durant la phase demande de certificat au moment de l'enregistrement, ou à l'adresse de résidence, en indiquant les raisons de la suspension et la date et l'heure de prise d'effet de celle-ci.

L'autorité de certification enverra une communication analogue à la tierce partie concernée.

L. Méthode de remplacement des clés

L.1. Remplacement des certificats qualifiés et des clés du titulaire

Les certificats qualifiés de signature électronique délivrés par l'autorité de certification dans le cadre des éléments décrits dans le présent manuel opérationnel ont une validité de 36 (trente-six) mois à compter de la date de délivrance.

Au terme de cette période, la génération d'une nouvelle paire de clés de signature sera nécessaire et, simultanément, la délivrance d'un nouveau certificat.

Dans ce cas, la procédure suivie pour la délivrance du nouveau certificat sera similaire à celle indiquée au moment de la première délivrance, à l'exclusion de la phase d'identification du titulaire qui ne devra pas être répétée.

L.2. Remplacement des clés de l'autorité de certification

L.2.1. Remplacement d'urgence des clés de l'autorité de certification

En cas de panne du dispositif de signature (HSM) contenant les clés de certification (CA et TSCA), ou de désastre affectant le siège central, la procédure à utiliser est traité à la section *P. Procédure de gestion des catastrophes*.

L.2.2. Remplacement planifié des clés de certification

L'autorité de certification procèdera conformément aux dispositions de l'art. 30 du DPCM, dans les délais prévus par la réglementation en vigueur, avant l'expiration du certificat lié aux paires de clés de certification (de l'autorité de certification et d'horodatage), utilisées par les systèmes de délivrance des certificats de signature et d'horodatage.

L.3. Clés du système d'horodatage (TSA)

Conformément aux indications de l'art. 49, paragr. 2, du DPCM, afin de limiter le nombre d'horodatage générés avec la même paire de clés, ces dernières sont remplacées dans les 90 (quatre-vingt-dix) jours à compter de leur date de délivrance. Un certificat associé à la nouvelle paire de clés est délivré simultanément, n'impliquant pas la révocation du précédent lié à la paire de clés remplacée.

M. Registre des certificats

M.1. Procédures de gestion du registre des certificats

INTESA publie les informations suivantes dans le registre des certificats :

1. Les certificats des clés de signature et du système d'horodatage.
2. Les certificats des clés de certification (CA et TSCA).
3. Les certificats délivrés à la suite du remplacement des clés de certification.
4. Les certificats pour les clés de signature de l'AgID (DPCM, art.42, paragr. 1).
5. Les listes de révocation et de suspension (CRL).

Les opérations concernant le registre des certificats sont mises en œuvre uniquement par des personnes dûment autorisées, présentes en quantité adéquate afin d'empêcher les actions illicites de la part d'un nombre limité de membres du personnel.

L'autorité de certification conserve une copie de référence du registre des certificats, non accessible depuis l'extérieur : celle-ci met à jour en temps réel la copie opérationnelle, à laquelle les utilisateurs peuvent accéder avec le protocole LDAP.

La correspondance entre la copie de référence et la copie opérationnelle est systématiquement vérifiée.

M.2. Accès logique au registre des certificats

La copie de référence est placée à l'intérieur d'un réseau spécifique, protégé par des dispositifs adéquats. Elle n'est donc accessible qu'au serveur de délivrance des certificats qui enregistre les certificats délivrés et les CRL.

L'accès aux copies opérationnelles est disponible à l'adresse ***ldap://x500.e-trustcom.intesa.it*** avec le protocole LDAP.

L'autorité de certification permet également l'accès aux CRL via le protocole http, à l'URL indiquée dans le champ CDP (*CRL Distribution Point*, point de distribution des CRL) du certificat.

M.3. Accès physique aux locaux des systèmes affectés au registre des certificats

Le personnel autorisé à gérer directement le registre des certificats peut accéder au local où le système est installé et y travailler uniquement dans le cadre d'un double contrôle, afin d'éviter toute action illégale.

Les personnes en charge de la gestion des systèmes, du réseau, de la maintenance, etc., ne peuvent accéder au local où est installé le système pour y exercer leur fonction qu'en présence d'employés autorisés à gérer le registre des certificats, conformément aux modalités décrites précédemment pour les opérateurs autorisés.

N. Procédures de protection des données personnelles

Les mesures de sécurité en matière de protection des données à caractère personnel sont conformes aux dispositions prévues par le règlement européen (EU) 679/2016 (RGPD) et ses modifications et ajouts ultérieurs.

O. Procédures de gestion des copies de sécurité

Les fichiers numériques faisant l'objet de copies de sécurité sont les suivantes :

- REGISTRE DES CERTIFICATS, fichier numérique contenant le matériel indiqué au paragr. M.
- INFORMATIONS opérationnelles, fichier numérique où sont mémorisées toutes les informations reçues par le titulaire au moment de l'enregistrement et de la demande de certificat ainsi que les demandes de révocation et de suspension, accompagnées de la documentation pertinente.
- JOURNAL D'AUDIT, fichier constitué de l'ensemble des enregistrements effectués automatiquement par les systèmes installés auprès du service de certification du QTSP (art.36 du DPCM).
- ARCHIVE NUMÉRIQUE DES HORODATAGES, contenant les horodatages générés par le système d'horodatage (art. 53, paragr. 1 du DPCM).
- REGISTRE OPÉRATIONNEL DES HORODATAGES, registre dans lequel sont automatiquement mémorisés les événements liés aux activités d'horodatage, prévoyant l'enregistrement de toute anomalie ou tentative de manipulation susceptible d'affecter le fonctionnement du système d'horodatage est prévu (art. 52 du DPCM).

La conservation de toutes les copies de sécurité décrites ci-dessus, est conforme aux dispositions des règlementations en vigueur en la matière.

P. Procédures de gestion des catastrophes

Le QTSP INTESA est doté d'un plan d'urgence pour la gestion des catastrophes qui prévoit les phases suivantes :

- Gestion de l'urgence : durant cette phase, la continuité de l'accès aux CRL est garantie ; leur délivrance peut subir des retards dérivant de la nécessité d'activer le serveur de sauvegarde de l'autorité de certification (situé sur le site de sauvegarde) ;
- Gestion de la période de transition : durant cette phase, la délivrance des certificats est garantie ainsi que le rétablissement de solutions ultérieures de reprise après sinistre ;
- Retour au mode de fonctionnement habituel : sur le site original ou sur un site alternatif mais définitif.

Il convient de souligner que la présence de duplications de la copie opérationnelle du registre des certificats distribuées à plusieurs endroits permet, en cas d'interruption du fonctionnement d'un des sites, d'accéder au contenu du registre des certificats mis à jour jusqu'au moment de l'interruption.

En vue de faire face à la gestion de l'urgence, la duplication des données du système de délivrance des certificats est prévue sur le site de sauvegarde du registre des certificats. Du personnel en mesure d'activer les fonctions de délivrance des CRL interviendra également dans les 24 heures. Le personnel précité reçoit une formation adéquate, non seulement pour la gestion des systèmes logiciels et informatiques, mais également pour la gestion des urgences.

Une copie papier du plan de gestion des urgences est conservée sur tous les sites concernés par la gestion des catastrophes.

Q. Procédures pour l'apposition et la définition de la référence temporelle

Toutes les machines faisant partie de l'infrastructure à clés publiques de l'autorité de certification sont synchronisées avec l'I.N.RI.M. – *Istituto Nazionale di Ricerca Metrologica* (Institut National de Recherche Métrologique) de Turin, anciennement *Istituto Elettrotecnico Nazionale* (Institut National Electrotechnique) Galileo Ferraris. Cette fonction est possible grâce à un logiciel spécifique, installé sur chaque serveur, qui se connecte au serveur configuré à distance via le protocole NTP (*Network Time Protocol*, protocole de temps réseau).

Le *Network Time Protocol* (NTP) représente l'une des méthodes les plus sûres et flexibles pour le passage d'informations de date et d'heure sur le réseau Internet. Il permet de synchroniser continuellement les ordinateurs reliés par réseaux locaux, métropolitains ou même mondiaux (Internet) en utilisant une structure hiérarchique en pyramide.

L'I.N.RI.M fournit un service de synchronisation pour les systèmes informatiques reliés au réseau Internet, reposant sur deux serveurs NTP primaires, installés dans le laboratoire de temps-fréquence. Ceux-ci sont synchronisés à l'aide d'un générateur de code de date par les horloges atomiques à faisceau de césium, utilisées également pour générer l'échelle de temps nationale italienne UTC (IT). L'écart temporel entre les serveurs NTP de l'I.N.RI.M NTP et l'échelle de temps nationale italienne est surveillée et elle est habituellement inférieure à quelques millisecondes. La précision de synchronisation dépend du type de réseau et de la distance présente entre le serveur NTP et le système devant être synchronisé ; les valeurs d'écart type sont inférieures à la milliseconde pour les systèmes appartenant au même réseau et peuvent arriver à quelques centaines de millisecondes pour les réseaux à distance.

Le logiciel installé sur le site de l'autorité de certification se connecte au serveur à distance à intervalles réguliers ; après avoir obtenu l'heure réelle, il veille à corriger l'heure de la machine locale grâce à des algorithmes sophistiqués.

Les références temporelles utilisées par les applications sont des chaînes au format date (DD/MM/YYYY hh:mm:ss) et sont précises à la seconde près. Elles représentent l'heure locale, selon la configuration de la machine. Ces références sont conformes à l'art. 51 du DPCM.

Chaque enregistrement présent dans le journal d'Audit contient une référence temporelle ; cette dernière ayant été générée selon la modalité décrite ci-dessus est opposable aux tiers (art. 41 du DPCM).

Q.1. Procédures de demande et de vérification des horodatages

L'autorité de certification appose un horodatage (horodatage électronique qualifié conforme au règlement eIDAS) sur tous les documents signés par le titulaire dans le cadre des services décrits par ce manuel opérationnel.

L'apposition de cet horodatage est un processus intégré à l'opération de signature et ne requiert aucune action spécifique de la part du titulaire.

R. Délai d'exécution et tableau RACI pour la délivrance des certificats

Le Tableau ci-après reporte le « Process Lead Time » (délais d'exécution) pour la gestion des demandes de délivrance, révocation, suspension et réactivation des certificats ;

Personne	Demande	Partie impliquée	Action de la partie impliquée	Partie impliquée	Action de la partie impliquée
Utilisateur demandeur, Titulaire certificat	*Demande de délivrance du Certificat à LRA*	*Banque ou Institut (au titre de) RA locale*	*Émet l'ordre de publication du certificat à l'autorité après vérification identité*	*Autorité de Certification*	*Traitement demande de certification*
Utilisateur demandeur, Titulaire certificat	*Demande de révocation du Certificat à RA ou LRA*	*Intesa (au titre d') Autorité d'enregistrement (RA) ou Banque ou Institut (au titre de LRA)*	*Émet l'ordre de révocation du certificat à l'autorité après vérification identité*	*Autorité de Certification*	*Traitement demande de révocation*
Utilisateur demandeur, Titulaire certificat	*Demande de suspension du Certificat à RA ou LRA*	*Intesa (au titre d') Autorité d'enregistrement (RA) ou Banque ou Institut (en qualité de LRA)*	*Émet l'ordre de suspension du certificat à l'autorité après vérification identité*	*Autorité de Certification*	*Traitement demande de suspension*
Utilisateur demandeur, Titulaire certificat	*Demande de réactivation du Certificat à RA ou LRA*	*Intesa (au titre d') Autorité d'enregistrement (RA) ou Banque ou Institut (au titre de LRA)*	*Émet l'ordre de réactivation du certificat à CA après vérification identité*	*Autorité de Certification*	*Traitement demande de réactivation*

Ci-après le tableau RACI identifie les responsabilités des parties concernées par les demandes de délivrance,

révocation, suspension et réactivation des certificats.

Personne Impliquée	Responsable	Chargé de	Consulté	Informé
Autorité d'enregistrement	***X***			
Autorité d'enregistrement local	***X***			
Autorité de Certification		***X***		
Utilisateur, demandeur, titulaire du certificat			***X***	***X***

S. Références techniques

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)

------- FIN DU DOCUMENT -------