Politique de Certification

Certificate Policy
Certificate Practice Statement

CODE DU DOCUMENT	ICERT-INDI-MO*
VERSION	4.2
DATE	24/03/2020

* à partir de la version 4.0, les documents ICERT-INDI-MO et ICERT-INDI-MO-ENT ont été fusionnés dans ce document

a

InfoCert
TINEXTA GROUP

1

TABLE DES MATIÈRES

TABLE DES FIGURES

1 INTRODUCTION

1.1 Présentation générale

Un certificat relie la clé publique à un ensemble d'informations qui identifient la personne qui détient la clé privée correspondante : cette personne physique ou morale est le **Sujet** du certificat. Le certificat est utilisé par d'autres personnes pour trouver la clé publique, distribuée avec le certificat, et vérifier la signature électronique qualifiée apposée ou associée à un document. Le certificat garantit la correspondance entre la clé publique et le Sujet. Le degré de fiabilité de cette association dépend de plusieurs facteurs : la procédure selon laquelle l'Autorité de Certification a délivré le certificat, les mesures de sécurité adoptées, les obligations assumées par le Sujet pour la protection de sa clé privée et les garanties offertes.
Le présent document est la Politique de Certification du **Prestataire de Services de Confiance InfoCert** *(Trust Service Provider*) qui, parmi les services de confiance, fournit également des services de signature électronique qualifiée. Ce document contient les politiques et les pratiques suivies dans le processus d'identification et de délivrance du certificat qualifié, les mesures de sécurité adoptées, les obligations, les garanties et les responsabilités, et décrit en général tout ce qui fait qu'un certificat qualifié est fiable, conformément à la législation en vigueur en matière de services de confiance, de signature électronique et de cachet électronique qualifiés, ainsi que de signature numérique.
Le fait de publier cette Politique de Certification et d'y faire référence dans les certificats permet aux utilisateurs d'évaluer les caractéristiques et la fiabilité du service de certification et donc du lien entre les clés et le Sujet.
Le contenu est basé sur la réglementation en vigueur à la date de sa délivrance et transpose les recommandations du document « Request for Comments: 3647 – Internet X.509 Public Key Infrastructure Certificate Policy and Certification Practices Framework » © Internet Society 2003.

Cette Politique de Certification contient également les politiques et les pratiques suivies par InfoCert dans le processus de vérification des demandes, d'identification des demandeurs et de délivrance des certificats pour l'authentification de sites internet conformément à l'article 34 du règlement délégué (UE) 2018/389 [12] complétant la directive (UE) 2015/2366 (DSP2) [11], conformément aux exigences définies par la norme ETSI TS 119 495 (ci-après dénommés « Certificats DSP2 »).

1.2 Nom et identification du document

Ce document est dénommé « Prestataire de Services de Confiance – Politique de Certification » et est caractérisé par le code : **ICERT-INDI-MO**. La version et le niveau d'édition sont identifiables dans l'en-tête de chaque page.

La version 4.0 de ce document s'inscrit dans la continuité des précédentes Politiques de Certification ci-dessous et les remplace :

- ICERT-INDI-MO, version 3.5 du 30/11/2018 pour la délivrance de certificats qualifiés à une

personne physique et morale, y compris au moyen d'un système CMS
- ICERT-INDI-MO-ENT, version 3.5 du 30/11/2018, pour la délivrance de certificats qualifiés à une personne physique, de type *LongTerm* et *OneShot*

décrivant dans un seul document les politiques et procédures de gestion des certificats qualifiés conformément au règlement eIDAS [1].

Le document est associé aux identifiants d'objet (OID), décrits ci-dessous, qui sont référencés dans l'extension *CertificatePolicy* des certificats, en fonction de leur utilisation prévue. La signification des OID est la suivante :

L'identifiant d'objet (OID) qui identifie InfoCert est 1.3.76.36.

Les politiques pour les certificats qualifiés sont :

Politique de certification-certificat qualifié délivré à une personne physique	1.3.76.36.1.1.48.1 conforme à la politique QCP-n 0.4.0.194112.1.0
Politique de certification-certificat qualifié délivré à une personne physique et clés sur dispositif (SSCD)	1.3.76.36.1.1.48.2 conforme à la politique QCP-n 0.4.0.194112.1.0
Politique de certification-certificat qualifié délivré à une personne morale également sur dispositif (SSCD) Également disponible pour DSP2 (QSealC)	1.3.76.36.1.1.47 conforme à la politique QCP-l 0.4.0.194112.1.1

Les politiques pour les certificats qualifiés sur dispositif qualifié sont :

Politique de certification-certificat qualifié délivré à une personne physique et clés sur dispositif qualifié (QSCD)	1.3.76.36.1.1.1/1.3.76.36.1.1.61 conforme à la politique QCP-n-qscd 0.4.0.194112.1.2
Politique de certification-certificat qualifié délivré à une personne physique pour signature automatique à distance sur dispositif (QSCD)	1.3.76.36.1.1.2/1.3.76.36.1.1.62 conforme à la politique QCP-n-qscd 0.4.0.194112.1.2
Politique de certification-certificat qualifié délivré à une personne physique pour signature à distance sur dispositif (QSCD)	1.3.76.36.1.1.22/1.3.76.36.1.1.63 conforme à la politique QCP-n-qscd 0.4.0.194112.1.2
Politique de certification-certificat qualifié délivré à une personne physique à travers un système CMS sur dispositif (QSCD)	1.3.76.36.1.1.32/1.3.76.36.1.1.66 conforme à la politique QCP-n-qscd 0.4.0.194112.1.2
Politique de certification-certificat qualifié délivré à une personne morale sur dispositif (QSCD) Également disponible pour DSP2 (QSealC)	1.3.76.36.1.1.46 conforme à la politique QCP-l-qscd 0.4.0.194112.1.3
Politique de certification-certificat qualifié délivré à une personne physique pour signature à distance sur dispositif qualifié	1.3.76.36.1.1.35/1.3.76.36.1.1.65 conforme à la politique QCP-n-qscd 0.4.0.194112.1.2
Politique de certification-certificat qualifié délivré à une personne physique pour signature à distance sur dispositif qualifié de type *one-shot*	1.3.76.36.1.1.34/1.3.76.36.1.1.64 conforme à la politique QCP-n-qscd 0.4.0.194112.1.2

D'autres OID peuvent figurer sur le certificat pour indiquer l'existence de limites d'utilisation. Ces OID sont énumérés au § 4.5.3. La présence des limites d'utilisation ne modifie en rien les règles établies dans le reste de la Politique de Certification.
En outre, tous les certificats conformes aux recommandations de l'avis de l'AgID n° 121/2019, à compter du 5 juillet 2019, contiendront un élément *PolicyIdentifier* supplémentaire avec valeur agIDcert (OID 1.3.76.16.6) dans le champ *CertificatePolicies* (OID 2.5.29.32).[1]Ce document est publié sous forme électronique sur le site web du prestataire de services de confiance à l'adresse suivante : http://www.firma.infocert.it, section « Documentation».

1.3 Entités intervenantes et responsabilités

1.3.1 Certification Authority – Autorité de Certification

L'**Autorité de Certification** est le tiers de confiance qui émet les certificats de signature électronique qualifiée en les signant avec sa propre clé privée, appelée clé d'AC ou clé racine.
InfoCert est l'Autorité de Certification **(AC**) qui délivre les Certificats Qualifiés, les publie dans l'annuaire et les révoque, en opérant conformément aux règles techniques édictées par l'Autorité de Contrôle et conformément aux prescriptions du règlement eIDAS [1] et celles du code de l'administration numérique [2].

Les données complètes concernant l'organisation qui exerce la fonction d'AC sont les suivantes :

Dénomination sociale	**InfoCert – Société anonyme** **Société sous la direction et la coordination de Tinexta S.p.A.**
Siège social statutaire	Piazza Sallustio n° 9, 00187, Rome (RM)
Siège opérationnel	Via Marco e Marcelliano n° 45, 00147, Rome (RM)
Représentant légal	Danilo Cattaneo En qualité d'administrateur délégué
Numéro de téléphone	+39 06 836691
N° d'immatriculation RCS	Numéro fiscal 07945211006
N° de TVA	07945211006
Site web	https://www.infocert.it

1.3.2 Registration authority – Autorité d'Enregistrement (AE)

Les ***Registration Authorities*** **ou Autorités d'Enregistrement** sont des entités auxquelles l'AC a conféré un mandat avec représentation, grâce auquel elle confie l'exécution d'une ou plusieurs

[1] L'absence de cet OID peut conduire à l'inadéquation des services de réseau offerts dans le contexte spécifique italien. En ce sens, on peut citer l'exemple de l'absence d'obligation d'indiquer le numéro d'identification fiscale du propriétaire dans le certificat qualifié pour générer la signature , alors qu'il s'agit d'un élément indispensable pour plusieurs administrations publiques italiennes.

activités propres au processus d'enregistrement, comme :

- l'identification du Sujet ou du Demandeur,
- l'enregistrement des données du Sujet,
- la transmission des données du Sujet aux systèmes de l'AC,
- la collecte de la demande de certificat qualifié,
- la distribution et/ou l'initialisation du dispositif de signature sécurisé, le cas échéant,
- l'activation de la procédure de certification de la clé publique,
- la fourniture d'un soutien au Sujet, au Demandeur et à l'AC dans les phases éventuelles de renouvellement, de révocation ou de suspension des certificats.

Fondamentalement, l'Autorité d'Enregistrement effectue toutes les activités d'interface entre l'Autorité de Certification et le Demandeur ou le Sujet, sur la base des accords conclus. Le mandat avec représentation, connu sous le nom de « Convention AEO », réglemente le type d'activités confiées par l'AC à l'AE et leur mode d'exécution d'un point de vue opérationnel.
Les AE sont mises en place par l'AC après une formation adéquate du personnel employé ; l'AC vérifie que les procédures utilisées sont conformes à la présente Politique de Certification.

1.3.2.1 Opérateur d'Enregistrement (OE)

L'AE peut désigner, au moyen de formulaires spécifiques, des personnes physiques ou morales à qui elle confie l'exécution des activités d'identification du Sujet. Les **Opérateurs d'Enregistrement** opèrent sur la base des instructions reçues par l'AE dont ils dépendent et qui a pour mission de contrôler que les procédures mises en œuvre sont correctes.

1.3.3 Sujet

Le **Sujet** est la personne physique ou morale propriétaire du certificat qualifié, dans lequel sont insérées les données d'identification fondamentales. Dans certaines parties de la Politique de Certification et dans certaines limites d'utilisation, il peut aussi être appelé Propriétaire.

1.3.4 Utilisateur

C'est celui qui reçoit un document informatique signé avec le certificat numérique du Sujet, et qui se fie à la validité du certificat lui-même (et/ou à la signature électronique qui y est présente) pour évaluer l'exactitude et la validité du document en question, dans les contextes où il est utilisé.

1.3.5 Demandeur

Il s'agit de la personne physique ou morale qui demande à l'AC de délivrer des certificats numériques pour un Sujet, en supportant éventuellement les coûts, en ayant ainsi droit de suspendre ou de révoquer les certificats en question. Le cas échéant, son rôle peut également être assumé par l'AE.
On peut citer, plus précisément, les cas suivants :

- il peut correspondre au Sujet s'il s'agit d'une personne physique ;
- il peut être la personne physique qui a le pouvoir de demander un certificat pour une personne morale ;
- il peut être la personne morale qui demande le certificat pour des personnes physiques qui lui sont liées par des relations d'affaires ou dans le cadre d'organisations ;
- il peut être le parent ou le tuteur dans le cas d'une personne mineure de plus de 14 ans.

Le Demandeur peut être la personne physique ou morale dont découlent les pouvoirs de signature ou le rôle du Sujet. Dans ce cas, lorsque le Demandeur est également défini comme un *Tiers Concerné*, le certificat indiquera l'Organisation à laquelle le Sujet en question est lié et/ou son rôle. Sauf indication contraire dans la documentation contractuelle, le Demandeur correspond au Sujet.

1.3.6 Autorité

1.3.6.1 AgID – Agenzia per l'Italia Digitale (Agence pour l'Italie numérique)

L'Agenzia per l'Italia Digitale **(AgID**) est l'organe de contrôle des prestataires de services de confiance au sens de l'article 17 du règlement eIDAS. À ce titre, l'AgID contrôle les prestataires de services de confiance qualifiés établis en Italie afin de s'assurer qu'ils respectent les exigences du règlement.

1.3.6.2 Organisme d'Évaluation de la Conformité

L'organisme d'Évaluation de la Conformité **(OEC**) est un organisme accrédité conformément au règlement eIDAS, qui est compétent pour évaluer la conformité du prestataire de services de confiance qualifié et des services de confiance qualifiés qu'il fournit selon les règlements et normes applicables.

1.3.6.3 Autorité Nationale Compétente (ANC)

Dans le cadre de la DSP2[11], l'autorité de surveillance nationale des intermédiaires financiers est l'organe responsable de l'autorisation des PSP dans chaque État membre. Si l'autorisation est accordée, l'ANC délivre un numéro d'autorisation et publie ces informations dans ses registres publics.

1.3.6.4 Autorité Bancaire Européenne (ABE)

L'Autorité Bancaire Européenne **(ABE**) s'emploie à assurer un niveau de réglementation et de surveillance cohérent dans le secteur bancaire européen. Dans le cadre de la DSP2[11], elle contrôle et garantit la transparence des actions des prestataires de services de paiement (PSP) autorisés par les ANC compétentes pour chaque État membre. Elle est chargée du développement et de la gestion du « Registre électronique central », dans lequel chaque ANC doit publier la liste des noms et les informations concernant les sujets autorisés.

1.4 Utilisation du certificat

1.4.1 Utilisations autorisées

Les certificats émis par l'AC InfoCert, selon les procédures indiquées dans la présente Politique de Certification, sont des Certificats Qualifiés conformément au code de l'administration numérique – CAD – et au règlement eIDAS.

Le certificat émis par l'AC sera utilisé pour vérifier la signature qualifiée ou le cachet électronique du Sujet auquel le certificat appartient.

L'AC InfoCert propose certains produits disponibles sur le site InfoCert pour la vérification des signatures. D'autres produits de vérification ayant des fonctionnalités et des limites correspondant aux spécifications du fournisseur peuvent être disponibles sur le marché.

1.4.2 Utilisations non autorisées

L'utilisation du certificat en dehors des limites et des contextes spécifiés dans la Politique de Certification et dans les contrats, et en tout cas en violation des limites d'utilisation et de valeur *(key usage, extended key usage, user notice*) indiquées dans le certificat, n'est pas autorisée.

1.5 Gestion de la Politique de Certification

1.5.1 Contacts

InfoCert est responsable de la définition, de la publication et de la mise à jour de ce document. Toute question, réclamation, observation ou demandes d'éclaircissement concernant la présente Politique de Certification doit être envoyée à l'adresse et à la personne indiquées ci-dessous :

InfoCert S.p.A..
Responsable du Service de Certification Numérique
Piazza Luigi da Porto n° 3
35131 Padoue
Téléphone : +39 06 836691
Fax : +39 049 0978914
Centre d'appel : +39 06 54641489
Site web : https://www.firma.infocert.it
courriel : firma.digitale@legalmail.it

Le Sujet et le Demandeur peuvent demander une copie de la documentation le concernant en remplissant et en envoyant le formulaire disponible sur le site www.firma.infocert.it et en suivant la procédure qui y est indiquée. La documentation sera envoyée sous format électronique à l'adresse électronique indiquée sur le formulaire.

1.5.2 Entités responsables de l'approbation de la Politique de Certification

Cette Politique de Certification est vérifiée par le Responsable de la Sécurité et des Politiques, le Responsable de la Protection de la Vie Privée, le Responsable du Service de Certification, le Service Juridique et le Département de Conseil, et est approuvée par la direction de l'entreprise.

1.5.3 Procédures d'approbation

La rédaction et l'approbation de la Politique de Certification suivent les procédures prévues par le Système de Management Qualité de l'entreprise ISO 9001:2015.
Au plus une fois par an, le Prestataire de Services de Confiance vérifie que la présente Politique de Certification est conforme à son processus de prestation de services de certification.

1.6 Définitions et acronymes

1.6.1 Définitions

Les définitions utilisées dans la préparation de ce document sont énumérées ci-dessous. Pour les termes définis dans le règlement eIDAS [1] et dans le code de l'administration numérique – CAD [2], veuillez vous référer aux définitions qui y figurent. Le cas échéant, le terme anglais correspondant, généralement utilisé dans la presse, les normes et les documents techniques, est indiqué entre crochets.

Terme	Définition
Autocertification	C'est la déclaration adressée à l'AC – faite personnellement par celui qui sera le Sujet du certificat numérique – qui consiste à reconnaître l'existence d'états, de faits, de qualités en assumant les responsabilités établies par la loi.
OEC – Organisme d'Évaluation de la Conformité	Organisme accrédité conformément au règlement eIDAS compétent pour évaluer la conformité du prestataire de services de confiance qualifié et des services de confiance qualifiés qu'il fournit. Il rédige le REC.
REC – Rapport d'évaluation de la conformité	Rapport par lequel l'organisme d'évaluation de la conformité confirme que le prestataire de services de confiance qualifié et les services de confiance eux-mêmes satisfont aux exigences du règlement (cf. eIDAS [1]).
Système de gestion de cartes (CMS)	Instrument d'authentification, d'identification, de collecte et de conservation des données relatives aux Sujets ou aux Demandeurs.
Certificat de signature électronique	Une attestation électronique qui associe les données de validation d'une signature électronique à une personne physique et confirme au moins le nom ou le pseudonyme de cette personne (cf. eIDAS [1]) .
Certificat de cachet électronique	Une attestation électronique qui associe les données de validation d'un cachet électronique à une personne morale et confirme le nom de cette personne (cf. eIDAS [1]).
Certificat qualifié de signature électronique	Un certificat de signature électronique délivré par un prestataire de services de confiance qualifié et conforme aux exigences visées à l'annexe I du règlement eIDAS (cf. eIDAS [1]).
Certificat qualifié de cachet électronique (QSealC)	Un certificat de cachet électronique délivré par un prestataire de services de confiance qualifié et conforme aux exigences visées à l'annexe III du règlement eIDAS (cf. eIDAS [1]).
Certificat de cachet électronique pour DSP2 (QSealC DSP2)	QSealC visé à l'article 34 du règlement délégué (UE) 2018/389 [12] complétant la directive (UE) 2015/2366 (DSP2) [11], conformément aux exigences définies par la norme ETSI TS 119 495 (ci-après dénommé « QSealC DSP2 »)
Certificat *LongTerm*	Certificat qualifié de signature électronique qualifiée pour la procédure à distance. L'utilisation de ce certificat est limitée exclusivement à un domaine informatique pour lequel il a été délivré.

Terme	Définition
Certificat *OneShot*	Il s'agit d'un certificat qualifié de signature électronique qualifiée pour la procédure à distance réglementé dans la présente Politique de Certification dont les clés, une fois générées, ne sont disponibles que dans le cadre d'un domaine informatique et exclusivement pour la transaction de signature pour laquelle il a été émis. La clé privée est détruite immédiatement après son utilisation.
Clé de certification ou clé racine	Bi-clé cryptographique utilisée par l'AC pour signer les certificats et les listes de certificats révoqués ou suspendus.
Clé privée	L'élément de la bi-clé asymétrique utilisé par le Sujet, au moyen duquel il appose la signature électronique qualifiée sur le document informatique (cf. CAD [2]).
Clé publique	L'élément de la bi-clé asymétrique destiné à être rendu public, grâce auquel la signature électronique qualifiée apposée sur le document informatique par le Sujet est vérifiée (cf. CAD [2]).
Code d'urgence (ERC – *Emergency Request Code*)	Code de sécurité donné au Sujet pour transmettre sa demande de suspension d'un certificat sur les portails du PSC.
Validation	Le processus de vérification et de confirmation de la validité d'une signature ou d'un cachet électronique (cf. eIDAS [1]).
Données de validation	Données utilisées pour valider une signature électronique (cf. eIDAS [1]).
Données d'identification personnelle	Un ensemble de données permettant d'établir l'identité d'une personne physique ou morale, ou d'une personne physique représentant une personne morale (cf. eIDAS [1]).
Données pour la création d'une signature électronique	Les données uniques utilisées par le signataire pour créer une signature électronique (cf. eIDAS [1]).
Dispositif pour la création d'une signature électronique (dispositif sécurisé de création de signature électronique SSCD)	Un logiciel ou matériel configuré utilisé pour créer une signature électronique (cf. eIDAS [1]).
Dispositif de création de signature électronique qualifié (QSCD)	Un dispositif de création de signature électronique qui respecte les exigences fixées à l'annexe II du règlement eIDAS (cf. eIDAS [1]).
Document électronique	Tout contenu conservé sous forme électronique, notamment un texte ou un enregistrement sonore, visuel ou audiovisuel (cf. eIDAS [1]).
Domaine informatique	Il correspond aux applications au moyen desquelles le certificat qualifié est délivré au Sujet et dans lesquelles le Sujet peut utiliser le certificat pour la signature de documents informatiques. Les applications peuvent être gérées directement par le Certificateur ou par le Demandeur et peuvent également contenir des dispositions supplémentaires particulières en fonction de la procédure d'identification adoptée pour la délivrance du certificat qualifié.
Signature automatique	Procédure informatique particulière de signature électronique effectuée après autorisation du signataire qui garde le contrôle exclusif de ses propres clés de signature, en l'absence d'une supervision ponctuelle et continue de ce dernier.

Terme	Définition
Signature numérique	Un type particulier de signature électronique avancée basée sur un certificat qualifié et sur un système de clés cryptographiques, l'une publique et l'autre privée, étroitement liées, qui permet au Sujet – par le biais de la clé privée – et au destinataire – par le biais de la clé publique – respectivement, de rendre manifeste et de vérifier l'origine et l'intégrité d'un document informatique ou d'un ensemble de documents informatiques (cf. CAD [2]).
Signature électronique	Données sous forme électronique, qui sont jointes ou associées logiquement à d'autres données sous forme électronique et que le signataire utilise pour signer (cf. eIDAS [1]).
Signature électronique avancée	Une signature électronique qui respecte les exigences fixées à l'article 26 du règlement eIDAS (cf. eIDAS [1]).
Signature électronique qualifiée	Une signature électronique avancée qui est créée à l'aide d'un dispositif de création de signature électronique qualifié, et qui repose sur un certificat qualifié de signature électronique (cf. eIDAS [1]).
Signature à distance	Procédure particulière de signature électronique qualifiée ou de signature numérique, générée sur HSM – module matériel de sécurité – qui permet de garantir le contrôle exclusif des clés privées par leur propriétaire
Signataire	Une personne physique qui crée une signature électronique (cf. eIDAS [1]).
Journaux d'évènements	Dans les journaux d'évènements sont enregistrés, automatiquement ou manuellement, tous les événements prévus par les Règles Techniques [9].
Identification électronique	Le processus consistant à utiliser des données d'identification personnelle sous une forme électronique représentant de manière unique une personne physique ou morale, ou une personne physique représentant une personne morale (cf. eIDAS [1]).
Liste des Certificats Révoqués ou Suspendus [LCR]	Il s'agit d'une liste de certificats qui ont été « invalidés » avant leur date d'expiration naturelle. L'opération est appelée révocation si elle est définitive, et suspension si elle est temporaire. Lorsqu'un certificat est révoqué ou suspendu, son numéro de série est ajouté à la LCR, qui est ensuite publiée dans l'annuaire.
Politique de Certification [*certificate practice statement* – déclaration des pratiques de certification]	La Politique de Certification définit les procédures que l'AC applique pour l'exécution du service. Pour l'élaboration Politique de Certification, les indications fournies par l'Autorité de Contrôle et celles de la littérature internationale ont été suivies.
Moyen d'identification électronique	Un élément matériel et/ou immatériel contenant des données d'identification personnelle et utilisé pour s'authentifier pour un service en ligne (cf. eIDAS [1]).
OCSP – Protocole de vérification de certificat en ligne (*Online Certificate Status Protocol*)	Protocole défini par l'IETF dans la RFC 6960 qui permet aux applications de vérifier la validité du certificat de façon plus rapide et plus ponctuelle que la LCR, dont il partage les données.

Terme	Définition
OTP – Mot de passe à usage unique (*One Time Password*)	Un OTP (mot de passe à usage unique) est un mot de passe qui n'est valable que pour une seule transaction. L'OTP est généré et mis à la disposition du Sujet juste avant d'apposer sa signature électronique qualifiée. Il peut être basé sur des dispositifs matériels ou des procédures logicielles.
Partie utilisatrice	Une personne physique ou morale qui se fie à une identification électronique ou à un service de confiance (cf. eIDAS [1]).
Prestataire de services de confiance	Une personne physique ou morale qui fournit un ou plusieurs services de confiance, en tant que prestataire de services de confiance qualifié ou non qualifié (cf. eIDAS [1]).
Prestataire de services de confiance qualifié	Un prestataire de services de confiance qui fournit un ou plusieurs services de confiance qualifiés et a obtenu de l'organe de contrôle le statut qualifié (cf. eIDAS [1]).
Produit	Un dispositif matériel ou logiciel, ou les composants correspondants du dispositif matériel ou logiciel, qui sont destinés à être utilisés pour la fourniture de services de confiance (cf. eIDAS [1]).
Officier public	Personne qui, dans le cadre des activités qu'elle exerce, est autorisée à fournir la preuve de l'identité de personnes physiques, en vertu de la loi pertinente.
Annuaire [*Directory*]	L'annuaire est une archive qui contient : ▪ tous les certificats émis par l'AC dont la publication a été demandée par le Sujet ; ▪ la Liste des Certificats Révoqués et Suspendus (LCR).
Révocation ou suspension d'un certificat	Il s'agit de l'opération par laquelle l'AC annule la validité du certificat avant sa date d'expiration naturelle.
Rôle	Le terme Rôle indique de manière générique le titre et/ou l'habilitation professionnelle du Sujet, ou le Pouvoir éventuel de représenter des personnes physiques ou des organismes de droit privé ou public, ou l'appartenance à ces organismes ainsi que l'exercice de fonctions publiques.
Service de confiance	Un service électronique normalement fourni contre rémunération qui consiste : a) en la création, en la vérification et en la validation de signatures électroniques, de cachets électroniques ou d'horodatages électroniques, de services d'envoi recommandé électronique et de certificats relatifs à ces services ; ou b) en la création, en la vérification et en la validation de certificats pour l'authentification de sites web ; ou c) en la conservation de signatures électroniques, de cachets électroniques ou des certificats relatifs à ces services (cf. eIDAS [1]).
Service de confiance qualifié	Un service de confiance qui répond aux exigences pertinentes définies dans le règlement (cf. eIDAS [1]).
Cachet électronique	Des données sous forme électronique, qui sont jointes ou associées logiquement à d'autres données sous forme électronique pour garantir l'origine et l'intégrité de ces dernières (cf. eIDAS [1]).

Terme	Définition
Cachet électronique avancé	Un cachet électronique qui respecte les exigences fixées à l'article 36 du règlement eIDAS (cf. eIDAS [1]).
Cachet électronique qualifié	Un cachet électronique avancé qui est créé à l'aide d'un dispositif de création de cachet électronique qualifié et qui repose sur un certificat qualifié de cachet électronique (cf. eIDAS [1]).
État membre	État membre de l'Union européenne
Temps universel coordonné [Coordinated Universal Time] :	Échelle de temps avec une précision de l'ordre de la seconde, telle que définie dans la recommandation UIT-R TF.460-5.
Horodatage électronique	Des données sous forme électronique qui associent d'autres données sous forme électronique à un instant particulier et établissent la preuve que ces dernières données existaient à cet instant (cf. eIDAS [1]).
Horodatage électronique qualifié	Un horodatage électronique qui respecte les exigences fixées à l'article 42 du règlement eIDAS (cf. eIDAS [1]).
WebCam	Petite caméra vidéo conçue pour diffuser des images en streaming par internet et capturer des images photographiques. Connectée à un PC ou intégrée à des dispositifs mobiles, elle est utilisée pour les chats vidéos ou les visioconférences.

1.6.2 Acronymes et abréviations

Acronyme	
AgID	Agenzia per l'Italia Digitale (Agence pour l'Italie numérique) : Autorité de Surveillance des Prestataires de Services de Confiance
AC	Autorité de Certification
OEC	Organisme d'Évaluation de la Conformité
CAD	Code de l'administration numérique
REC	Rapport d'Évaluation de la Conformité
CC	Critères Communs
CIE	Carte d'Identité Électronique
CMS	Système de gestion de cartes (*Card Management System*)
CNS – TS-CNS	*Carta Nazionale dei servizi* ; CEAM où figure le numéro d'identification fiscale Tessera Sanitaria – Carta Nazionale dei Serivizi ; Carte Vitale – CEAM où figure le numéro d'identification fiscale
LCR	Liste des Certificats Révoqués
DMZ	Zone démilitarisée (*Demilitarized Zone*)
DN	Nom distinctif (*Distinguished Name*)
NAE	Niveau d'Assurance de l'Évaluation

Acronyme	
ABE	Autorité Bancaire Européenne
eID	Identité électronique (*Electronic Identity*)
eIDAS	Règlement sur l'identification électronique et les services de confiance pour les transactions électroniques
ERC	Code d'urgence (*Emergency Request Code*)
ETSI	Institut européen des normes de télécommunications (*European Telecommunications Standards Institute*)
FIPS	*Federal Information Processing Standard*
HSM	Boîte noire transactionnelle (*Hardware Secure Module*) : dispositif sécurisé de création de signature, avec des fonctionnalités similaires à celles des cartes à puce, mais avec une mémoire et des performances supérieures
HTTP	Protocole de transfert hypertexte (*HyperText Transfer Protocol*)
IETF	*Internet Engineering Task Force*
OE	Opérateur d'Enregistrement
ISO	Organisation internationale de normalisation (*International Organization for Standardization*) : fondée en 1946, l'ISO est une organisation internationale composée d'organismes nationaux de normalisation
UIT	Union Internationale des Télécommunications : fondée en 1865, c'est l'organisation internationale qui définit les normes en matière de télécommunications
IUP	Identifiant Unique du Propriétaire : il s'agit d'un code associé au Sujet qui l'identifie de manière unique auprès de l'AC ; le Sujet a des codes différents pour chaque certificat en sa possession
LDAP	*Lightweight Directory Access Protocol* : protocole utilisé pour accéder au registre des certificats
NA	Niveau d'Assurance
ANC	Autorité Nationale Compétente
N° RCS	Numéro de RCS (*National Trade Register*)
OID	Identifiant d'objet (*Object Identifier*) : il consiste en une séquence de nombres, enregistrée selon la procédure indiquée dans la norme ISO/IEC 6523, qui identifie un objet donné au sein d'une hiérarchie
OTP	Mot de passe à usage unique (*One Time Password*)
PEC	Courrier électronique certifié (*Posta Elettronica Certificata*)
PIN	Numéro d'identification personnel (*Personal Identification Number*) : code associé à un dispositif sécurisé de signature, utilisé par le Sujet pour accéder aux fonctions du dispositif en question
PKCS	Standards de cryptographie à clé publique (*Public-Key Cryptography Standards*)
IGC	Infrastructure de Gestion de Clés : ensemble de ressources, de processus et de moyens technologiques qui permettent à des tiers de confiance de vérifier et/ou de garantir l'identité d'un Sujet, ainsi que

Acronyme	
	d'associer une clé publique à un Sujet
DSP2	Directive sur les Services de Paiement 2
PSP	Prestataire de Services de Paiement
QSealC	Certificat de cachet électronique qualifié
AE	Autorité d'Enregistrement
RFC	Demande de commentaires (*Request for Comments*) : document rédigé sur l'initiative d'experts techniques contenant des informations ou des spécifications concernant les nouvelles recherches, innovations et méthodologies dans le domaine des TI, avant d'être évalué par la communautaire Internet
RSA	Découle des initiales des inventeurs de l'algorithme : River, Shamir, Adleman
SGSI	Système de gestion de la sécurité de l'information
SPID	Système public d'identité numérique (*Sistema Pubblico di Identità Digitale*)
SSCD - QSSCD	*Secure Signature Creation Device* : dispositif sécurisé de création de signatures électroniques *Qualified Secure Signature Creation Device* : dispositif sécurisé qualifié pour la création de signatures électroniques
NIF	Numéro d'Identification Fiscale
UUID	Identifiant universel unique (*Universally Unique Identifier*)
URL	Localisateur uniforme de ressource
N° TVA	Numéro de TVA
X500	Norme UIT-T pour les services LDAP et annuaires
X509	Norme UIT-T pour les IGC

2 PUBLICATION ET ARCHIVAGE

2.1 Archivage

Les certificats publiés, les LCR et les Politiques de Certification sont publiés et disponibles 24 heures sur 24, 7 jours sur 7.

2.2 Publication des informations relatives à la certification

2.2.1 Publication de la Politique de Certification

La présente Politique de Certification, la liste des certificats des clés de certification et les autres informations relatives à l'AC requises par la loi sont publiées sur la liste des certificateurs (à l'adresse https://eidas.agid.gov.it/TL/TSL-IT.xml)et sur le site web de l'autorité de certification (cf. § 1.5.1).

2.2.2 Publication des certificats

Le Sujet ou le Demandeur, représentant légal de la personne morale, qui souhaite rendre public son certificat, peut en faire la demande en envoyant le formulaire approprié (disponible sur le site www.firma.infocert.it) à InfoCert, rempli et signé numériquement avec la clé correspondant au certificat dont la publication est demandée. L'envoi doit être effectué par courrier électronique adressé à richiesta.pubblicazione@cert.legalmail.it en suivant la procédure décrite sur le site en question. Cette option n'est pas disponible pour les certificats *LongTerm* et *OneShot*.

2.2.3 Publication des listes de révocation et de suspension

Les listes de révocation et de suspension sont publiées dans l'annuaire des certificats accessible par le protocole LDAP ou http à l'adresse indiquée dans l'attribut « CRL Distribution Points » du certificat. Cet accès peut se faire par le biais des logiciels mis à disposition par l'AC et/ou des fonctionnalités présentes dans les produits disponibles sur le marché qui interprètent le protocole LDAP et/ou HTTP.

L'AC peut proposer d'autres procédures que celle indiquée pour consulter la liste des certificats publiés et leur validité.

2.3 Période ou fréquence de publication

2.3.1 Fréquence de publication de la Politique de Certification

La Politique de Certification est publiée à une fréquence variable lorsque des changements surviennent. En cas de changements importants, l'AC doit se soumettre à un audit d'un OEC accrédité, présenter le rapport de certification (REC – Rapport d'Évaluation de la Conformité) ainsi que la Politique de Certification à l'Autorité de Contrôle (AgID) et attendre l'autorisation de publication.

2.3.2 Fréquence de publication des listes de révocation et de suspension

Les LCR sont publiées toutes les heures.

2.4 Contrôle de l'accès aux archives publiques

Les informations concernant les certificats publiés, les LCR et les Politiques de Certification publiés sont publiques. L'AC n'a pas imposé de restriction quant à l'accès à leur lecture et a mis en œuvre toutes les contre-mesures pour empêcher toute modification/suppression non autorisée.

3 IDENTIFICATION ET AUTHENTIFICATION

3.1 Dénomination

3.1.1 Types de noms

Le Sujet du certificat est identifié grâce à l'attribut *Distingued Name* (DN) qui, par conséquent, doit être valorisé et conforme à la norme X500. Les certificats sont délivrés conformément à la spécification RFC-5280 et aux normes ETSI EN 319 412 de 1 à 5 et conformément aux indications de l'avis de l'AgID n° 121/2019 [13]

3.1.2 Nécessité de donner une signification au nom

L'attribut du certificat Distinguished Name (DN) identifie de manière unique la personne à laquelle le certificat est délivré.

3.1.3 Anonymat et pseudonymat des demandeurs

Le Sujet peut demander à l'AC que le certificat contienne un pseudonyme au lieu de ses données réelles uniquement en cas d'identification selon la procédure 1_LiveID (cf. § 3.2.3.1). Cette option n'est pas disponible pour les certificats *LongTerm* et *OneShot*.

Étant donné que le certificat est qualifié, l'AC conservera les informations concernant l'identité réelle de la personne pendant vingt (20) ans après la délivrance du certificat en question.

3.1.4 Règles pour l'interprétation des types de noms

InfoCert suit la norme X500.

3.1.5 Unicité des noms

Lorsque le Sujet est une personne physique :
Afin de garantir l'unicité du Sujet, le certificat doit indiquer le nom et le prénom ainsi qu'un code d'identification unique
En général, c'est le numéro d'identification fiscale (NIF) qui est utilisé. Le NIF est attribué par les autorités du pays dont le Sujet est citoyen ou par le pays dans lequel est basée l'organisation dans laquelle il travaille. Pour les citoyens italiens, le code d'identification unique est le numéro d'identification fiscale.
En l'absence d'un numéro d'identification fiscale, le certificat pourra indiquer :

- un numéro d'identification extrait d'un document d'identité en cours de validité, utilisé dans la procédure de reconnaissance. Le format est conforme à la norme ETSI 319 412-1
- un identifiant univoque déterminé par l'AC. Dans ce cas, le format utilisé est l'UUID (Universal Unique Identifier) de type 4 décrit dans la RFC 4122.
- un identifiant unique tel que décrit dans l'*eIDAS eID profile* dans le cadre du réseau de coopération eIDAS. Le document de référence est « eIDAS SAML AttributeProfileVersion »

version 1.2. (https://ec.europa.eu/cefdigital/wiki/display/CEFDIGITAL/eIDAS+eID+Profile)

Toutefois, étant donné que le numéro d'identification fiscale est utilisé par toutes les administrations publiques italiennes comme identifiant du citoyen et du contribuable, le fait de ne pas l'indiquer dans le certificat de signature signifie qu'il n'est pas approprié pour l'administration publique italienne.

Lorsque le Sujet est une personne morale :
Dans le cas d'une personne morale, afin de garantir l'univocité du Sujet, le certificat doit indiquer le nom de l'organisation, ainsi qu'un code d'identification unique, au choix parmi :

- TVA (Numéro de TVA)
- RCS (Numéro du registre du commerce et des sociétés)

Dans le cas des personnes morales italiennes, utilisez le numéro de TVA ou le numéro de RCS. Si l'organisation n'a ni numéro de TVA ni numéro de RCS, mais seulement un numéro fiscal, vous pouvez utiliser les deux lettres « CF » suivies de « :IT- » (exemple : CF:IT- 97735020584), comme prévu dans l'avis AgID 121/2019 [13].
.

3.1.6 Reconnaissance, authentification et rôle des marques enregistrées

Lorsqu'ils demandent un certificat à l'AC, le Sujet et le Demandeur, garantissent qu'ils opèrent dans le plein respect des réglementations nationales et internationales sur la propriété intellectuelle.

L'AC ne contrôle pas l'utilisation des marques et peut refuser de générer ou peut demander de révoquer un certificat faisant l'objet d'un litige.

3.2 Validation initiale de l'identité

Ce chapitre décrit les procédures utilisées pour identifier le Sujet ou le Demandeur au moment de la demande de délivrance du certificat qualifié.

La procédure d'identification implique que le Sujet soit reconnu par l'AC, également par l'AE ou par l'un de ses opérateurs, qui vérifiera l'identité selon l'une des procédures définies dans la Politique de Certification.

3.2.1 Méthode pour prouver la possession de la clé privée

InfoCert établit que le demandeur possède ou contrôle la clé privée correspondant à la clé publique à certifier en vérifiant la signature de la demande de certificat à l'aide de la clé privée correspondant à la clé publique à certifier.

3.2.2 Authentification de l'identité des organisations

Cf. § 3.2.4

3.2.3 Identification de la personne physique

Sans préjudice de la responsabilité de l'AC, l'identité du Sujet peut être vérifiée par les entités autorisées à effectuer cette reconnaissance, selon les procédures suivantes, conformément à l'article 24 eIDAS :

Modalité	Entités habilitées à procéder à l'identification	Outils d'authentification mis en place dans la phase d'identification
1 LiveID	• Autorité de Certification (AC) • Autorité d'Enregistrement (AE) • Opérateur d'Enregistrement • Officier public • Employeur pour l'identification de ses salariés, collaborateurs, agents	Sans objet.
2 AMLID	• Entités soumises aux obligations de lutte contre le blanchiment de capitaux en vertu de la règlementation transposant la directive 2005/60/CE du Parlement européen et du Conseil relative à la prévention de l'utilisation du système financier aux fins du blanchiment de capitaux et du financement du terrorisme, et de la réglementation d'exécution européenne ultérieure	Sans objet.
3 SignID	• Autorité de Certification (AC) • Autorité d'Enregistrement (AE) • Opérateur d'Enregistrement	Utilisation d'une signature électronique qualifiée délivrée par un prestataire de services de confiance qualifié
4 AutID	• Autorité de Certification (AC) • Autorité d'Enregistrement (AE) • Opérateur d'Enregistrement	• Utilisation d'un moyen d'identification électronique préexistant
5 VidéoID	• Autorité de Certification (AC) • Autorité d'Enregistrement (AE) • Opérateur d'Enregistrement	Sans objet.

3.2.3.1 Reconnaissance effectuée selon la procédure 1 – LiveID

La procédure d'identification **LiveID** prévoit une rencontre en face à face entre le Sujet et l'une des entités autorisées à effectuer la reconnaissance.

Le Sujet présente au responsable de l'AC, spécialement formé à cet effet, l'original d'un ou plusieurs documents d'identification en cours de validité figurant dans la liste des documents acceptés publiée sur le site de l'AC[2].
Afin de garantir l'unicité du sujet et de son nom, celui-ci doit également être en possession du code d'identification unique visé au § 3.1.5. La personne autorisée à procéder à la reconnaissance peut demander à ce que soient montrés des documents prouvant la possession de cet identifiant unique.
Les Autorités d'Enregistrement opérant à l'étranger, ou dans tous les cas qui identifient des Sujets résidant à l'étranger, peuvent être autorisées par InfoCert à accepter des pièces d'identité délivrées par les autorités de pays appartenant à l'Union européenne figurant dans la liste des documents acceptés publiée sur le site de l'AC.
L'identification peut également être effectuée par un Officier public conformément à la réglementation régissant son activité. Le Sujet remplit la demande de certification et la signe devant un Officier public, en faisant authentifier sa signature conformément à la réglementation en vigueur. La demande est ensuite soumise à l'AC à l'une des Autorités d'Enregistrement agréées.
L'identification déjà effectuée par l'employeur, aux fins de la conclusion du contrat de travail, est considérée comme valable par l'AC selon la procédure de reconnaissance suivante (Employee_ ID), après vérification des procédures opérationnelles d'identification et d'authentification. De même, l'identification effectuée par l'employeur dans le cadre de l'activation des relations d'agence, après vérification des procédures opérationnelles d'identification et d'authentification, est considérée comme valable conformément à la procédure de reconnaissance suivante.
Cette procédure d'identification exige que l'AC accorde un mandat de représentation à l'employeur, qui agit alors en tant qu'AE[3]. Les certificats délivrés selon cette procédure d'identification ne peuvent être utilisés qu'aux fins professionnelles pour lesquelles ils ont été délivrés et contiennent une limite d'utilisation spécifique.
Les données d'enregistrement pour la procédure d'identification LiveID sont conservées par l'AC sous format analogique ou électronique.

3.2.3.2 Reconnaissance effectuée selon la procédure 2 – AMLID

Dans la procédure 2 – AMLID, l'AC s'appuie sur l'identification effectuée par l'une des entités soumises aux obligations de lutte contre le blanchiment de capitaux en vertu de la règlementation en vigueur du moment, transposant la directive 2005/60/CE du Parlement européen et du Conseil relative à la prévention de l'utilisation du système financier aux fins du blanchiment de capitaux et du financement du terrorisme, et de la législation européenne d'application ultérieure.
En ce qui concerne plus particulièrement le contexte italien, les données utilisées pour la reconnaissance sont délivrées par le Sujet conformément au Décret législatif italien n° 231/2007 tel que modifié et complété, en vertu duquel les clients sont tenus de fournir – sous leur propre responsabilité – toutes les informations nécessaires et actualisées pour permettre aux entités soumises aux obligations de remplir leurs obligations d'identification des clients.

[2] La liste des pièces d'identité acceptées est établie par l'AC après analyse des pièces d'identité en question et des caractéristiques objectives qu'elles présentent quant à la certitude de l'identité et à la sécurité dans le processus de délivrance par les Autorités de Délivrance. La liste est notifiée à l'AgID et mise à jour à chaque modification.

[3] Avant l'attribution du mandat, l'AC procède à une évaluation minutieuse de la sécurité des procédures d'identification du salarié et de la manière d'attribuer et de gérer les outils d'identification personnelle par l'intermédiaire de systèmes informatiques auxquels le salarié (ou l'agent, ou le salarié retraité) accède afin de demander un certificat de signature numérique à l'AC. Ces cas seront communiqués à l'Autorité de Contrôle.

Cette procédure d'identification exige que l'AC accorde un mandat de représentation à l'entité soumise aux obligations, qui agit alors en tant qu'AE. Les données d'identification du Sujet collectées au moment de la reconnaissance sont conservées par l'AC, généralement sous forme électronique, mais elles peuvent également être conservées sous forme analogique.

3.2.3.3 Reconnaissance effectuée selon la procédure 3 – SignID

Dans la **procédure 3 SignID** , l'AC InfoCert est basée sur la reconnaissance déjà effectuée par une AC délivrant des certificats qualifiés (QPSC)**.** Le Sujet est déjà en possession d'un certificat qualifié encore en cours de validité, qu'il utilise à l'égard d'InfoCert. Dans ce cas, les données d'enregistrement sont conservées exclusivement sous forme électronique.

3.2.3.4 Reconnaissance effectuée selon la procédure 4 – AUTID

Dans la **procédure 4 AutID**, l'AC se base sur un moyen d'identification électronique préexistant :

- notifié par l'État membre, offrant un niveau de garantie *élevé,* conformément à l'article 9 du règlement eIDAS ;
- notifié par l'État membre, offrant un niveau de garantie *substantiel,* conformément à l'article 9 du règlement eIDAS, à condition qu'il fournisse une assurance équivalente en termes de fiabilité à la présence physique ;
- non notifié et délivré par une autorité publique ou une entité privée, à condition qu'il fournisse une garantie équivalente à la présence physique en termes de fiabilité, et que celle-ci soit confirmée par un organisme d'évaluation de la conformité.

En ce qui concerne plus particulièrement le contexte italien, les moyens d'identification électronique sont la CNS (*Carta Nazionale dei Servizi*), ou la TS-CNS (*Tessera Sanitaria – Carta Nazionale dei Servizi*), la CIE (Carte d'Identité Électronique), le titre de séjour électronique et les identités délivrées dans le cadre du système public d'identité numérique SPID.

Les moyens d'identification électroniques utilisables par l'AC et l'AE sont énumérés dans la liste publiée sur le site de l'AC et notifiée à l'AgID.
InfoCert évaluera la possibilité se s'appuyer sur des identifications effectuées par des personnes en possession d'une certification délivrée par un OEC qui atteste que la méthode d'identification utilisée est conforme à l'article 24 lettre d) eIDAS.

3.2.3.5 Reconnaissance effectuée selon la procédure 5 – VideoID

Dans la **procédure 5 VideoID**, le Sujet doit disposer d'un dispositif qui peut être connecté à internet (PC, smartphone, tablette, etc.), d'une webcam et d'un système audio en bon état de fonctionnement.
L'Opérateur d'Enregistrement, dûment formé, vérifie l'identité du Sujet ou du Demandeur en vérifiant l'existence d'une ou plusieurs pièces d'identité en cours de validité, avec une photographie récente et reconnaissable et figurant dans la liste des documents acceptés publiée sur le[4]site de l'AC.

[4] La liste des pièces d'identité acceptées est établie par l'AC après analyse des pièces d'identité en question et des caractéristiques objectives qu'elles présentent quant à la certitude de l'identité et à la sécurité dans le processus de délivrance par les Autorités de Délivrance. La liste est notifiée à l'AgID et mise à jour à chaque modification. Pour des raisons de sécurité et de procédures anti-fraude, le type de documents acceptés par cette procédure se limite aux pièces d'identité les plus courantes.

Les Autorités d'Enregistrement opérant à l'étranger, ou dans tous les cas qui identifient des Sujets résidant à l'étranger, peuvent être autorisées par InfoCert à accepter des pièces d'identité délivrées par les autorités de pays appartenant à l'Union européenne, après analyse des pièces d'identité en question et des caractéristiques objectives qu'elles présentent quant à la certitude de l'identité et à la sécurité dans le processus de délivrance par les Autorités de délivrance, et après formation spécifique[5].
L'Opérateur d'Enregistrement a le droit de refuser la pièce d'identité utilisée par le Sujet ou le Demandeur en la déclarant irrecevable s'il considère qu'elle ne présente pas les caractéristiques énumérées. Les données d'enregistrement, constituées de fichiers audio-vidéo et de métadonnées structurées sous format électronique, sont conservées sous une forme protégée.

3.2.4 Identification de la personne morale

La demande de certificat pour une personne morale doit être faite par une personne physique identifiée selon l'une des procédures décrites ci-dessus (cf. § 3.2.3).
Elle doit également présenter les documents concernant la personne morale et ceux prouvant son habilitation à effectuer la demande au nom de la personne morale.

La personne morale peut être un prestataire de services de paiement (PSP) soumis à la directive DSP2.

3.2.5 Informations non vérifiées du Sujet ou du Demandeur

Le Sujet peut obtenir, directement ou, le cas échéant, avec le consentement du Tiers Concerné, l'inscription dans le certificat d'informations concernant :

- Titres et/ou habilitation professionnelles ;
- Pouvoirs de représentation de personnes physiques ;
- Pouvoirs de représentation de personnes morales ou d'appartenance à celles-ci ;
- Exercice de fonctions publiques, pouvoirs de représentation d'organisations et d'organismes de droit public ou d'appartenance à ceux-ci.

Le certificat avec le **Rôle** est conforme à l'avis AgID n° 121/2019 [13].

Le Sujet doit fournir la déclaration apte à démontrer l'existence réelle du Rôle spécifique également en en fournissant la preuve par le biais d'une autocertification[6]. L'AC n'assume aucune responsabilité, sauf en cas de dol ou de négligence, eu égard à l'inscription dans le certificat d'informations autocertifiées par le Sujet.

La dénomination ou la raison sociale et le code d'identification de l'**Organisation** seront plutôt inclus dans le certificat si celle-ci a autorisé la délivrance du certificat au Sujet, même sans l'indication explicite d'un rôle. Dans ce cas, l'AC effectue un contrôle de la régularité formelle des documents présentés par le Sujet. La demande de certificats indiquant le rôle et/ou l'organisation ne peut provenir que d'organisations ayant une forme juridique définie.

[5] Ces cas seront communiqués à l'Autorité de Contrôle.

[6] Si le Sujet a uniquement fait la demande d'inscription du rôle dans le certificat au moyen d'une autocertification, le certificat ne contiendra pas d'informations relatives à l'organisation à laquelle le rôle pourrait éventuellement être lié.

3.2.6 Validation de l'autorité

L'AC ou l'AE vérifie les informations demandées définies aux § 3.2.3, 3.2.4 et 325, pour identification et validation de la demande.
Lorsque cela est prévu ou nécessaire, l'AC ou l'AE peut utiliser des bases de données publiques pour valider les informations fournies par le Demandeur.

Dans le cas d'une demande QSealC DSP2 , l'AC ou l'AE vérifie les attributs spécifiques fournis par le Demandeur (numéro d'autorisation, nom et état de l'ANC, rôle du PSP) en utilisant les informations authentiques mises à disposition par l'ABE dans son registre central ou, le cas échéant, dans les registres mis à disposition par les ANC de chaque État membre.

Si l'ANC nationale a prévu des règles pour la validation de ces attributs, le PSC applique les règles indiquées.

3.3 Identification et authentification pour le renouvellement des clés et des certificats

3.3.1 Identification et authentification pour le renouvellement des clés et des certificats

Ce paragraphe décrit les procédures utilisées pour l'authentification et l'identification du Sujet en cas de renouvellement du certificat qualifié de signature électronique.

Le certificat contient une indication de la période de validité dans le champ « validity » (validité) avec les attributs « not before » (date de début de validité du certificat) et « not after » (date de fin de validité du certificat). En dehors de cette plage de dates, y compris les heures, les minutes et les secondes, le certificat est considéré comme non valable.

Le Sujet peut toutefois le renouveler avant son expiration, en utilisant les instruments proposés par l'AC, en présentant une demande de renouvellement qui est signée avec la clé privée correspondant à la clé publique contenue dans le certificat à renouveler. Après la révocation ou l'expiration du certificat, il n'est plus possible de le renouveler. Il doit alors être nouvellement émis.

3.4 Identification et authentification pour les demandes de révocation ou de suspension

La révocation ou la suspension du certificat peut se faire sur demande authentifiée du Sujet ou du Demandeur (Tiers Concerné dans le cas où ce dernier a exprimé son consentement à l'inscription du Rôle) ou à l'initiative de l'AC.

3.4.1 Demande de la part du Sujet

Le Sujet peut demander la révocation ou la suspension du certificat en remplissant et en signant numériquement le formulaire qui se trouve sur le site de l'AC (cf. § 4.9).

La demande de suspension peut être faite par le biais d'un formulaire internet. Dans ce cas, le Sujet est authentifié en fournissant le code d'urgence délivré au moment de la délivrance du certificat, ou par un autre système d'authentification décrit dans la documentation contractuelle

délivrée au moment de l'enregistrement.

Le Sujet en possession d'une signature à distance peut également demander la révocation du certificat en utilisant son espace réservé auquel il accède par un système d'authentification à deux facteurs (§ 4.2.2)

Si la demande est faite à l'Autorité d'Enregistrement, le Sujet est authentifié selon les procédures prévues pour l'identification.

Si le Sujet est une personne morale, la demande de suspension ou de révocation doit être effectuée par un représentant légal ou une personne ayant une procuration spécifique.

3.4.2 Demande de la part du Demandeur

Le Demandeur ou un Tiers Concerné demandant la révocation ou la suspension du certificat du Sujet est authentifié en signant le formulaire de demande de révocation ou de suspension spécifique fourni par l'AC. La demande doit être faite selon les procédures indiquées au § **Errore. L 'origine riferimento non è stata trovata.** ou 4.9.15.2. L'AC se réserve le droit de définir d'autres moyens de transmission de la demande de révocation ou de suspension du Demandeur dans des conventions spécifiques à conclure avec celui-ci.

4 FONCTIONNEMENT

4.1 Demande de certificat

4.1.1 Qui peut demander un certificat

Le certificat qualifié pour une personne physique peut être demandé par :

- le Sujet
  - en s'adressant directement à l'AC sur le site www.firma.infocert.it, ou
  - en s'adressant à une Autorité d'Enregistrement
- le Demandeur pour le compte du Sujet
  - en s'adressant directement à l'AC sur le site www.firma.infocert.it ou en concluant un accord commercial avec l'AC
  - en s'adressant à une Autorité d'Enregistrement
  - en signant le mandat avec représentation avec l'AC et en devenant une Autorité d'Enregistrement au sein d'un domaine informatique.

Le certificat qualifié pour une personne morale peut être demandé par :

- le Demandeur représentant la personne morale
  - en s'adressant directement à l'AC sur le site www.firma.infocert.it ou en concluant un accord commercial avec l'AC
  - en s'adressant à des Autorités d'Enregistrement spécialement formées pour délivrer des certificats de ce type.

4.1.2 Processus d'enregistrement et responsabilité

Le processus d'enregistrement comprend : la demande de la part du Sujet, la génération de la bi-clé, la demande de certification de la clé publique et la signature des contrats, pas nécessairement dans cet ordre.

Dans ce processus, les différents acteurs ont des responsabilités différentes et contribuent conjointement à ce que la délivrance du certificat soit menée à bien :

- le Sujet a la responsabilité de fournir des informations correctes et véridiques sur son identité, de lire attentivement les documents mis à sa disposition par l'AC, également par l'intermédiaire de l'AE, mais aussi de suivre les instructions de l'AC et/ou de l'AE lorsqu'il fait la demande du certificat qualifié. Lorsque le Sujet est une personne morale, ces responsabilités incombent au représentant légal ou à la personne disposant de la procuration spécifique, qui demande le certificat qualifié ;
- le Demandeur, le cas échéant, a la responsabilité d'informer le Sujet pour le compte duquel il fait la demande de certificat des obligations découlant du certificat, de fournir des informations correctes et véridiques sur l'identité de la personne, de suivre les procédures et les indications de l'AC et/ou de l'AE ;
- l'Autorité d'Enregistrement, le cas échéant, et également par l'intermédiaire de

l'Opérateur d'Enregistrement, est chargée d'identifier avec certitude le Sujet et le Demandeur, d'informer les différentes entités/personnes sur les obligations découlant du certificat et de suivre en détail les processus définis par l'AC ;
- l'Autorité de Certification est responsable en dernier ressort de l'identification du Sujet et de l'aboutissement du processus d'enregistrement du certificat qualifié.

Si le Sujet est une personne morale, lorsque les clés sont générées dans un dispositif du Sujet, le Demandeur doit également envoyer la demande en format PKCS#10 signée par le Demandeur lui-même.

4.2 Traitement de la demande

Pour obtenir un certificat de signature électronique, le Sujet et/ou le Demandeur doivent :
- prendre connaissance de la documentation contractuelle et tout autre document d'information ;
- suivre les procédures d'identification adoptées par l'Autorité de Certification, telles que décrites au point 3.2.3 ;
- fournir toutes les informations nécessaires pour l'identification, accompagnées, le cas échéant, des documents appropriés ;
- signer la demande d'enregistrement et de certification en acceptant les conditions contractuelles qui régissent la prestation de services, sur les formulaires analogiques ou électroniques mis à disposition par l'AC.

4.2.1 Informations que le Sujet doit fournir

4.2.1.1 Personne physique

Pour la demande d'un certificat qualifié de signature électronique, le Sujet ou le Demandeur qui demande le certificat de la personne physique doit fournir les informations suivantes :
- Prénom et nom de famille ;
- Date et lieu de naissance ;
- NIF (numéro d'identification fiscale dans le contexte italien) ou, à défaut, code d'identification similaire tel que le numéro du document d'identité. Dans les cas où la réglementation applicable du pays en matière de confidentialité ne permet pas l'utilisation publique de ces informations, InfoCert ne les inscrira pas dans le certificat.
- Références du document d'identification présenté pour l'identification, tels que son type, son numéro, l'entité émettrice et la date de délivrance ;
- Au moins une information de contact pour l'envoi de communications de l'AC au Sujet, au choix entre
  - Adresse de résidence
  - Adresse e-mail ;
- Numéro de téléphone portable pour la transmission de l'OTP s'il s'agit de la technologie OTP adoptée.

En alternative, le Sujet (ou le Demandeur) peut fournir un autre nom, sous lequel il est communément connu, qui sera inscrit dans un champ spécial appelé commonName (nom commun) du SubjectDN du certificat. Dans le cas où aucun autre nom n'est fourni par le Sujet ou

le Demandeur, c'est le nom et le prénom du sujet qui seront insérés dans le champ commonName.

4.2.1.2 Personne morale

En ce qui concerne la demande de certificat qualifié pour une personne morale, le Demandeur identifié comme étant le représentant légal ou la personne physique ayant procuration, doit fournir les informations suivantes :

- Nom et prénom du Demandeur ;
- Code NIF ou code d'identification similaire du Demandeur (numéro d'identification fiscale dans le contexte italien) ;
- Références du document d'identification présenté pour l'identification du Demandeur, tels que son type, son numéro, l'entité émettrice et la date de délivrance ;
- E-mail pour envoyer des communications de l'AC au Demandeur ;
- Nom du Sujet personne morale ;
- N° TVA ou RCS (numéro de TVA ou numéro du registre du commerce et des sociétés pour les Sujets italiens).

Au cas où la personne morale souhaite certifier ses bi-clés, le Demandeur doit également fournir le fichier au format PKCS#10 de la demande signée par le Demandeur.
Les informations fournies sont stockées dans les archives de l'AC (phase d'enregistrement) et serviront de base à la génération du certificat qualifié.

Dans le cas d'une demande de QSealC DSP2, la personne (PSP), identifiée comme étant le représentant légal ou la personne physique ayant procuration, **doit fournir les informations supplémentaires suivantes** :

- numéro d'autorisation qui identifie de manière unique le prestataire de services de paiement (PSP) ;
- rôle(s) du prestataire de services de paiement (PSP) ;
- nom et état de l'autorité nationale compétente (ANC) qui a autorisé le prestataire de services de paiement (PSP) et a délivré le numéro d'autorisation.

4.2.2 Exécution des fonctions d'identification et d'authentification

Lors de l'enregistrement initial et de la collecte de la demande d'enregistrement et de certification, le Sujet ou le Demandeur, représentant légal de la personne morale, reçoit les codes de sécurité qui lui permettent de procéder à la fois à l'activation du dispositif de signature ou de la procédure de signature, s'il s'agit d'une signature à distance, et/ou à la demande éventuelle de suspension du certificat (code d'urgence ERC ou code similaire, s'il est prévu dans le contrat). Ces codes de sécurité sont livrés sous pli fermé ou, s'il s'agit de codes électroniques, transmis dans des fichiers cryptés.
L'AC peut prévoir que le Sujet ou le Demandeur représentant légal de la personne morale choisisse lui-même le code PIN de signature ; dans ce cas, il est de la responsabilité du Sujet ou du Demandeur de se souvenir de son code PIN.
L'AC peut également prévoir que le certificat de signature pour la procédure à distance puisse être utilisé par le biais d'un système d'authentification fourni par l'AE, offrant un niveau de sécurité au

moins substantiel ou élevé après avoir vérifié les caractéristiques du système en question, dans le cadre de la certification du dispositif de signature sécurisé. Dans ces cas, le système d'authentification peut également être utilisé pour toute demande de suspension et de révocation du certificat.

4.2.3 Approbation ou rejet de la demande de certificat

Après l'enregistrement initial, l'AC ou l'AE peut refuser de délivrer le certificat de signature en cas d'informations manquantes ou incomplètes, de contrôles de la cohérence et de la consistance des informations fournies, de contrôles à des fins de lutte anti-fraude, de doutes sur l'identité du Sujet ou du Demandeur, etc.

4.2.4 Délai maximum de traitement de la demande de certificat

Le délai entre la demande d'enregistrement et la délivrance du certificat dépend de la modalité de demande choisie par le Sujet (ou le Demandeur) et de l'éventuelle nécessité de collecter des informations supplémentaires ou de livrer physiquement le dispositif.

4.3 Délivrance du certificat

4.3.1 Actions de l'AC lors de la délivrance du certificat

4.3.1.1 Délivrance du certificat sur un dispositif de signature (carte à puce ou jeton numérique)

La bi-clé cryptographique est générée par l'AC directement sur les dispositifs de signature sécurisés, en utilisant les applications mises à disposition par l'AC, après authentification sécurisée.

L'AE envoie la demande de certification de la clé publique au format PKCS#10 à l'Autorité de Certification, demande signée numériquement avec le certificat de signature qualifié spécifiquement autorisé à cet effet.

Après avoir vérifié la validité de la signature sur le PKCS#10 et si la personne qui présente la demande en a le titre, l'Autorité de Certification génère le certificat qualifié, qui est envoyé sur un canal sécurisé à l'intérieur du dispositif.

4.3.1.2 Délivrance du certificat sur un dispositif de signature à distance (HSM)

Le Sujet ou le Demandeur doit s'authentifier auprès des services ou des applications mis à disposition par l'AE.

La bi-clé cryptographique est générée par l'AE directement sur le module de sécurité matériel (HSM). Ensuite, l'AE envoie la demande de certification de la clé publique au format PKCS#10 à l'Autorité de Certification, demande qui est signée numériquement avec le certificat de signature qualifié pour procédure automatique spécifiquement autorisée à cette fin.

Après avoir vérifié la validité de la signature sur le PKCS#10 et si la personne qui présente la demande en a le titre, l'Autorité de Certification génère le certificat qualifié, qui est stocké sur le module de sécurité matériel (HSM).

4.3.1.3 Délivrance du certificat par un système de gestion de cartes (CMS)

La bi-clé cryptographique est générée par l'AE directement sur les dispositifs à l'aide d'un système de gestion de cartes authentifié. Le système gère le cycle de vie complet du dispositif cryptographique, en envoyant à l'Autorité de Certification la demande de certification de la clé publique au format PKCS#10 à travers un canal sécurisé authentifié.

Après avoir vérifié la validité de la signature sur le PKCS#10 et si la personne qui présente la demande en a le titre, l'Autorité de Certification génère le certificat qualifié, qui est envoyé sur un canal sécurisé à l'intérieur du dispositif.

4.3.1.4 Délivrance du certificat à une personne morale

La bi-clé cryptographique est générée par l'AE directement sur le module de sécurité matériel (HSM). Ensuite, l'AE envoie la demande de certification de la clé publique au format PKCS#10 à l'Autorité de Certification, demande qui est signée numériquement avec le certificat de signature qualifié pour procédure automatique spécifiquement autorisée à cette fin.

Après avoir vérifié la validité de la signature sur le PKCS#10 et si la personne qui présente la demande en a le titre, l'Autorité de Certification génère le certificat qualifié, qui est stocké sur le module de sécurité matériel (HSM).

Dans le cas où la bi-clé est générée dans le dispositif HSM du Sujet, celui-ci doit envoyer le PKCS#10 signé et après avoir vérifié la validité de la signature sur le PKCS#10 et si la personne qui présente la demande en a le titre, l'Autorité de Certification génère le certificat qualifié, qui est stocké sur le module de sécurité matériel (HSM) en question.

4.3.1.5 Délivrance d'un certificat à des fins de test

Il est parfois nécessaire d'utiliser des certificats pour effectuer certains tests en cours de production.
Dans ce cas, les données doivent être enregistrées avant la délivrance du certificat. Cet enregistrement doit être approuvé par le responsable de l'AC.
Dans les cas prévus, l'Autorité d'Enregistrement doit être la même que celle utilisé par InfoCert pour les délivrances internes, ou celle utilisée par la procédure du Client faisant l'objet d'une session de test.
Les données utilisées pour l'enregistrement doivent indiquer clairement dans l'objet qu'il s'agit d'un certificat de test et non d'un certificat réel.
Cette procédure ne peut pas être utilisée pour les tests de perfomance ou les tests cycliques sur les enregistrements et les délivrances.
Dès lors que le certificat n'est plus nécessaire, par exemple à la fin d'une session d'essais spécifique, il doit être automatiquement révoqué.

4.3.2 Notification aux demandeurs que le certificat a été délivré

En cas de délivrance sur un dispositif cryptographique, le Sujet (ou le Demandeur) n'a pas besoin de recevoir une notification l'en avisant car le certificat est présent dans le dispositif qu'il a reçu.
Dans le cas des certificats LongTerm et OneShot, l'AC notifie au Demandeur par une procédure automatisée que le certificat du Sujet a été délivré. Le Demandeur informe le Sujet selon les formes et les modalités prévues dans le contrat.

Dans les autres cas, le Sujet recevra la notification par courriel, à l'adresse e-mail qu'il a indiquée lors de l'inscription. Ces informations peuvent également être partagées avec le Demandeur.

4.3.3 Activation

4.3.3.1 Activation du dispositif de signature (carte à puce ou jeton numérique)

Après avoir reçu le dispositif, le Sujet utilise les codes d'activation reçus de manière confidentielle et le logiciel spécifique que l'AC met à disposition pour activer le dispositif en sélectionnant simultanément le code PIN de signature, qui est un code de sécurité confidentiel dont la conservation et la protection relèvent de la responsabilité exclusive du Sujet.

4.3.3.2 Activation du dispositif de signature à distance (HSM)

Le Sujet, ou le Demandeur dans le cas d'une personne morale, authentifié sur les portails de l'AC grâce aux codes d'activation reçus de manière confidentielle, sélectionne le code PIN de signature, qui est un code de sécurité confidentiel dont la conservation et la protection relèvent de la responsabilité exclusive du Sujet. Le code PIN est ensuite confirmé en saisissant le mot de passe à usage unique reçu par SMS, ou généré sur le jeton numérique ou appli jeton numérique associée au certificat.
Dans certains cas, le certificat peut déjà être actif et utilisable lorsqu'il est délivré.

4.4 Acceptation du certificat

4.4.1 Comportements constituant une acceptation du certificat

Sans objet.

4.4.2 Publication du certificat de la part de l'Autorité de Certification

Une fois que la procédure de certification aura été menée à bien, le certificat sera inscrit dans l'annuaire de référence des certificats et ne sera pas rendu public. Un Sujet qui souhaite rendre son certificat public peut en faire la demande en suivant la procédure décrite au § 2.2.2. La demande sera traitée dans un délai de trois jours ouvrés. Cette option n'est pas disponible pour les certificats *LongTerm* et *OneShot*.

4.4.3 Notification à d'autres personnes que le certificat a été délivré

Sans objet.

4.5 Utilisation de la bi-clé et du certificat

4.5.1 Utilisation de la clé privée et du certificat de la part du Sujet

Le Sujet doit conserver de manière sécurisée le dispositif de signature, s'il existe, ou les outils d'authentification pour la signature à distance. Il doit conserver les informations permettant l'utilisation de la clé privée séparément du dispositif, s'il existe, ou des outils ou des codes d'authentification. Il doit veiller à protéger la confidentialité du code d'urgence nécessaire à la suspension du certificat, le cas échéant, et garantir sa conservation. Il doit utiliser le certificat uniquement pour les procédures prévues par la Politique de Certification et par les lois nationales et internationales en vigueur. De plus, il doit utiliser le certificat LongTerm et OneShot dans le cadre du domaine informatique défini dans le contrat.
Il ne doit pas apposer de signatures électroniques en utilisant des clés privées pour lesquelles le certificat a été révoqué ou suspendu et ne doit pas apposer de signatures électroniques en utilisant un certificat émis par une AC révoquée.

4.5.2 Utilisation de la clé publique et du certificat par l'utilisateur final

L'utilisateur final doit connaître le champ d'application du certificat figurant dans la Politique de Certification et dans le certificat en question. Il doit vérifier la validité du certificat avant d'utiliser la clé publique qu'il contient et que le certificat n'est ni suspendu ni révoqué en contrôlant les listes correspondantes dans l'annuaire des certificats. Il doit également vérifier l'existence et le contenu de toute limite à l'utilisation de la bi-clé, des pouvoirs de représentation et des habilitations professionnelles.

4.5.3 Limites d'utilisation et de valeur

Les certificats de signature qualifiés pour procédure automatique contiennent la limite d'utilisation prévue par l'Autorité de Contrôle, sous forme de politiques de certification supplémentaires, identifiées par les OID suivants :

1.3.76.36.1.1.24.1	**Ce certificat n'est valable que pour les signatures apposées par procédure automatique. La présente déclaration constitue la preuve de l'adoption de cette procédure pour les documents signés.**
1.3.76.36.1.1.24.2	The certificate may be used only for automatic procedure signature purposes
1.3.76.36.1.1.23	Le propriétaire du certificat doit utiliser ce dernier uniquement aux fins pour lesquelles il a été délivré. The certificate holder must use the certificate only for the purposes for which it is issued.

1.3.76.36.1.1.25	« L'utilisation du certificat est limitée aux relations avec » suivi du nom de la personne avec laquelle le certificat peut être utilisé. "The certificate may be used only for relations with the" followed by the name of the subject with which the certificate can be used

Les certificats délivrés sur la base d'une identification de type 4-AutID, utilisant des identités numériques SPID, contiennent l'OID 1.3.76.16.5 et la limite d'utilisation suivante :

> "*Certificate issued through Sistema Pubblico di Identità Digitale (SPID) digital identity, not usable to require other SPID digital identity*" (Certificat délivré à travers l'identité numérique du système public d'identité numérique italien – SPID – non utilisable pour demander une autre identité numérique SPID)

Cette limite est conforme à l'avis n° 17 du 24 janvier 2019

Le Sujet ou le Demandeur a également le droit de demander à l'Autorité de Certification d'inclure dans le certificat des limites d'utilisation personnalisées (200 caractères maximum). La demande d'inclure d'autres limites d'utilisation spécifiques sera évaluée par l'AC sur la base des aspects juridiques, techniques et d'interopérabilité et sera valorisée en conséquence.

Limites d'utilisation pour les certificats à LongTerm et OneShot

Les certificats de type LongTerm peuvent être limités exclusivement à une utilisation dans le domaine informatique spécifié dans le contrat, pour la signature des documents informatiques mis à la disposition du Sujet par l'AC ou par le Demandeur. Dans ce cas, les documents informatiques peuvent être liés à la relation entre le Demandeur et le Sujet, ou il peut s'agir de documents de tiers.

Le certificat LongTerm contient donc l'une des limites d'utilisation suivantes :

- Le certificat ne peut être utilisé que dans les relations entre le propriétaire et le demandeur. *The certificate can be used only in the relationships between the holder and the requestor* (max 200 caractères).
- Certificat de signature pour des produits et services mis à disposition par [Nom du Sujet]. Certificate to subscribe product and services made available by [Nom du Sujet] (max 200 caractères).

Le certificat OneShot contient la limite d'utilisation suivante :

- L'utilisation du certificat est techniquement limitée à la signature des documents sur lesquels la signature est apposée. The use of the certificate is technically limited to the signature of the underlying documents.

Sans préjudice de la responsabilité de l'AC visée dans le Code d'administration numérique – DAC – (article 30), il appartient à l'utilisateur de vérifier que sont respectées les limites d'utilisation et de valeur figurant dans le certificat. L'AC n'est donc pas responsable des dommages résultant de l'utilisation d'un certificat qualifié qui dépasse les limites fixées par le certificat ou du dépassement de la valeur limite.

4.6 Renouvellement du certificat

4.6.1 Raisons du renouvellement

Le renouvellement permet d'obtenir un nouveau certificat de signature à utiliser pour signer des documents et des transactions. Pour les certificats de signature automatique, LongTerm, OneShot et les certificats délivrés à une personne morale, aucun renouvellement n'est prévu ; on procède uniquement à une nouvelle reconnaissance et à une nouvelle délivrance.

4.6.2 Qui peut demander le renouvellement

Le Sujet peut demander le renouvellement du certificat avant sa date d'expiration uniquement s'il n'a pas été révoqué et si toutes les informations fournies lors de la précédente délivrance sont toujours valables. Après la date d'expiration, aucun renouvellement ne sera possible ; un nouveau certificat devra alors être demandé.
La procédure de renouvellement s'applique exclusivement aux certificats délivrés par InfoCert.

4.6.3 Traitement de la demande de renouvellement du certificat

Le renouvellement s'effectue à travers un service fourni par l'AC, dans le cadre des relations commerciales et contractuelles définies avec le sujet et avec l'AE, le cas échéant.

4.7 Nouvelle délivrance du certificat

Sans objet.

4.8 Modification du certificat

Sans objet.

4.9 Révocation et suspension du certificat

La révocation ou la suspension d'un certificat rend celui-ci invalide avant sa date d'expiration et invalide toute signature apposée après la publication de la révocation. Les certificats révoqués ou suspendus sont insérés dans une Liste des Certificats Révoqués et Suspendus (LCR) signée par l'AC émettrice qui les a délivrés. Cette liste est publiée dans l'annuaire des certificats à intervalles précis. L'AC peut forcer une publication non programmée de la LCR dans des circonstances particulières. La révocation et la suspension prennent effet à partir du moment de la publication de la liste ; c'est alors la date d'enregistrement de l'événement dans les journaux d'évènements de l'autorité de certification qui fait foi.

4.9.1 Raisons de la révocation

Les conditions selon lesquelles la demande de révocation doit être faite sont les suivantes :

1. la clé privée a été compromise, ou dans l'un des cas suivants :
   - le dispositif de signature sécurisé contenant la clé a été perdu ;
   - la clé ou son code d'activation (PIN) ne sont plus tenus secrets ou, pour les

certificats de signature à distance, le dispositif OTP a été compromis ou perdu ;
- un événement quel qu'il soit a compromis le niveau de fiabilité de la clé.

2. le Sujet n'est plus en mesure d'utiliser le dispositif de signature sécurisé en sa possession, par exemple en raison d'une panne ;
3. les données du Sujet figurant dans le certificat ont changé, y compris celles concernant le Rôle, de sorte que ces données ne sont plus correctes et/ou véridiques ;
4. la relation entre le Sujet et l'AC, ou entre le Demandeur et l'AC, prend fin ;
5. une condition substantielle de non-respect de la présente Politique de Certification est vérifiée.

4.9.2 Qui peut demander la révocation ?

La révocation du certificat peut être demandée :

- par le Sujet, propriétaire du certificat ;
- par le Demandeur ou un Tiers Concerné ;
- d'office par l'AC ;
- par l'ANC, en cas de demande de révocation du QSealC DSP2.

4.9.3 Procédures de demande de révocation

Ci-dessous sont indiquées les procédures par lesquelles les personnes ayant droit à la révocation peuvent la demander.

Demande de la part du sujet : la demande de révocation peut être faite en signant un formulaire qui se trouve sur le site d'InfoCert. Le formulaire mentionné ci-dessus peut être remis à l'AE ou envoyé directement à l'AC par courrier recommandé, courrier électronique certifié ou fax, accompagné d'une photocopie d'une pièce d'identité en cours de validité. En outre, l'AC ou l'AE peut proposer d'autres procédures pour transmettre la demande de révocation, à condition que celles-ci permettent d'identifier correctement la personne. L'AC ou l'AE doit le communiquer au Sujet de façon adéquate.

L'AC ou l'AE vérifie l'authenticité de la demande avant de procéder à la révocation du certificat, en le notifiant immédiatement au Sujet, et le cas échéant, au Demandeur.

Si le certificat faisant l'objet de la demande de révocation contient des informations concernant le Rôle du Sujet, l'AC communiquera la révocation au Tiers Concerné avec lequel les conventions spécifiques sont mises en œuvre. Si le certificat qui fait l'objet de la demande de révocation fait référence à l'Organisation, l'AC informera cette dernière de la révocation. Pour la demande de révocation de la part du Sujet, d'autres procédures peuvent être spécifiées dans les accords qui pourraient être conclus entre le Sujet et l'AC

En cas de demande de révocation pour des certificats LongTerm et OneShot, le Sujet peut demander la révocation du certificat en s'authentifiant auprès des systèmes fournis par l'AE et/ou l'AC, également par le biais de services applicatifs, en suivant les procédures décrites dans la documentation contractuelle.

Demande de la part du Demandeur ou d'un Tiers Concerné : il peut demander la révocation du certificat du Sujet selon les mêmes procédures que celles selon lesquelles le Sujet peut la demander. Il doit également indiquer les données du Sujet du certificat communiquées à l'AC au moment de la délivrance du certificat.

L'AC ou l'AE vérifie l'authenticité de la demande afin que l'AC puisse procéder à la révocation du certificat. Immédiatement après, elle le notifie au Sujet en utilisant les moyens de communication établis au moment de la demande du certificat. Pour la demande de révocation de la part du Sujet, d'autres procédures peuvent être spécifiées dans les accords qui pourraient être conclus entre le Sujet et l'AC ou l'AE.

En cas de demande de révocation pour des certificats LongTerm et OneShot, le Demandeur peut demander la révocation du certificat en s'authentifiant auprès des systèmes proposés par l'AC, également par le biais de services applicatifs, en suivant les procédures décrites dans la documentation contractuelle.

Révocation d'office par l'AC/AE : si nécessaire, l'AC peut révoquer le certificat, en informant la personne au préalable, en indiquant la raison de la révocation ainsi que la date et l'heure de prise d'effet de cette révocation.

Si le certificat faisant l'objet de la révocation contient des informations concernant le Rôle du Sujet, l'AC/AE communiquera la révocation au Tiers Concerné avec lequel les conventions spécifiques sont mises en œuvre. Si le certificat qui fait l'objet de la demande de révocation fait référence à l'Organisation, l'AC informera cette dernière de la révocation. L'AC/AE informera également le Demandeur de la révocation.

Demande de la part de l'ANC : dans le cas d'une demande de révocation du QSealC DSP2, la révocation peut être demandée par l'ANC qui a délivré le numéro d'autorisation au prestataire de services de paiement (PSP) figurant dans le certificat.

4.9.4 Délai de grâce de la demande de révocation

Le délai de grâce de la LCR est la période qui s'écoule entre le moment de la publication de la LCR suivante par l'AC et le moment où expire la LCR en cours. Afin de ne causer de dysfonctionnement à aucune des parties concernées, cette période est plus longue que celle dont l'AC a besoin pour générer et publier une nouvelle LCR. De cette façon, la LCR en cours reste valable au moins jusqu'à ce qu'elle soit remplacée par la nouvelle LCR.

4.9.5 Délai maximum pour le traitement de la demande de révocation

La demande est traitée dans un délai d'une heure, à moins que d'autres contrôles de son authenticité ne soient nécessaires. Si la demande est authentifiée correctement, elle sera traitée immédiatement, sinon le certificat sera suspendu en attendant une vérification plus approfondie concernant l'authenticité de la demande reçue.

4.9.6 Exigences relatives à la vérification de la révocation

Sans objet.

4.9.7 Fréquence de publication de la LCR

Les certificats révoqués ou suspendus sont insérés dans une Liste des Certificats Révoqués et Suspendus (LCR) signée par l'AC émettrice et publiée dans l'annuaire public. La publication de la LCR est programmée une fois toutes les heures (publication ordinaire). L'AC peut, dans des circonstances particulières, forcer la publication non programmée de la LCR (publication extraordinaire immédiate), par exemple lorsque la révocation ou la suspension d'un certificat intervient en raison de la compromission présumée de la confidentialité de la clé privée (révocation ou suspension immédiate). La LCR est toujours publiée dans son intégralité. C'est la date fournie par le système de l'Autorité d'Horodatage InfoCert qui fait foi du moment de la publication de la LCR et cet enregistrement est reporté dans les journaux d'évènements. Chaque élément de la liste LCR contient dans son extension la date et l'heure de la révocation ou de la suspension. L'AC se réserve le droit de publier séparément d'autres LCR, sous-ensembles de la LCR plus générale, afin d'alléger la charge du réseau. L'acquisition et la consultation de la LCR sont effectuées par les utilisateurs. La LCR à consulter pour le certificat spécifique est indiquée dans le certificat lui-même selon les règles en vigueur.

4.9.8 Latence maximale de la LCR

Une fois que l'authenticité de la demande de révocation ou de suspension a été vérifiée, le délai d'attente entre sa transmission à l'AC et sa mise en œuvre par la publication de la LCR est d'une heure maximum.

4.9.9 Services en ligne de vérification du statut de révocation du certificat

Outre la publication de la LCR dans les annuaires LDAP et http, InfoCert fournit également un service OCSP permettant de vérifier le statut du certificat. L'URL du service est indiquée dans le certificat. Le service est disponible 24 heures sur 24, 7 jours sur 7.

4.9.10 Exigences relatives aux services de vérification en ligne

Voir appendice A

4.9.11 Autres formes de révocation

Sans objet.

4.9.12 Exigences spécifiques en cas de compromission

Sans objet.

4.9.13 Raisons de la suspension

La suspension doit être effectuée si les conditions suivantes sont remplies :

1. une demande de révocation a été faite sans pouvoir établir son authenticité en temps utile ;
2. le Sujet, le Demandeur ou le Tiers Concerné, l'AE ou l'AC ont des éléments de doute quant à la validité du certificat ;
3. des doutes subsistent quant à la sécurité du dispositif de signature ou du dispositif OTP, le

cas échéant ;
4. une interruption temporaire de la validité du certificat est nécessaire.

Dans les cas ci-dessus, la suspension du certificat est demandée en précisant éventuellement sa durée. À l'expiration de ce délai, ou sur demande de réactivation du certificat, il s'ensuit soit une révocation définitive, soit la reprise de sa validité.

4.9.14 Qui peut demander la suspension ?

La suspension peut être demandée par le Sujet à tout moment et pour n'importe quelle raison. En outre, la suspension du certificat peut également être demandée par le Demandeur ou le Tiers Concerné, pour les raisons et de la manière prévues dans la présente Déclaration des Pratiques de Certification (*Certificate Practise Statement*). Enfin, le certificat peut être suspendu d'office par l'AC.

4.9.15 Procédures de demande de suspension

La demande de suspension se fait de différentes manières en fonction de la personne qui s'en charge. La suspension est toujours limitée dans le temps. La suspension prend fin à 24:00:00 le dernier jour de la période demandée.

4.9.15.1 Suspension demandée par le Sujet

Le Sujet doit demander la suspension selon l'une des procédures suivantes :

1. en utilisant la fonction de suspension disponible sur le site web de l'AC, en communiquant les données demandées et en utilisant le code d'urgence fourni lors de la délivrance du certificat, s'il est connu.
2. en utilisant (le cas échéant) la fonction de suspension avec OTP disponible sur le site web indiqué dans la documentation contractuelle fournie au moment de l'enregistrement.
3. en appelant le centre d'appel de l'AC et en fournissant les informations demandées. En l'absence du code d'urgence et uniquement dans le cas d'une demande de suspension pour cause de compromission de la clé, le centre d'appel suspend immédiatement le certificat – après avoir vérifié le numéro de téléphone d'où provient l'appel – ce, pour une durée de 10 (dix) jours calendaires en attendant la demande écrite du Sujet ; si l'AC ne reçoit pas la demande signée dans le délai indiqué, elle procède à la réactivation du certificat.
4. par les canaux de contact de l'Autorité d'Enregistrement, qui demande les données et documents nécessaires, procède à toutes les vérifications sur l'identité du Sujet, puis demande la suspension à l'AC
5. en utilisant la fonction de suspension disponible sur le site web de l'AE comme interface avec les services CMS.

Si le certificat faisant l'objet de la demande de suspension contient des informations concernant le Rôle du Sujet, l'AC communiquera la révocation au Tiers Concerné avec lequel les conventions spécifiques sont mises en œuvre.

Si le certificat qui fait l'objet de la demande de suspension fait référence à l'Organisation, l'AC informera cette dernière de la suspension.

Si le contrat relatif au certificat faisant l'objet de la suspension le prévoit, l'AC notifiera également la suspension au Demandeur.

4.9.15.2 Suspension demandée par le Demandeur ou par le Tiers Concerné

Le Demandeur ou le Tiers Concerné peut demander la suspension du certificat du Sujet en remplissant le formulaire spécifique disponible sur le site de l'AC et auprès de l'AE, en fournissant la justification de la demande, en joignant la documentation pertinente, le cas échéant, et en indiquant les données du Sujet communiquées à l'AC au moment de la délivrance du certificat.

L'AC vérifie l'authenticité de la demande, en informe le Sujet selon les procédures de communication établies au moment de la demande de certificat et procède à la suspension. Pour la demande de suspension de la part du Demandeur ou du Tiers Concerné, d'autres procédures peuvent être spécifiées dans les accords qui pourraient être conclus entre ce dernier et l'AC.

En cas de demande de suspension pour des certificats LongTerm et OneShot, le Demandeur peut demander la suspension du certificat en s'authentifiant auprès des systèmes proposés par l'AC, également par le biais de services applicatifs, en suivant les procédures décrites dans la documentation contractuelle.

4.9.15.3 Suspension à l'initiative de l'AC

Sauf en cas d'urgence, l'AC informe au préalable le Sujet de son intention de suspendre le certificat, en précisant les raisons de la suspension, la date de prise d'effet et la date d'expiration. Dans tous les cas, ces dernières informations seront communiquées au Sujet dans les meilleurs délais.
Si le certificat faisant l'objet de la suspension contient des informations concernant le Rôle du Sujet, l'AC communiquera la suspension au Tiers Concerné avec lequel les conventions spécifiques sont mises en œuvre. Si le certificat qui fait l'objet de la suspension fait référence à l'Organisation, l'AC informera cette dernière de la suspension.

Si le contrat relatif au certificat faisant l'objet de la suspension le prévoit, l'AC notifiera également la suspension au Demandeur.

4.9.16 Limites de la période de suspension

À l'expiration de la période de suspension demandée, la validité du certificat est rétablie en retirant le certificat de la Liste des Certificats Révoqués et Suspendus (LCR). La réactivation doit avoir lieu dans les 24 heures suivant la fin de la suspension. Si le jour d'expiration de la suspension coïncide avec ou suit le jour d'expiration du certificat, la suspension se transforme en révocation, avec effet au début de la suspension.

Lorsque cela est prévu dans le contrat, il est possible de demander la réactivation du certificat avant la date d'expiration de la suspension.

Dans les cas où le certificat a été suspendu par un CMS, il est possible d'utiliser la fonction de réactivation disponible sur le site web d'interface avec les services CMS.

4.10 Services concernant le statut du certificat

4.10.1 Caractéristiques de fonctionnement

Les informations sur le statut des certificats sont disponibles à travers les LCR et le service OCSP. Le numéro de série d'un certificat révoqué reste dans la LCR même après la fin de la validité du certificat et au moins jusqu'à l'expiration du certificat de l'AC.
Les informations fournies par le service OCSP pour les certificats sont mises à jour en temps réel.

4.10.2 Disponibilité du service

Le service OCSP et les LCR sont disponibles 24 heures sur 24, 7 jours sur 7.

4.10.3 Caractéristiques optionnelles

Sans objet.

4.11 Résiliation des services de l'AC

La relation entre le Sujet et/ou le Demandeur et l'Autorité de Certification prend fin lorsque le certificat expire ou est révoqué, sauf dans des cas particuliers définis au niveau contractuel.

4.12 Dépôt auprès de tiers et récupération de la clé

Sans objet.

5 MESURES DE SÉCURITÉ ET CONTRÔLES

Le PSC InfoCert a créé un système de sécurité pour le système d'information lié au service de certification numérique. Le système de sécurité mis en place comprend trois niveaux :

- un niveau physique qui vise à assurer la sécurité des environnements dans lesquels le PSC gère le service,
- un niveau procédural, avec des aspects purement organisationnels,
- un niveau logique, à travers la fourniture de mesures technologiques matérielles et logicielles qui répondent aux problèmes et aux risques associés au type de service et à l'infrastructure utilisés.

Ce système de sécurité est conçu pour éviter les risques liés au dysfonctionnement des systèmes, du réseau et des applications, ainsi qu'à l'interception non autorisée ou à la modification des données.

Un extrait de la politique de sécurité d'InfoCert est disponible sur demande à l'adresse de courrier électronique certifié infocert@legalmail.it.

5.1 Sécurité physique

Les mesures adoptées doivent offrir des garanties de sécurité suffisantes en ce qui concerne :

- Les caractéristiques du bâtiment et de la construction ;
- Les systèmes anti-intrusion actifs et passifs ;
- Le contrôle des accès physiques ;
- L'alimentation électrique et le conditionnement d'air ;
- La protection contre les incendies ;
- La protection contre les dégâts des eaux ;
- Le mode de stockage des supports magnétiques ;
- Les sites de stockage des supports magnétiques.

5.1.1 Emplacement et construction de la structure

Le centre de données InfoCert est situé à Padoue. Le site de reprise après sinistre se trouve à Modène et est relié au centre de données susmentionné par une connexion dédiée et redondante sur deux circuits MPLS différents à 40 Gbit/s chacun pouvant être mis à niveau jusqu'à 100 Gbit/s.

À l'intérieur des deux sites se trouvent des salles placées sous haute protection, tant physique que logique, renfermant les équipements informatiques qui constituent le cœur des services de certification numérique, d'horodatage, de signature à distance et automatique.

Pour les services offrant une continuité opérationnelle dont les valeurs RTO/RPO sont proches de zéro, certains éléments des services d'AC liés à la publication des LCR et à l'OCSP sont hébergés sur le cloud AWS respectivement dans la région Europe Francfort et la région Europe Irlande. En outre, une copie cryptée des données est effectuée dans la région Europe Francfort afin de garantir l'adéquation opérationnelle de l'AC « InfoCert Qualified Electronic Signature CA 4 ».

AWS est certifié selon les normes ISO/IEC ISO/IEC 27001:2013, 27017:2015, 27018:2019 e ISO/IEC 9001:2015.

Figure 1 – Localisation du centre de données InfoCert et site de reprise après sinistre

5.1.2 Accès physique

L'accès au centre de données est réglementé par les procédures de sécurité d'InfoCert. À l'intérieur du centre de données se trouve la zone du bunker où se trouvent les systèmes de l'AC, pour lesquels un facteur de sécurité supplémentaire est nécessaire.

5.1.3 Système électrique et de climatisation

Le site qui héberge le centre de données InfoCert à Padoue, bien que non certifié, a les caractéristiques d'un centre de données de niveau 3.

Les locaux techniques sont équipés d'un système d'alimentation électrique conçu pour prévenir les pannes et surtout les dysfonctionnements. L'alimentation des systèmes comprend les technologies les plus modernes afin de renforcer la fiabilité et d'assurer la redondance des fonctionnalités les plus critiques aux fins des services fournis.

L'infrastructure électrique comprend :

- Des alimentations sans interruption, équipées d'accumulateurs, en courant alternatif (UPS) ;
- La disponibilité du courant alternatif (220-380V AC) ;
- Des armoires électriques redondantes avec des lignes protégées dimensionnées pour l'absorption fixée ;
- Un service de générateurs d'urgence ;
- Un système de commutation automatique et de synchronisation entre les générateurs, le réseau et les batteries (STS).

Chaque armoire technologique installée au centre de données bénéficie de deux lignes électriques qui assurent la haute disponibilité (HA) en cas d'interruption de l'une des deux lignes disponibles.

L'armoire technologique est surveillée à distance ; des contrôles constants sont effectués sur l'état de la ligne électrique (ON/OFF) et la puissance électrique absorbée (chaque ligne ne doit pas dépasser 50 % de la charge).

La température de la zone technique est normalement maintenue entre 20 °C et 27 °C avec une humidité relative entre 30 % et 60 %. Les installations sont équipées de batteries à condensation avec un système de collecte et d'évacuation des condensats hermétique et contrôlé par des détecteurs d'inondation. L'ensemble du système de conditionnement d'air est relié aux générateurs de secours en cas de coupure de courant. La capacité de réfrigération de chaque armoire est garantie avec une charge maximale prévue de 10 KW et un maximum de 15 KW sur deux armoires côte à côte.

5.1.4 Prévention et protection contre les dégâts des eaux

L'emplacement de l'immeuble ne présente pas de risques environnementaux en raison de sa proximité avec des installations « dangereuses ». Lors de la conception du bâtiment, des précautions appropriées ont été prises pour isoler les locaux potentiellement dangereux, tels que ceux contenant le groupe électrogène et la centrale thermique.
La zone qui abrite l'équipement se trouve au rez-de-chaussée, dans une position surélevée par rapport au niveau de la rue.

5.1.5 Prévention et protection contre les incendies

Dans le centre de données, il existe un système de détection de fumée géré par une unité de contrôle analogique adressée NOTIFIER avec des capteurs optiques dans les pièces et dans le faux plafond et des capteurs d'air installés sous le plancher et dans les conduits d'air.
Le système de détection automatique des incendies est relié aux systèmes d'extinction écologiques au gaz NAFS125 et PF23 et, dans certaines pièces, à des systèmes d'extinction par aérosol.
En cas d'intervention simultanée de deux détecteurs dans la même zone, la décharge de l'extincteur commandée est celle de la zone concernée.
Un système d'extinction spécifique est prévu pour chaque compartiment coupe-feu.
Il existe également des extincteurs portables conformément aux lois et réglementations en vigueur.
Les conduits d'air primaire utilisés pour les salles d'équipement sont dotés de clapets coupe-feu aux traversées des compartiments coupe-feu, actionnés par le système de détection automatique d'incendie.

5.1.6 Supports de stockage

En ce qui concerne la plateforme de stockage, la solution existante prévoit l'utilisation de systèmes NetApp (FAS 8060) pour la partie NAS. En revanche, pour la partie SAN, une infrastructure a été mise en place pour la partie centre de données basée sur les technologies Infinidat, y compris deux boîtiers de génération InfiniBox F4000 et F6000 ; pour la partie d'AC, l'infrastructure est basée sur la technologie Pure Storage.

5.1.7 Élimination des déchets

InfoCert est certifiée ISO 14001 pour la gestion environnementale durable de son cycle de production, y compris la collecte sélective et l'élimination durable des déchets. En ce qui concerne le contenu informatif des déchets électroniques, avant d'être éliminés, tous les supports sont nettoyés selon les procédures prévues, ou par des entreprises d'assainissement certifiées.

5.1.8 Sauvegarde hors site

Il est réalisé sur le site de reprise après sinistre, avec un dispositif EMC Data Domain 4200, sur lequel le domaine des données principal du site de Padoue réplique les données de sauvegarde.

5.2 Contrôles procéduraux

5.2.1 Rôles clés

Les rôles clés sont confiés à des personnes ayant l'expérience, le professionnalisme et les compétences techniques et juridiques nécessaires, qui sont contrôlées en permanence au moyen d'évaluations annuelles.
La liste des noms et l'organigramme des rôles clés ont été déposés auprès de l'AgID lors de la première accréditation et sont constamment mis à jour pour suivre l'évolution naturelle de l'organisation de l'entreprise.

5.3 Contrôle du personnel

5.3.1 Qualifications, expérience et autorisations requises

Après avoir procédé à la planification annuelle des ressources humaines, le responsable de la fonction/structure organisationnelle identifie les caractéristiques et les compétences de la ressource à insérer (profil du poste). Ensuite, de concert avec le responsable de la sélection, le processus de recherche et de sélection est mis en œuvre.

5.3.2 Procédures de vérification de l'expérience passée

Les candidats identifiés participent au processus de sélection en passant un premier entretien avec le responsable de la sélection, un entretien qui aura pour but de faire connaissance et de juger de la motivation du candidat. Suivra un entretien technique avec le chef de fonction/structure organisationnelle, visant à vérifier les compétences que le candidat déclare posséder. Il existe d'autres outils de vérification qui consistent à soumettre le candidat à des exercices et à lui faire passer des tests.

5.3.3 Exigences en matière de formation

Afin de garantir que personne ne puisse individuellement compromettre ou altérer la sécurité globale du système ou exercer des activités non autorisées, il est prévu de confier la gestion opérationnelle du système à différentes personnes, avec des tâches distinctes et clairement

définies. Le personnel responsable de la conception et de la prestation de services de certification est salarié d'InfoCert. Ces personnes ont été sélectionnées sur la base de leur expérience en matière de conception, de mise en œuvre et de gestion de services informatiques, elles sont dignes de confiance et font preuve de discrétion. Des formations périodiques sont planifiées pour sensibiliser le personnel aux tâches assignées. En particulier, avant que le personnel prenne part aux activités opérationnelles, il suit une formation visant à lui apporter toutes les compétences (techniques, organisationnelles et procédurales) nécessaires pour accomplir les tâches qui lui sont assignées.

5.3.4 Fréquence de mise à jour de la formation

Au début de chaque année, une analyse des besoins de formation est effectuée en vue de définir les activités de formation à fournir au cours de l'année. L'analyse est structurée de la façon suivante :

- Rencontre avec la Direction pour la collecte des données concernant les besoins de formation nécessaires à la réalisation des objectifs de l'entreprise ;
- Entretien avec les responsables pour identifier les besoins de formation spécifiques de leur secteur ;
- Retour des données collectées à la direction de l'entreprise pour clôture et approbation du plan de formation.

Au mois de février, le plan de formation ainsi défini est partagé et rendu public.

5.3.5 Fréquence de rotation des équipes

La présence au siège est régie par un plan de roulement du personnel qui est préparé chaque mois par le chef de l'unité organisationnelle, au moins 10 jours à l'avance. Chaque quart de travail dure huit heures.
Sans préjudice de la possession des exigences techniques et professionnelles nécessaires, la société veille à ce qu'un maximum de travailleurs s'alternent dans le travail posté, en donnant la priorité aux salariés qui en font la demande.
Aucune équipe de nuit n'est prévue. Les horaires de présence sur place s'étalent sur un créneau horaire de 07h00 à 21h00 du lundi au vendredi et de 07h00 à 12h00 le samedi.

5.3.6 Sanctions en cas d'actions non autorisées

Pour la procédure de sanction, il est fait référence à la convention collective nationale du travail du secteur de la métallurgie pour les travailleurs de l'industrie métallurgique privée et du montage d'installations, « CCNL Metalmeccanici e installazione impianti industria privata ».

5.3.7 Contrôles du personnel non salarié

Le recours au personnel non salarié est réglementé par une politique spécifique de l'entreprise

5.3.8 Documents que le personnel doit fournir

Au moment de l'embauche, le salarié doit fournir la copie d'une pièce d'identité valide, la copie d'une carte Vitale valide et une photo d'identité pour le badge d'accès aux locaux. Il doit ensuite remplir et signer le consentement au traitement des données à caractère personnel et

l'engagement de ne divulguer aucune information et/ou aucun document confidentiel. Enfin, il doit prendre connaissance du Code d'éthique et de la nétiquette InfoCert.

5.4 Gestion du des journaux d'évènements

Les événements liés à la gestion de l'AC et à la durée de vie du certificat sont consignés dans les journaux d'évènements, conformément au règlement et aux règles techniques[5].

5.4.1 Types d'événements stockés

Les événements de sécurité, le démarrage et l'arrêt, les pannes du système et les défaillances matérielles, l'activité du pare-feu et du routeur ainsi que les tentatives d'accès au système IGC sont tous enregistrés.
Tous les documents et données utilisés lors de l'identification et de l'acceptation de la demande du Demandeur sont conservés : copie de la carte d'identité, contrats, Kbis, etc.
Les événements liés à l'enregistrement et au cycle de vie des certificats sont enregistrés : demandes et renouvellement de certificats, enregistrements de certificats, génération, diffusion et éventuellement révocation/suspension.
Tous les événements concernant la personnalisation du dispositif de signature sont enregistrés.
Tous les accès physiques aux salles hautement sécurisées où se trouvent les machines de l'AC sont enregistrés.
Tous les accès logiques aux applications de l'AC sont enregistrés.
Chaque événement est enregistré avec la date et l'heure de l'événement dans le système.

5.4.2 Fréquence de traitement et stockage des journaux d'évènements

Le traitement et le regroupement des données ainsi que le stockage sur le système de conservation des données InfoCert ont lieu mensuellement.

5.4.3 Période de conservation des journaux d'évènements

Les journaux d'évènements sont conservés pendant 20 ans par l'AC.

5.4.4 Protection des journaux d'évènements

La protection des journaux d'évènements est garantie par le système de conservation des documents électroniques InfoCert, accrédité auprès de l'AgID selon la réglementation en vigueur.

5.4.5 Procédures de sauvegarde des journaux d'évènements

Le système de conservation des documents électroniques met en œuvre une politique et une procédure de sauvegarde, comme prévu dans le manuel de sécurité du système en question.

5.4.6 Système de stockage des journaux d'évènements

Les journaux d'événements sont collectés par le biais de procédures automatiques spécifiques ; le stockage se fait de la manière prévue par le système de stockage selon les termes d'InfoCert et décrite dans le manuel de sécurité du système en question.

5.4.7 Notification en cas d'identification de vulnérabilités

Sans objet.

5.4.8 Évaluations des vulnérabilités

InfoCert effectue périodiquement des évaluations de vulnérabilité et des tests de pénétration. À la lumière des résultats, elle met en œuvre toutes les contre-mesures pour sécuriser les applications.

5.5 Archivage des dossiers

5.5.1 Types de dossier archivés

Sont rédigés et archivés les dossiers concernant les événements les plus importants d'une Autorité de Certification. Les dossiers sont conservés pendant 20 ans par l'Autorité de Certification dans le système de conservation des documents InfoCert.

5.5.2 Protection des dossiers

La protection est garantie par le système de conservation des documents InfoCert, accrédité auprès de l'AgID.

5.5.3 Procédures de sauvegarde des dossiers

Le système de conservation met en œuvre une politique et une procédure de sauvegarde, comme prévu dans le manuel de sécurité du système en question.

5.5.4 Exigences relatives à l'horodatage des dossiers

Sans objet.

5.5.5 Système de stockage des archives

Les dossiers sont collectés par le biais de procédures automatiques spécifiques ; le stockage se fait de la manière prévue par le système de stockage selon les termes d'InfoCert et décrite dans le manuel de sécurité du système en question.

5.5.6 Procédures de récupération et de vérification des informations contenues dans les archives

Des procédures et des systèmes automatiques sont en place pour contrôler l'état du système de certification et de l'ensemble de l'infrastructure technique de l'AC.

5.6 Remplacement de la clé privée de l'AC

L'AC effectue les procédures de remplacement périodique de la clé privée de certification, utilisée pour la signature des certificats, afin que le sujet puisse utiliser le certificat en sa possession

jusqu'à son renouvellement. Tout remplacement entraînera une modification de cette Politique de Certification et une notification à l'Autorité de Contrôle (AgID).

5.7 Compromission de la clé privée de l'AC et reprise après sinistre

5.7.1 Procédures de gestion des incidents

L'AC a décrit les procédures de gestion des incidents au sein du SMSI certifié ISO 27000. Tout incident, dès qu'il est détecté, fait l'objet d'une analyse ponctuelle, d'une identification des mesures correctives et d'un rapport par le responsable du service. Le rapport doit être signé numériquement ; une copie doit également être envoyée à l'AgID, avec une déclaration des actions d'intervention visant à éliminer les causes qui ont pu donner lieu à l'incident, si elles sont sous le contrôle d'InfoCert conformément à l'article 19 du règlement.

5.7.2 Corruption des machines, du logiciel ou des données

En cas de défaillance du dispositif de signature HSM sécurisé contenant les clés de certification, il faut utiliser la copie de sauvegarde de la clé de certification, sauvegardée et conservée comme il se doit. Il n'est pas nécessaire de révoquer le certificat de l'AC correspondant.

Les logiciels et les données font l'objet de sauvegardes régulières, conformément aux procédures internes.

5.7.3 Procédures en cas de compromission de la clé privée de l'AC

La compromission de la clé de certification est considérée comme un événement particulièrement critique, car elle invaliderait les certificats émis signés avec cette même clé. Une attention particulière est donc accordée à la protection de la clé de certification et à toutes les activités de développement et de maintenance du système qui peuvent avoir un impact sur celle-ci.
InfoCert a décrit la procédure à suivre en cas de compromission de la clé, dans le cadre du SMSI certifié ISO 27000, en fournissant également la preuve à l'AgID et à l'OEC.

5.7.4 Continuité des services de l'AC en cas de sinistre

InfoCert a adopté les procédures nécessaires pour assurer la continuité du service même dans des situations très critiques ou en cas de catastrophe.

5.8 Cessation du service de l'AC ou de la l'AE

En cas de cessation de l'activité de certification, InfoCert communiquera cette intention à l'Autorité de Contrôle (AgID) et à l'Organisme d'Évaluation de la Conformité (OEC) au moins 6 mois à l'avance, en indiquant, le cas échéant, le certificateur remplaçant, le dépositaire de l'annuaire des certificats et de la documentation connexe. InfoCert informe tous les détenteurs de certificats qu'elle a elle-même délivrés de sa cessation d'activités avec le même préavis. Si aucun certificateur de remplacement n'est indiqué dans la communication, il sera clairement indiqué que tous les certificats non encore expirés au moment de la cessation d'activités de l'AC seront

révoqués.

6 CONTRÔLES DE SÉCURITÉ TECHNOLOGIQUE

6.1 Installation et génération de la bi-clé de certification

Afin de mener à bien son activité, l'Autorité de Certification doit générer la bi-clé de certification pour la signature des certificats des Sujets.

Les clés ne sont générées que par le personnel explicitement chargé de cette fonction. La génération des clés et de la signature se fait au sein de modules cryptographiques dédiés et certifiés, comme l'exige la réglementation en vigueur.

Les clés privées de l'AC sont protégées grâce au module cryptographique qui génère et utilise la clé. La clé privée ne peut être générée qu'avec la présence simultanée de deux opérateurs chargés de la générer. Les clés sont générées en présence du responsable du service.

Les clés privées de l'AC sont dupliquées, dans le seul but de les restaurer suite à la rupture du dispositif de signature sécurisé, selon une procédure contrôlée qui prévoit une répartition de la clé et du contexte sur plusieurs dispositifs, conformément aux critères de sécurité du dispositif HSM.

Le module cryptographique utilisé pour la génération de la clé et la signature a des exigences afin de garantir :

- la conformité de la bi-clé avec les exigences des algorithmes de génération et de vérification utilisés ;
- l'équiprobabilité de générer toutes les bi-clés possibles ;
- l'identification de la personne qui active la procédure de génération ;
- que la génération de la signature a lieu à l'intérieur du dispositif de telle sorte que la valeur de la clé privée utilisée ne puisse pas être interceptée.

6.1.1 Génération de la bi-clé du Sujet

Les clés asymétriques sont générées à l'intérieur d'un dispositif sécurisé de création de signature SSCD ou QSCD également de type HSM en utilisant les fonctionnalités natives offertes par les dispositifs eux-mêmes.
Dans le cas où le dispositif n'est pas mis à disposition par l'AC, le Demandeur doit s'assurer que le dispositif est conforme à la réglementation en vigueur, en présentant la documentation appropriée et en se soumettant à des audits périodiques. Dans le cas de HSM InfoCert, nous nous réservons le droit de superviser la cérémonie des clés.

6.1.2 Remise de la clé privée au Demandeur

La clé privée est contenue dans le dispositif cryptographique, qu'il s'agisse d'un SSCD ou d'un QSCD. Pour les certificats LongTerm et OneShot, le dispositif cryptographique est toujours HSM. Une fois que le dispositif cryptographique a été remis au Sujet, ce dernier entre en pleine

possession de la clé privée, qu'il peut utiliser uniquement avec le code PIN, dont il est le seul à avoir connaissance.
Dans le cas d'un processus d'enregistrement effectué en présence du Sujet, le dispositif est livré dès que les clés sont générées.
En cas de processus d'enregistrement non effectué en présence du Sujet, le dispositif est livré selon les modalités prévues dans le contrat, en veillant toujours à ce que le dispositif et les informations nécessaires à son utilisation soient acheminés par des canaux différents ou soient livrés au Sujet à deux moments différents. Dans certains cas, les dispositifs peuvent déjà être à la disposition du Sujet, livrés au préalable selon des procédures sécurisées et après identification du Sujet en question.

6.1.3 Remise de la clé publique à l'AC

Sans objet.

6.1.4 Remise de la clé publique aux utilisateurs

Si le Demandeur en fait la demande – à l'exception des certificats LongTerm et OneShot – il est également publiédans l'annuaire public, où l'utilisateur peut le récupérer.

6.1.5 Algorithme et longueur des clés

La bi-clé de certification asymétrique est générée à l'intérieur du dispositif cryptographique matériel cité ci-dessus. L'algorithme asymétrique RSA est utilisé avec des clés d'au moins 4096 bits.
Pour les clés du Sujet, l'algorithme de cryptage asymétrique utilisé est le RSA et la longueur de la clé est d'au moins 2048 bits.

6.1.6 Contrôle de la qualité et génération de la clé publique

Les dispositifs utilisés sont certifiés selon des standards de sécurité élevées (cf. § 6.2.1) et donnent la garantie que la clé publique est correcte et aléatoire. Avant de délivrer le certificat, l'AC vérifie que la clé publique n'a pas déjà été utilisée.

6.1.7 Objectif d'utilisation de la clé

Le but de l'utilisation de la clé privée est déterminé par l'extension KeyUsage telle que définie dans la norme X509. Pour les certificats décrits dans la présente Politique de Certification, la seule utilisation autorisée est celle de « non-répudiation »

6.2 Protection de la clé privée et contrôles techniques du module cryptographique

6.2.1 Contrôles et standards des modules cryptographiques

Les modules cryptographiques utilisés par InfoCert pour les clés de certification (AC) et le répondeur OCSP sont validés selon FIPS 140 niveau 3 et les Critères Communs (CC) Niveau

d'assurance de l'évaluation de la sécurité des technologies de l'information (EAL) EAL 4 + Type 3 (EAL 4 augmenté des composants d'assurance AVA_VLA.4 et AVA_MSU.3) en Europe.
Les cartes à puce utilisées par InfoCert sont validées selon les Critères Communs (CC) Niveau d'assurance de l'évaluation de la sécurité des technologies de l'information (EAL) EAL 4 + Type 3 (EAL 4 augmenté des composants d'assurance AVA_VLA.4 et AVA_MSU.3) ou EAL5 augmenté des composants d'assurance ALC_DVS.2 , AVA_VAN.5 .
Les modules cryptographiques utilisés par InfoCert pour les clés de signature à distance et automatique du Sujet sont validés selon FIPS 140 niveau 3 et les Critères Communs (CC) Niveau d'assurance de l'évaluation de la sécurité des technologies de l'information EAL 4.

6.2.2 Contrôle de la clé privée d'AC par plusieurs personnes

L'accès aux dispositifs contenant les clés de certification n'est possible qu'avec deux personnes authentifiées en même temps.

6.2.3 Dépôt de la clé privée d'AC auprès de tiers

Sans objet.

6.2.4 Sauvegarde de la clé privée d'AC

Les clés sont sauvegardées dans un coffre-fort auquel seul le personnel n'ayant pas accès aux dispositifs HSM a accès. Une éventuelle restauration nécessite donc la présence à la fois du personnel qui a accès aux dispositifs et de ceux qui ont accès au coffre-fort.

6.2.5 Archivage de la clé privée d'AC

Sans objet.

6.2.6 Transfert de la clé privée à partir d'un module ou dans un module cryptographique

Sans objet.

6.2.7 Stockage de la clé privée dans un module cryptographique

La clé de certification est générée et stockée dans une zone sécurisée du dispositif cryptographique, géré par le Certificateur, qui empêche son exportation. De plus, si la protection est forcée, le système d'exploitation du dispositif verrouille ce dernier ou le rend illisible.

6.2.8 Méthode d'activation de la clé privée

La clé privée de certification est activée par le logiciel de l'AC en double contrôle, c'est-à-dire par deux personnes ayant un rôle de confiance spécifique et en présence du responsable du service.
Le Sujet ou le Demandeur, représentant légal de la personne morale est responsable de la protection de sa clé privée par un mot de passe fort afin d'empêcher toute utilisation non autorisée. Pour activer la clé privée, le Sujet doit s'authentifier.

6.2.9 Méthode de désactivation de la clé privée

Sans objet.

6.2.10 Méthode de destruction de la clé privée de l'AC

Le personnel d'InfoCert dans ce rôle s'occupe de la destruction de la clé privée lorsque le certificat a expiré ou a été révoqué, conformément aux procédures de sécurité prévues par les politiques de sécurité et les spécifications du fabricant du dispositif.

6.2.11 Classification des modules cryptographiques

Sans objet.

6.3 Autres aspects de la gestion des clés

Sans objet.

6.3.1 Archivage de la clé publique

Sans objet.

6.3.2 Durée de validité du certificat et de la bi-clé

La durée de validité du certificat est déterminée sur la base :

- de l'état de la technologie ;
- des dernières avancées dans le domaine des connaissances cryptographiques de pointe ;
- de l'utilisation prévue du certificat lui-même.

La durée de validité du certificat est mentionnée à l'intérieur de la manière indiquée au paragraphe § 3.3.1.

Actuellement, le certificat de l'AC a une durée de 16 ans ; les certificats délivrés aux personnes physiques ou morales sont valables pour une durée maximale de 39 mois.

6.4 Données d'activation de la clé privée

Veuillez vous référer aux paragraphes 4.2 et 6.3.

6.5 Contrôles sur la sécurité informatique

6.5.1 Exigences de sécurité spécifiques pour les ordinateurs

Le système d'exploitation des ordinateurs utilisés dans les activités de certification pour la génération des clés, la génération des certificats et la gestion de l'annuaire des certificats est durci, c'est-à-dire qu'il est configuré de manière à minimiser l'impact des éventuelles vulnérabilités en éliminant toutes les fonctionnalités qui ne sont pas nécessaires au fonctionnement et à la gestion de l'AC.

Les administrateurs du système, désignés à cette fin conformément aux dispositions de la réglementation en vigueur, accèdent par l'intermédiaire d'une application « root on demand » qui

ne permet l'utilisation des privilèges de l'utilisateur *root* qu'après authentification individuelle. Les accès sont suivis, journalisés et conservés pendant 12 mois.

6.6 Opérativité sur les systèmes de contrôle

InfoCert attache une importance stratégique au traitement sécurisé des informations et reconnaît la nécessité de développer, maintenir, contrôler et améliorer en permanence un système de management de la sécurité de l'information (SGSI) conformément à la norme ISO/IEC 27001.
InfoCert est certifiée ISO/IEC 27001:2005 depuis mars 2011 pour les activités EA:33-35. En mars 2015, elle a été certifiée pour la nouvelle version de la norme ISO/IEC 27001:2013.
Dans le SMGI, des procédures et des contrôles sont prévus pour :

- Gestion des actifs ;
- Contrôle des accès ;
- Sécurité physique et environnementale ;
- Sécurité des activités opérationnelles ;
- Sécurité des communications ;
- Acquisition, développement et maintenance des systèmes ;
- Gestion des incidents ;
- Continuité opérationnelle.

Toutes les procédures sont approuvées par les responsables concernés et partagées en interne dans le système de management des documents InfoCert.

6.7 Contrôles de sécurité du réseau

Pour le service de certification, InfoCert a conçu une infrastructure de sécurité du réseau basée sur l'utilisation de mécanismes de pare-feu et du protocole SSL afin de créer un canal sécurisé entre les Autorités d'Enregistrement et le système de certification, ainsi qu'entre ce dernier et les administrateurs/opérateurs.

Les systèmes et les réseaux d'InfoCert sont connectés à Internet de manière contrôlée par des systèmes de pare-feu qui permettent de diviser la connexion en zones progressivement plus sûres : réseau internet, réseaux DMZ (zone démilitarisée) ou périmétriques, réseaux internes. Tout le trafic circulant entre les différentes zones est soumis à l'acceptation du pare-feu, sur la base d'un ensemble de règles établies. Les règles définies sur les pare-feux sont conçues selon les principes de « refus par défaut » (ce qui n'est pas expressément autorisé est interdit par défaut, c'est-à-dire que les règles n'autoriseront que ce qui est strictement nécessaire au bon fonctionnement de l'application) et de « défense en profondeur » (des niveaux successifs de défense sont organisés, d'abord au niveau du réseau, à travers des barrières successives de pare-feux, avec pour finir un durcissement au niveau du système).

6.8 Système d'horodatage

InfoCert fournit un service d'horodatage qualifié. Pour le marquage temporel, il faut se référer à la Politique de Certification ICERT-INDI-TSA qui se trouve sur le site du prestataire de services de confiance InfoCert.

7 FORMAT DU CERTIFICAT, DE LA LCR ET DE L'OCSP

7.1 Format du certificat

Le certificat contient les informations indiquées dans la demande de certification.
Le format du certificat produit est conforme au règlement eIDAS et à l'avis n° 121/2019 [9] ; de cette manière, la lisibilité et la vérifiabilité complètes sont totalement garanties dans le contexte de la règlementation et des certificateurs européens.
InfoCert utilise la norme ITU X.509, version 3, pour toute la structure de l'IGC.
En appendice A se trouve la présentation des certificats racine et des Sujets, qu'il s'agisse de personnes physiques ou morales.

7.1.1 Numéro de version

Tous les certificats délivrés par InfoCert sont X.509 version 3.

7.1.2 Extensions du certificat

Les certificats qualifiés sont caractérisés par les extensions contenues dans la clause 3.2.6 de la déclaration de certificat qualifié (QCStatement) telle que définie dans l'IETF RFC 3739. Leur utilisation est réglementée par la norme ETSI 319 412-5.
Voir l'appendice A pour les extensions du certificat.

7.1.3 OID de l'algorithme de signature

Les certificats sont signés avec l'algorithme suivant :
sha256WithRSAEncryption [iso(1) member-body(2) us(840) rsadsi(113549) pkcs(1) pkcs-1(1) 11].

7.1.4 Formes de nom

Chaque certificat contient un numéro de série unique au sein de l'AC qui l'a délivré.

7.1.5 Contraintes liées aux noms

Voir à ce sujet le paragraphe 3.1.

7.1.6 OID du certificat

Voir à ce sujet le paragraphe 1.2.

7.2 Format de la LCR

InfoCert utilise le profil RFC5280 « Internet X.509 Public Key Infrastructure Certificate Revocation List (CRL) » pour constituer les LCR et ajoute au format de base les extensions définies par la RFC 5280 : « Authority Key Identifier », « CRL Number », « Issuing Distribution Point » et « expiredCertsOnCRL »

7.2.1 Numéro de version

Toutes les LCR publiées par InfoCert sont des LCR X.509 version 2.

7.2.2 Extensions de la LCR

Pour les extensions de la LCR, voir à l'appendice A.

7.3 Format de l'OCSP

Afin de pouvoir déterminer l'état de révocation du certificat sans avoir recours à la LCR, InfoCert met à disposition des services OCSP conformes au profil RFC6960 « X.509 Internet Public Key Infrastructure Online Certificate Status Protocol - OCSP ». Ce protocole spécifie les données à échanger par une application qui veut vérifier le statut du certificat et le service OCSP.

7.3.1 Numéro de version

Le protocole OCSP utilisé par InfoCert est conforme à la version 1 du RFC6960.

7.3.2 Extensions de l'OCSP

Pour les extensions de l'OCSP, voir l'appendice A.

8 CONTRÔLES ET ÉVALUATIONS DE CONFORMITÉ

Afin d'obtenir le statut de prestataire de services de confiance qualifié et non qualifié conformément au règlement eIDAS, il est nécessaire de suivre la procédure prévue à l'article 21 dudit règlement.
InfoCert a présenté une demande spécifique à l'AgID afin de se faire reconnaître comme « prestataire de services de confiance qualifié » en joignant un rapport d'évaluation de la conformité au règlement (REC) délivré par un organisme d'évaluation agréé par l'organisme national responsable (OEC), qui en Italie est ACCREDIA.
InfoCert fournit le service en tant que prestataire de services de confiance qualifié conformément au règlement (UE) n° 910/2014 du 23/07/2014, sur la base d'une évaluation de la conformité effectuée par l'organisme d'évaluation de la conformité CSQA Certificazioni S.r.l., au sens du règlement mentionné ci-dessus et à la norme ETSI EN 319 401, selon le schéma d'évaluation eIDAS défini par ACCREDIA par rapport aux normes ETSI EN 319_403 et UNI CEI EN ISO/IEC 17065:2012.

8.1 Fréquence ou circonstances de l'évaluation de la conformité

L'évaluation de la conformité est répétée tous les deux ans, mais chaque année, l'OEC effectue un audit de surveillance.

8.2 Identité et qualifications de la personne effectuant le contrôle

Le contrôle est effectué par :

Dénomination sociale	**CSQA Certification S.r.l.**
Siège social statutaire	Via S. Gaetano n. 74, 36016 Thiene (VI)
Numéro de téléphone	+39 0445 313011
N° d'immatriculation RCS	Numéro fiscal 02603680246 N° de RCS VI 02603680246 / N° de REA 258305
N° de TVA	02603680246
Site web	http://www.csqa.it

8.3 Relations entre InfoCert et OEC

InfoCert et CSQA n'ont aucun intérêt financier ni aucune relation d'affaires.
Il n'existe aucune relation commerciale ni de partenariat en cours qui pourraient créer des préjugés en faveur ou à l'encontre d'InfoCert dans l'évaluation objective du CSQA.

8.4 Aspects à évaluer

L'OEC est appelé à évaluer la conformité à la Politique de Certification, au règlement et à la réglementation applicable concernant les procédures adoptées, l'organisation de l'AC, l'organisation des rôles, la formation du personnel et la documentation contractuelle.

8.5 Actions en cas de non-conformité

En cas de non-conformité, l'OEC décidera s'il faut quand même envoyer le rapport à l'AgID ou se réserver le droit de procéder à un nouvel audit une fois que la non-conformité aura été corrigée.
InfoCert s'engage à résoudre toutes les non-conformités en temps utile, en mettant en œuvre toutes les mesures d'amélioration et d'ajustement nécessaires.

9 AUTRES ASPECTS JURIDIQUES ET COMMERCIAUX

9.1 Tarifs

9.1.1 Tarifs pour la délivrance et le renouvellement des certificats

Dans le cas des certificats LongTerm ou OneShot, en règle générale, les coûts de délivrance du certificat sont supportés par le Demandeur et non par le Sujet, sur la base des tarifs définis dans le contrat de services entre le Demandeur et InfoCert. Toutefois, le contrat avec le Sujet peut également prévoir des tarifs spécifiques dans les relations avec le Sujet.

Dans les autres cas, les tarifs sont disponibles sur https://www.firma.infocert.it/ et http://ecommerce.infocert.it, ou auprès des Autorités d'Enregistrement. L'AC peut conclure des accords commerciaux avec l'AE et/ou les Demandeurs en prévoyant des tarifs spécifiques.

9.1.2 Tarifs pour accéder aux certificats

L'accès à l'annuaire public des certificats publiés est libre et gratuit.

9.1.3 Tarifs pour accéder aux informations sur l'état de suspension et de révocation des certificats

L'accès à la Liste des Certificats Révoqués ou Suspendus est libre et gratuit.

9.1.4 Tarifs pour d'autres services

Les tarifs sont disponibles sur https://www.firma.infocert.it/ et http://ecommerce.infocert.it, ou auprès des Autorités d'Enregistrement.

L'AC peut conclure des accords commerciaux avec l'AE et/ou les Demandeurs en prévoyant des tarifs spécifiques.

9.1.5 Politiques de remboursement

Si le service est acheté par un consommateur, le Sujet a le droit de se rétracter du contrat dans les 14 jours suivant la date de conclusion du contrat en se faisant rembourser le prix payé. Les instructions pour l'exercice du droit de rétractation et la demande de remboursement sont disponibles sur le site https://help.infocert.it/ ou auprès de l'AE.

9.2 Responsabilité financière

9.2.1 Couverture d'assurance

Le PSC InfoCert a souscrit un contrat d'assurance pour couvrir les risques liés à son activité et les dommages causés à des tiers, dont le texte a été traité et accepté par l'AgID et dont les plafonds sont les suivants :

- 10 000 000 euros par sinistre ;
- 10 000 000 euros par an.

9.2.2 Autres activités

Sans objet.

9.2.3 Garantie ou couverture d'assurance pour les entités utilisatrices

Voir le paragraphe 9.2.1.

9.3 Confidentialité des informations commerciales

9.3.1 Périmètre des informations confidentielles

Dans le cadre de l'activité faisant l'objet de la présente Politique de Certification, il n'est pas prévu de gérer des informations confidentielles.

9.3.2 Informations ne relevant pas du périmètre des informations confidentielles

Sans objet.

9.3.3 Responsabilité en termes de protection des informations confidentielles

Sans objet.

9.4 Confidentialité

Les informations relatives au Sujet et au Demandeur dont l'AC prend possession dans l'exercice de ses activités habituelles doivent être considérées, sauf consentement exprès, comme confidentielles et non publiables, à l'exception de celles qui sont explicitement destinées à un usage public [clé publique, certificat (si le Sujet le demande), dates de révocation et de suspension du certificat]. En particulier, les données à caractère personnel sont traitées par InfoCert conformément aux dispositions du Décret législatif italien n° 196 du 30 juin 2003, du règlement (UE) 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, pleinement contraignant depuis le 25 mai 2018 [4].

9.4.1 Programme de confidentialité

InfoCert adopte un ensemble de politiques par lesquelles elle met en œuvre et intègre la protection des données à caractère personnel dans son système de management de la sécurité de l'information certifié ISO 27001, en partageant avec ce dernier le processus d'amélioration continue.

9.4.2 Données traitées comme des données à caractère personnel

Sont traitées comme des données à caractère personnel les données qui relèvent de la définition correspondante visée dans la réglementation en vigueur [4] ; les données à caractère personnel sont donc toute information concernant une personne physique, identifiée ou identifiable, même indirectement, par référence à toute autre information, y compris un numéro d'identification personnel.

9.4.3 Données non considérées comme données à caractère personnel

Les données prévues d'être rendues publiques par la direction technique de l'AC, ou la clé publique, le certificat (si le Sujet le demande), les dates de révocation et de suspension du certificat, ne sont pas considérées comme des données à caractère personnel.

9.4.4 Responsable du traitement des données à caractère personnel

InfoCert S.p.A.
Siège opérationnel
Via Marco e Marcelliano 45
00147 Rome
richieste.privacy@legalmail.it

9.4.5 Politique de confidentialité et consentement au traitement des données à caractère personnel

La politique de confidentialité est disponible sur le site www.infocert.it. Des informations spécifiques peuvent être disponibles sur le site du Demandeur, qui recueille le consentement au traitement pour le compte d'InfoCert. Avant de procéder à tout traitement de données à caractère personnel, InfoCert recueille le consentement au traitement de la manière et dans les formes prévues par la loi [4].

9.4.6 Divulgation de données à la suite d'une demande des autorités

La divulgation de données à la demande des autorités est obligatoire et s'effectue selon les modalités établies par l'Autorité en question, au cas par cas.

9.4.7 Autres motifs de divulgation

Non prévus.

9.5 Propriété intellectuelle

Le copyright de ce document est la propriété d'InfoCert S.p.A. Tous droits réservés.

9.6 Représentation et garanties

InfoCert conserve la responsabilité du respect des procédures prescrites dans sa politique de sécurité de l'information, même lorsque certaines fonctions sont déléguées à une autre entité, conformément à l'article 2.4.1. de l'annexe du règlement d'exécution (UE) 2015/1502 de la Commission.
Dans ce dernier cas, la représentation est possible au moyen d'un mandat donné par InfoCert à l'Autorité d'Enregistrement (AE), qui définit le régime de responsabilité et les obligations des parties. En particulier, l'Autorité d'Enregistrement s'engage à exercer l'enregistrement dans le respect de la réglementation en vigueur et des procédures définies dans les Politiques de Certification, notamment en ce qui concerne l'identification personnelle certaine des personnes qui signent la demande de certification numérique et à transmettre les résultats de ces activités à InfoCert.
Le Propriétaire est responsable de la véracité des données communiquées lors de la demande d'enregistrement et de certification. Si, au moment de l'identification, il a dissimulé sa véritable identité ou déclaré de façon mensongère être une autre personne – également en utilisant de faux documents personnels – ou, si, en tout état de cause, il a agi de manière à compromettre le processus d'identification et les résultats connexes indiqués dans le certificat, il sera tenu pour responsable de tout dommage découlant de l'inexactitude des informations contenues dans le certificat pour le Certificateur et/ou pour des tiers, avec obligation de préserver et de dégager le Certificateur contre toute demande de dommages-intérêts.
Le Propriétaire et le Demandeur sont également responsables des dommages subis par le Certificateur et/ou les tiers en cas de retard de leur part dans l'activation des procédures prévues au point 4.9. de la présente Politique de Certification (révocation et suspension du certificat).

9.7 Limites de garantie

Le Certificateur ne fournit aucune garantie (i) sur le bon fonctionnement et la sécurité du matériel et des logiciels utilisés par le Propriétaire ; (ii) sur des utilisations de la clé privée, du dispositif de signature sécurisé – le cas échéant – et/ou du certificat de signature, autres que ceux prévus par la réglementation en vigueur et par la présente Politique de Certification ; (iii) sur le fonctionnement normal et continu des lignes électriques et téléphoniques nationales et/ou internationales ; (iv) sur la validité et la pertinence, y compris la valeur probante, du certificat de signature ou de tout message, acte ou document qui lui est associé ou qui est accompli à l'aide des clés auxquelles se réfère le certificat, sans préjudice de l'efficacité de la signature manuscrite reconnue comme signature électronique qualifiée, conformément à l'article 25 du règlement (UE) n° 910/2014 ; (v) sur la confidentialité et/ou l'intégrité de tout message, acte ou document associé au certificat de signature ou accompli à l'aide des clés auxquelles se réfère le certificat (en ce sens que toute violation de cette dernière est, en principe, détectable par le Propriétaire ou par le destinataire grâce à la procédure de vérification spécifique).
Le Certificateur garantit uniquement le fonctionnement du Service, selon les niveaux indiqués au point 9.17 de la Politique de Certification.

9.8 Limites de responsabilité

Le Certificateur n'assume aucune obligation de contrôle quant au contenu, au type ou au format électronique des documents et/ou, le cas échéant, des *hash* transmis par la procédure informatisée indiquée par le Demandeur ou le Propriétaire, en n'assumant aucune responsabilité quant à leur validité et au fait qu'ils sont issus de la volonté réelle du Propriétaire.
Sans préjudice des cas de dol ou de négligence, le Certificateur n'est pas responsable des dommages directs ou indirects subis par les Propriétaires et/ou les tiers du fait de l'utilisation ou de la non-utilisation des certificats de signature délivrés conformément aux dispositions de la présente Politique de Certification et des conditions générales des services de certification.
InfoCert n'est responsable d'aucun dommage direct et/ou indirect découlant également à titre subsidiaire (i) de la perte, (ii) d'une conservation inadéquate, (iii) d'une utilisation impropre, des outils d'identification et d'authentification et/ou (iv) du non-respect de ce qui précède, par le Propriétaire.
En outre, le Certificateur ne répond pas d'éventuels dommages et/ou retards dus à un dysfonctionnement ou à un blocage du système informatique et du réseau internet ; ce, à partir du moment où le contrat de services de certification est établi, mais également tout au long de son exécution.
Sauf en cas de dol ou de négligence, InfoCert ne sera soumise à aucune obligation et ne saura être tenue responsable en cas de dommages directs ou indirects, quelles que soient leur nature et leur ampleur, pouvant survenir au Propriétaire, au Demandeur et/ou à des tiers du fait d'altérations ou d'interventions sur le service ou l'équipement par des tiers non autorisés par InfoCert.

9.9 Indemnités

InfoCert est responsable de tout dommage directement provoqué, par dol ou négligence, à toute personne physique ou morale, résultant du non-respect des obligations découlant du règlement (UE) 910/2014 du Parlement européen et du Conseil du 23 juillet 2014 et du fait qu'InfoCert n'aurait pas pris toutes les mesures appropriées pour éviter le dommage en question.

Dans le cas visé à l'alinéa précédent, le Demandeur ou le Propriétaire aura le droit d'obtenir un montant en réparation des dommages directement subis du fait des comportements visés à l'alinéa précédent. La somme en question ne pourra en aucun cas dépasser les valeurs maximales prévues par l'article 3, alinéa 7, du règlement joint à l'avis n° 185/2017, pour chaque sinistre et par an.

Aucun remboursement ne pourra être demandé si le défaut d'utilisation du service est dû à une utilisation abusive du service de certification ou à l'opérateur du réseau de télécommunication ou à des circonstances imprévisibles, à des cas de force majeure ou à des causes non imputables à InfoCert, telles que des grèves, des émeutes, des tremblements de terre, des actes de terrorisme, des soulèvements populaires, des sabotages organisés, des événements chimiques et/ou bactériologiques, des guerres, des inondations, des mesures prises par les autorités compétentes en la matière ou l'inadéquation des structures, des machines matérielles et/ou des logiciels utilisés par le Demandeur

9.10 Terme et résiliation

9.10.1 Terme

Au terme de la relation entre l'AC et le Sujet, entre l'AC et l'AE, ou entre l'AC et le Demandeur, le certificat est révoqué. La durée du contrat de certification entre le Certificateur et le Sujet est la même que celle du certificat de signature indiqué dans le champ *« validity »* (validité) de ce dernier.
Avant la date d'expiration, le Propriétaire peut demander le renouvellement du certificat, selon la procédure indiquée dans la présente Politique de Certification. Le renouvellement entraîne la prolongation du contrat de certification jusqu'à l'expiration ou la révocation du certificat renouvelé et implique le paiement des montants fixés pour ce service. Un certificat expiré ou révoqué ne peut pas être renouvelé.

9.10.2 Résiliation

L'efficacité du contrat est subordonnée à l'issue positive de l'identification du Propriétaire. En cas d'issue négative de l'identification, le certificat numérique ne sera donc pas délivré par le Certificateur ou, s'il est délivré, il sera considéré comme dépourvu d'effet dès sa délivrance et le contrat sera réputé résilié de plein droit.
Le contrat sera résilié de plein droit avec interruption simultanée du Service et révocation du certificat délivré, au cas où le Propriétaire et/ou le Demandeur enfreindrait les dispositions des clauses du contrat visées à l'article 3 (Responsabilité du Propriétaire et du Demandeur) ; article 4.6 (Propriété intellectuelle), article 8 (Obligations du Propriétaire) ; article 11 (Montants), article 12.3 (Obligation de notifier les cas et les raisons de la suspension et de la révocation du certificat) ; le cas échéant, article 45 (Obligations supplémentaires du Propriétaire et du Demandeur) et, le cas échéant, article 47 (Obligations supplémentaires du Propriétaire), ainsi que les clauses prévues par la présente Politique de Certification. La résiliation interviendra de plein droit lorsque la partie concernée déclarera à l'autre partie, par courrier électronique certifié ou par lettre recommandée avec accusé de réception, qu'il entend se prévaloir de cette clause.
Dans le cas où le Propriétaire est un consommateur, les litiges en droit civil relatifs au contrat conclu par le consommateur sont soumis à la compétence territoriale obligatoire de la juridiction du lieu de résidence ou du domicile de ce dernier.
Le consommateur peut utiliser, sur une base volontaire, les méthodes de résolution extrajudiciaire des litiges prévues par le Code de la consommation italien et les autres lois applicables en la matière.
Nous vous informons également qu'en vertu du règlement (UE) n° 524/2013, pour la résolution des litiges relatifs aux contrats en ligne et aux services offerts en ligne, il est possible d'avoir recours à la procédure de règlement en ligne des litiges (RLL), prévue par la Commission européenne et disponible au lien suivant : https://webgate.ec.europa.eu/odr/ .
Le Certificateur a le droit de se rétracter du contrat de services de certification à tout moment, moyennant un préavis de 30 jours et, par conséquent, de révoquer le certificat.
Dans tous les cas où le Propriétaire ou le Demandeur manque à ses obligations, le Certificateur peut suspendre la prestation de services, y compris en suspendant le certificat. En particulier, en cas de non-paiement du prix du service, InfoCert aura quoi qu'il en soit le droit de résilier le contrat avec le Demandeur et le Propriétaire à tout moment, sans préavis ni frais, et par conséquent de révoquer tout certificat délivré.

En cas de rétractation de la part du Propriétaire ou de révocation du certificat, dans tous les cas, le prix est dû, s'il a déjà été payé, la somme est intégralement conservée par InfoCert également au titre du prix à payer pour la rétractation.
Dans tous les cas de résiliation, de cessation de l'efficacité du contrat et de sa dissolution, les effets produits par le contrat jusqu'à ce moment-là resteront valables.
Le Propriétaire reconnaît qu'en cas de cessation du contrat, pour quelque raison que ce soit, il ne sera plus possible d'utiliser le service.

9.10.3 Effets de la résiliation

La résiliation entraîne la révocation immédiate du certificat.

9.11 Canaux de communication officiels

Il convient de se référer aux canaux de contact du paragraphe 1.5.1.

9.12 Révision de la Politique de Certification

L'AC se réserve le droit d'apporter des modifications au présent document en raison d'exigences techniques ou de changements de procédures dus à des dispositions légales ou réglementaires ou à des optimisations du cycle de travail. Chaque nouvelle version de la Politique de Certification annule et remplace les versions précédentes, qui restent toutefois applicables aux certificats délivrés pendant leur validité, ce, jusqu'à leur première expiration.

Les changements qui n'ont pas d'impact significatif sur les utilisateurs entraînent la progression du numéro d'édition du document, tandis que les changements ayant un impact significatif sur les utilisateurs (tels que des changements significatifs dans les procédures opérationnelles) entraînent la progression du numéro de version du document. Dans tous les cas, la Politique de Certification sera publiée rapidement et mise à disposition selon les modalités prévues. Toute modification technique ou de procédure apportée à la présente Politique de Certification sera communiquée sans délai à l'AE.
En cas de changements importants, l'AC doit se soumettre à un audit d'un OEC accrédité, présenter le rapport de certification (REC – Rapport d'évaluation de la conformité) ainsi que la Politique de Certification à l'Autorité de Contrôle (AgID) et attendre l'autorisation de publication.

9.12.1 Historique des révisions

Version/n° d'édition	**4.2**
Date de version/d'édition :	24/03/2020
Description des modifications :	§ 5.1.1 Mise à jour technologique et références aux services hébergés sur le cloud AWS § 5.1.6 Mise à jour technologique des supports de stockage § Appendice A – insertion de la nouvelle *Electronic Signature Qualified*

	Root « InfoCert Qualified Electronic Signature CA 4 »
Raisons :	Nouvelle AC racine

Version/n° d'édition	**4.1**
Date de version/d'édition :	10/10/2019
Description des modifications :	§ 3.1.5 Ajout de la possibilité d'utiliser comme identifiant unique les identifiants prévus par le document eIDAS « eID Profile » du réseau de coopération EiDAS
Raisons :	-

Version/n° d'édition	**4.0** (version jamais publiée, mises à jour signalées dans la version 4.1)
Date de version/d'édition :	14/06/2019
Description des modifications :	Corrections formelles, mise à jour des définitions, acronymes, références $ 1.2 Mise à jour de la version du document, description OID agIDcert § 1.3.5 Mise à jour pour les mineurs $ 1.6.1 Introduction définitions Certificats OneShot, Certificats LongTerm et domaine informatique § 2.2.3 Mise à jour des points de distribution des LCR § 3.1.1 Mise à jour pour avis de l'AgID n° 121/2019 § 3.1.5 Mise à jour pour avis de l'AgID n° 121/2019 § 3.2.6 Description plus claire § 4.3.1.5 Description des certificats délivrés à des fins de tests $4.5.3 Ajout limite d'utilisation pour délivrance avec SPID et mise à jour de la description de la valeur limite § 4.9.2 Description plus claire $ 5.1.1 Clarification concernant l'emplacement du centre de données $ 5.3.7 Établie la description des accès physiques $ 5.4.1 Ajout de description des journaux d'accès physiques et logiques Regroupement des paragraphes suivants des deux manuels : • $ 2.2.2 Publication des certificats • $ 3.1.3 Anonymat et pseudonymat des demandeurs • $ 3.2.3.4 Reconnaissance effectuée selon la procédure 4 – AUTID • $ 4.1.1 Qui peut demander un certificat • $ 4.3.2 Notification aux demandeurs que le certificat a été

	délivré • $ 4.4.2 Publication du certificat de la part de l'Autorité de Certification • $ 4.5.1 Utilisation de la clé privée et du certificat de la part du Sujet • $ 4.6.1 Raisons du renouvellement • $ 4.9.3 Procédures de demande de révocation • $ 4.9.15 Procédures de demande de suspension • $ 6.1.1 Génération de la bi-clé du Sujet • $ 6.1.2 Remise de la clé privée au Demandeur • $ 6.1.4 Remise de la clé publique aux utilisateurs • $ 6.2.7 Stockage de la clé privée dans un module cryptographique • $ 9.1.1 Tarifs pour la délivrance et le renouvellement des certificats • $ 9.4.5 Politique de confidentialité et consentement au traitement des données à caractère personnel • $ 9.10.2 Résolution
Raisons :	Fusion de ICERT-INDI-MO, version 3.5 du 30/11/2018 et de ICERT-INDI-MO-ENT, version 3.5 du 30/11/2018. Mise à jour de l'avis de l'Agid n° 121/2019. Clarifications.

Version/n° d'édition	**3.5**
Date de version/d'édition :	30/11/2018
Description des modifications :	$ 1.2 Mise à jour de l'OID et description § 1.3 Mise à jour de la dénomination sociale du groupe $ 3.2.6 Identification de la personne morale PSP dans le cadre de la DSP2 $ 4.2.1.2 Informations sur la personne morale dans le cadre de la DSP2 $ 4.9 Demande de révocation de la part de l'ANC pour DSP2 Corrections typographiques et références
Raisons :	Délivrance de certificats de cachet QSealC conformément à la directive DSP2 Changement de dénomination sociale TecnoInvestimenti

Version/n° d'édition	**3.4**
Date de version/d'édition :	20/06/2018

Description des modifications :	§ 1.5.1 Changement du numéro du centre d'appel § 9.2.1 Mise à jour des plafonds de la couverture d'assurance
Raisons :	-

Version/n° d'édition	**3.3**
Date de version/d'édition :	04/09/2018
Description des modifications :	Chap. 1 Correction de « signature numérique » en « signature électronique qualifiée ». Quelques corrections terminologiques pour une meilleure compréhension, ajout de quelques définitions de termes utilisés dans le document § 3.1.5 Réécriture partielle du paragraphe pour une meilleure compréhension § 3.2.3 Réécriture du tableau et des sous-paragraphes pour une meilleure clarté du contenu et une contextualisation sur les marchés européens. Extension de la procédure 4 AutID aux moyens de l'identification électronique des États membres. Définition d'un document spécifique avec les types de documents et les moyens d'identification électronique acceptés § 4.2 Réécriture partielle du paragraphe pour une meilleure compréhension et contextualisation sur les marchés européens § 4.2.2 Systèmes d'authentification supplémentaires § 4.3.3.2 Possibilité de délivrance un certificat déjà actif § 4.5.3 Insertion d'une limite d'utilisation supplémentaire § 4.9.15 et 4.9.16 Suspension et réactivation via CMS § 9.4 Ajout de références au RGPD § 9.6, § 9.7, § 9.8, § 9.9, § 9.10 réécriture de certains paragraphes pour une meilleure contextualisation Certificats utilisateur : Ajout des certificats de personne morale sur QSCD, correction de certaines erreurs
Raisons :	-

Version/n° d'édition	**3.2**

Date de version/d'édition :	02/05/2017
Description des modifications :	Ajout d'informations concernant l'AC « InfoCert Firma Qualificata 2 » Ajout de certains OID relatifs à l'AC « InfoCert Firma Qualificata 2 » Correction d'ordre stylistique et orthographique
Raisons :	

Version/n° d'édition	**3.1**
Date de version/d'édition :	27/01/2017
Description des modifications :	§3.2.3 Élimination de toutes les références SPID comme outil d'authentification pour l'identification §3.2.3.1 Spécification de la reconnaissance par l'employeur § 4.8.12 Description de la procédure de réactivation de la suspension
Raisons :	-

Version/n° d'édition	**3.0**
Date de version/d'édition :	12/12/2016
Description des modifications :	Sans objet.
Raisons :	Nouvelle édition du document

9.12.2 Procédures de révision

Les procédures de révision de la Politique de Certification sont similaires aux procédures de rédaction. Les révisions sont effectuées de concert avec le Responsable du Service de Certification, le Responsable de la Sécurité, le Responsable de la Protection de la Vie Privée, le Service Juridique et le Département de Conseil, et sont approuvées par la direction.

9.12.3 Durée et mécanisme de notification

La Politique de Certification est publiée :

- en format électronique sur le site web du PSC (adresse : http://www.firma.infocert.it/doc/manuali.htm) ;
- en format électronique dans la liste publique des certificateurs tenue par l'AgID ;
- en format papier ; elle alors peut être demandée à l'Autorité d'Enregistrement ou au contact pour l'utilisateur final.

9.12.4 Cas dans lesquels l'OID doit changer

Sans objet.

9.13 Résolution des litiges

Il convient de se référer aux contrats régissant le service pour connaître en détail les façons de résoudre les litiges.

9.14 Juridiction compétente

Pour les consommateurs, la juridiction compétente est le tribunal de la ville où le consommateur est domicilié. Pour les entités autres que les consommateurs, la juridiction compétente est Rome. Dans les accords entre l'AC et l'AE, entre l'AC et le Demandeur ou entre l'AC et le Sujet, une juridiction différente peut être définie.

9.15 Loi applicable

La loi applicable à cette Politique de Certification est la loi italienne.

Ci-dessous est présentée une liste non exhaustive des principales références réglementaires applicables :

[1] Règlement (UE) 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 (également appelé « règlement eIDAS »).
[2] Décret législatif italien n° 82 du 7 mars 2005 (Journal officiel italien n° 112 du 16 mai 2005) – Code de l'administration numérique (également appelé *CAD*) tel que modifié et complété.
[3] *inutilisé*
[4] Décret législatif italien n° 196 du 30 juin 2003 (Journal officiel italien n° 174 du 29 juillet 2003) – Code de confidentialité tel que modifié et complété et règlement (UE) 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 (en vigueur depuis le 25 mai 2018).
[5] *inutilisé*.
[6] *inutilisé*
[7] Directive 2011/83/UE du Parlement européen et du Conseil du 25 octobre 2011 relative aux droits des consommateurs et législation nationale la transposant.
[8] Vérification préliminaire – 24 septembre 2015 [4367555] Traitement des données à caractère personnel dans le cadre du « Processus de délivrance avec reconnaissance par webcam » pour la signature électronique qualifiée ou numérique.
[9] Résolution CNIPA n° 45 du 21 mai 2009, telle que modifiée par les avis ultérieurs (remplacée par [13] depuis le 5 juillet 2019).
[10] Avis de l'AgID n° 189/2017.
[11] Directive 2015/2366/UE du Parlement européen et du Conseil du 25 novembre 2015

connue sous le nom de Directive sur les services de paiement – DSP2.
[12] Règlement délégué (UE) 2018/389 de la Commission du 27 novembre 2017 complétant la Directive (UE) 2015/2366 du Parlement européen et du Conseil par des normes techniques de réglementation relative à l'authentification forte du client et à des normes ouvertes communes et sécurisées de communication.
[13] Avis de l'AgID n° 121/2019 version 1.1 (remplace la délibération CNIPA n° 45/2009).

Toutes les circulaires et résolutions de l'[7]Autorité de Contrôle, ainsi que les actes d'exécution prévus dans le règlement eIDAS [1], sont également applicables.

9.16 Dispositions diverses

Il convient de se référer aux contrats régissant le service pour toute autre disposition ne figurant pas dans la présente Politique de Certification.

9.17 Autres dispositions

Les horaires de prestation de services sont les suivants (sauf accord contractuel contraire) :

Service	Horaire
Accès aux archives publiques des certificats (y compris les certificats, les LCR et l'OCSP).	De 0 h 00 à 24 h 00 7 jours sur 7 (disponibilité minimale 99 %)
Demande de révocation et de suspension des certificats.	De 0 h 00 à 24 h 00 7 jours sur 7 (disponibilité minimale 99 %)
Autres activités : enregistrement, génération, publication, renouvellement[8].	De 9 h 00 à 17 h 00 du lundi au vendredi, sauf les jours fériés De 9 h 00 à 13 h 00 le samedi
Demande et/ou vérification d'horodatage.	24 h/24, 7j/7 (disponibilité minimale 99 %)

[7] Disponibles à l'adresse suivante : https://www.agid.gov.it/index.php/it/piattaforme/firma-elettronica-qualificata.

[8] L'enregistrement est effectué auprès des Autorités d'Enregistrement qui peuvent avoir des horaires de guichet différents. En tout état de cause, InfoCert garantit la prestation de ses services aux heures mentionnées ci-dessus.

Appendice A

Electronic Signature Qualified Root « InfoCert Firma Qualificata 2 »

```
  0 1318: SEQUENCE {
  4 1038:   SEQUENCE {
  8    3:     [0] {
 10    1:       INTEGER 2
       :       }
 13    1:     INTEGER 1
 16   13:     SEQUENCE {
 18    9:       OBJECT IDENTIFIER
       :         sha256WithRSAEncryption (1 2 840 113549 1 1 11)
 29    0:       NULL
       :       }
 31  133:     SEQUENCE {
 34   11:       SET {
 36    9:         SEQUENCE {
 38    3:           OBJECT IDENTIFIER countryName (2 5 4 6)
 43    2:           PrintableString 'IT'
       :           }
       :         }
 47   21:       SET {
 49   19:         SEQUENCE {
 51    3:           OBJECT IDENTIFIER organizationName (2 5 4 10)
 56   12:           UTF8String 'INFOCERT SPA'
       :           }
       :         }
 70   34:       SET {
 72   32:         SEQUENCE {
 74    3:           OBJECT IDENTIFIER organizationalUnitName (2 5 4 11)
 79   25:           UTF8String 'Certificatore Accreditato'
       :           }
       :         }
106   20:       SET {
108   18:         SEQUENCE {
110    3:           OBJECT IDENTIFIER serialNumber (2 5 4 5)
115   11:           PrintableString '07945211006'
       :           }
       :         }
128   37:       SET {
130   35:         SEQUENCE {
132    3:           OBJECT IDENTIFIER commonName (2 5 4 3)
137   28:           UTF8String 'InfoCert Firma Qualificata 2'
       :           }
       :         }
       :       }
167   30:     SEQUENCE {
169   13:       UTCTime 19/04/2013 14:26:15 GMT
184   13:       UTCTime 19/04/2029 15:26:15 GMT
       :       }
199  133:     SEQUENCE {
202   11:       SET {
204    9:         SEQUENCE {
206    3:           OBJECT IDENTIFIER countryName (2 5 4 6)
211    2:           PrintableString 'IT'
       :           }
       :         }
215   21:       SET {
217   19:         SEQUENCE {
219    3:           OBJECT IDENTIFIER organizationName (2 5 4 10)
224   12:           UTF8String 'INFOCERT SPA'
       :           }
       :         }
238   34:       SET {
240   32:         SEQUENCE {
242    3:           OBJECT IDENTIFIER organizationalUnitName (2 5 4 11)
247   25:           UTF8String 'Certificatore Accreditato'
       :           }
```

```
      :         }
274   20:       SET {
276   18:         SEQUENCE {
278    3:           OBJECT IDENTIFIER serialNumber (2 5 4 5)
283   11:           PrintableString '07945211006'
      :           }
      :         }
296   37:       SET {
298   35:         SEQUENCE {
300    3:           OBJECT IDENTIFIER commonName (2 5 4 3)
305   28:           UTF8String 'InfoCert Firma Qualificata 2'
      :           }
      :         }
      :       }
335  290:     SEQUENCE {
339   13:       SEQUENCE {
341    9:         OBJECT IDENTIFIER rsaEncryption (1 2 840 113549 1 1 1)
352    0:         NULL
      :         }
354  271:       BIT STRING, encapsulates {
359  266:         SEQUENCE {
363  257:           INTEGER
      :             00 C5 A1 6E 5E 03 49 37 01 C5 3E FE FD AE 29 C9
      :             44 84 6A F1 5E 5A 8E 52 9B 40 40 92 D2 8F 2B 0F
      :             EC 86 8A 2A D1 B1 21 E5 FC 1C D6 AF C5 16 83 90
      :             B9 10 34 49 6A 97 EB 78 1A 02 0F C8 99 38 97 31
      :             DB 1F BD 9C D4 BB 36 48 7D 3A 5F BB 82 A3 98 86
      :             44 7D FE 15 4D 52 71 B7 2B CE F8 80 3C 1F B2 7A
      :             A5 19 D5 C2 A4 1B 2C 86 43 5C 01 B2 8A F1 A5 11
      :             14 79 A8 E4 5B 6C 2C 0E 26 3F 0D 8C 9E 4C 6D 48
      :                 [ Another 129 bytes skipped ]
624    3:           INTEGER 65537
      :           }
      :         }
      :       }
629  413:     [3] {
633  409:       SEQUENCE {
637   15:         SEQUENCE {
639    3:           OBJECT IDENTIFIER basicConstraints (2 5 29 19)
644    1:           BOOLEAN TRUE
647    5:           OCTET STRING, encapsulates {
649    3:             SEQUENCE {
651    1:               BOOLEAN TRUE
      :               }
      :             }
      :           }
654   88:         SEQUENCE {
656    3:           OBJECT IDENTIFIER certificatePolicies (2 5 29 32)
661   81:           OCTET STRING, encapsulates {
663   79:             SEQUENCE {
665   77:               SEQUENCE {
667    4:                 OBJECT IDENTIFIER anyPolicy (2 5 29 32 0)
673   69:                 SEQUENCE {
675   67:                   SEQUENCE {
677    8:                     OBJECT IDENTIFIER cps (1 3 6 1 5 5 7 2 1)
687   55:                     IA5String
      :                     'http://www.firma.infocert.it/documentazione/manu'
      :                     'ali.php'
      :                     }
      :                   }
      :                 }
      :               }
      :             }
      :           }
744   37:         SEQUENCE {
746    3:           OBJECT IDENTIFIER issuerAltName (2 5 29 18)
751   30:           OCTET STRING, encapsulates {
753   28:             SEQUENCE {
755   26:               [1] 'firma.digitale@infocert.it'
      :               }
      :             }
      :           }
783  213:         SEQUENCE {
786    3:           OBJECT IDENTIFIER cRLDistributionPoints (2 5 29 31)
791  205:           OCTET STRING, encapsulates {
794  202:             SEQUENCE {
```

```
 797  199:               SEQUENCE {
 800  196:                 [0] {
 803  193:                   [0] {
 806   42:                     [6]
       :                     'http://crl.infocert.it/crls/firma2/ARL.crl'
 850  146:                     [6]
       :                     'ldap://ldap.infocert.it/cn%3DInfoCert%20Firma%20'
       :                     'Qualificata%202,ou%3DCertificatore%20Accreditato'
       :                     ',o%3DINFOCERT%20SPA,c%3DIT?authorityRevocationLi'
       :                     'st'
       :                     }
       :                   }
       :                 }
       :               }
       :             }
 999   14:           SEQUENCE {
1001    3:             OBJECT IDENTIFIER keyUsage (2 5 29 15)
1006    1:             BOOLEAN TRUE
1009    4:             OCTET STRING, encapsulates {
1011    2:               BIT STRING 1 unused bit
       :                 '1100000'B
       :               }
       :             }
1015   29:           SEQUENCE {
1017    3:             OBJECT IDENTIFIER subjectKeyIdentifier (2 5 29 14)
1022   22:             OCTET STRING, encapsulates {
1024   20:               OCTET STRING
       :                 93 DD 21 FC 03 D0 15 0A 72 AD A3 CC D5 9A 09 9D
       :                 38 8B 9D E9
       :               }
       :             }
       :           }
       :         }
       :       }
1046   13:   SEQUENCE {
1048    9:     OBJECT IDENTIFIER sha256WithRSAEncryption (1 2 840 113549 1 1 11)
1059    0:     NULL
       :     }
1061  257:   BIT STRING
       :     96 1D 20 03 BC 24 21 EB F5 D4 D3 FE 4A 72 E4 06
       :     69 82 8F 17 A0 84 16 FE AF 6D 35 03 F0 66 47 5D
       :     FD B0 1F 80 B8 9B A2 5B DB 93 B6 53 B2 25 65 56
       :     FD F9 05 BF 6B 84 CE 7C 48 A3 F5 5D AF 5C DB A0
       :     9F F3 2E 33 86 8A 65 55 B8 5F 29 11 95 08 B8 F5
       :     BB 51 17 74 F8 42 51 06 FC 59 67 0C D0 0C 8B 39
       :     78 F7 AA 16 CC 87 BE D4 2F 42 BD 79 A4 6B C1 30
       :     04 35 B9 78 DC 9C BA E4 73 C7 B9 B3 67 93 D5 3D
       :             [ Another 128 bytes skipped ]
     : }
```

Electronic Signature Qualified Root ”InfoCert Qualified Electronic Signature CA 3”

```
   0 1881: SEQUENCE {
   4 1345:   SEQUENCE {
   8    3:     [0] {
  10    1:       INTEGER 2
       :       }
  13    1:     INTEGER 1
  16   13:     SEQUENCE {
  18    9:       OBJECT IDENTIFIER
       :         sha256WithRSAEncryption (1 2 840 113549 1 1 11)
  29    0:       NULL
       :       }
  31  165:     SEQUENCE {
  34   11:       SET {
  36    9:         SEQUENCE {
  38    3:           OBJECT IDENTIFIER countryName (2 5 4 6)
  43    2:           PrintableString 'IT'
       :           }
       :         }
  47   24:       SET {
  49   22:         SEQUENCE {
```

```
 51    3:           OBJECT IDENTIFIER organizationName (2 5 4 10)
 56   15:           UTF8String 'InfoCert S.p.A.'
       :           }
       :         }
 73   41:       SET {
 75   39:         SEQUENCE {
 77    3:           OBJECT IDENTIFIER organizationalUnitName (2 5 4 11)
 82   32:           UTF8String 'Qualified Trust Service Provider'
       :           }
       :         }
116   26:       SET {
118   24:         SEQUENCE {
120    3:           OBJECT IDENTIFIER '2 5 4 97'
125   17:           UTF8String 'VATIT-07945211006'
       :           }
       :         }
144   53:       SET {
146   51:         SEQUENCE {
148    3:           OBJECT IDENTIFIER commonName (2 5 4 3)
153   44:           UTF8String
       :             'InfoCert Qualified Electronic Signature CA 3'
       :           }
       :         }
       :       }
199   30:     SEQUENCE {
201   13:       UTCTime 12/12/2016 16:34:43 GMT
216   13:       UTCTime 12/12/2032 17:34:43 GMT
       :       }
231  165:     SEQUENCE {
234   11:       SET {
236    9:         SEQUENCE {
238    3:           OBJECT IDENTIFIER countryName (2 5 4 6)
243    2:           PrintableString 'IT'
       :           }
       :         }
247   24:       SET {
249   22:         SEQUENCE {
251    3:           OBJECT IDENTIFIER organizationName (2 5 4 10)
256   15:           UTF8String 'InfoCert S.p.A.'
       :           }
       :         }
273   41:       SET {
275   39:         SEQUENCE {
277    3:           OBJECT IDENTIFIER organizationalUnitName (2 5 4 11)
282   32:           UTF8String 'Qualified Trust Service Provider'
       :           }
       :         }
316   26:       SET {
318   24:         SEQUENCE {
320    3:           OBJECT IDENTIFIER '2 5 4 97'
325   17:           UTF8String 'VATIT-07945211006'
       :           }
       :         }
344   53:       SET {
346   51:         SEQUENCE {
348    3:           OBJECT IDENTIFIER commonName (2 5 4 3)
353   44:           UTF8String
       :             'InfoCert Qualified Electronic Signature CA 3'
       :           }
       :         }
       :       }
399  546:     SEQUENCE {
403   13:       SEQUENCE {
405    9:         OBJECT IDENTIFIER rsaEncryption (1 2 840 113549 1 1 1)
416    0:         NULL
       :         }
418  527:       BIT STRING, encapsulates {
423  522:         SEQUENCE {
427  513:           INTEGER
       :             00 B7 C1 D3 BF 11 CB A8 28 B6 91 DD E1 11 85 9F
       :             9D 9A 51 25 B3 B2 BC B2 AE AD DF 3E 5D 9F 5A A0
       :             F9 E4 64 C8 34 40 DA AB 7A EC 98 62 05 38 EC 91
       :             EA 84 F9 07 E6 58 DE 58 34 A0 EB 0D 11 19 50 BA
       :             E9 C0 13 C7 60 08 DB E5 AE 00 50 E9 7C 10 16 09
       :             9E 4D F4 EC 7B 14 99 6F D0 A4 67 68 CD 7D 88 1E
       :             D1 3E DA 25 BC 3C 66 61 8D B6 5D D6 F8 CF BA 7A
```

```
        :             55 96 86 62 CC 3F 9D D1 B0 2B 58 03 A7 21 49 BC
        :                   [ Another 385 bytes skipped ]
 944    3:           INTEGER 65537
        :           }
        :         }
        :       }
 949  400:     [3] {
 953  396:       SEQUENCE {
 957   15:         SEQUENCE {
 959    3:           OBJECT IDENTIFIER basicConstraints (2 5 29 19)
 964    1:           BOOLEAN TRUE
 967    5:           OCTET STRING, encapsulates {
 969    3:             SEQUENCE {
 971    1:               BOOLEAN TRUE
        :               }
        :             }
        :           }
 974   88:         SEQUENCE {
 976    3:           OBJECT IDENTIFIER certificatePolicies (2 5 29 32)
 981   81:           OCTET STRING, encapsulates {
 983   79:             SEQUENCE {
 985   77:               SEQUENCE {
 987    4:                 OBJECT IDENTIFIER anyPolicy (2 5 29 32 0)
 993   69:                 SEQUENCE {
 995   67:                   SEQUENCE {
 997    8:                     OBJECT IDENTIFIER cps (1 3 6 1 5 5 7 2 1)
1007   55:                     IA5String
        :                     'http://www.firma.infocert.it/documentazione/manu'
        :                     'ali.php'
        :                     }
        :                   }
        :                 }
        :               }
        :             }
        :           }
1064  239:         SEQUENCE {
1067    3:           OBJECT IDENTIFIER cRLDistributionPoints (2 5 29 31)
1072  231:           OCTET STRING, encapsulates {
1075  228:             SEQUENCE {
1078  225:               SEQUENCE {
1081  222:                 [0] {
1084  219:                   [0] {
1087   37:                     [6] 'http://crl.infocert.it/ca3/qc/ARL.crl'
1126  177:                     [6]
        :                     'ldap://ldap.infocert.it/cn%3DInfoCert%20Qualifie'
        :                     'd%20Electronic%20Signature%20CA%203,ou%3DQualifi'
        :                     'ed%20Trust%20Service%20Provider,o%3DINFOCERT%20S'
        :                     'PA,c%3DIT?authorityRevocationList'
        :                     }
        :                   }
        :                 }
        :               }
        :             }
        :           }
1306   14:         SEQUENCE {
1308    3:           OBJECT IDENTIFIER keyUsage (2 5 29 15)
1313    1:           BOOLEAN TRUE
1316    4:           OCTET STRING, encapsulates {
1318    2:             BIT STRING 1 unused bit
        :               '1100000'B
        :             }
        :           }
1322   29:         SEQUENCE {
1324    3:           OBJECT IDENTIFIER subjectKeyIdentifier (2 5 29 14)
1329   22:           OCTET STRING, encapsulates {
1331   20:             OCTET STRING
        :               9B 3B 1B 18 6A 3E A2 04 03 F4 D7 99 10 CF 97 11
        :               4C F1 AA DE
        :             }
        :           }
        :         }
        :       }
        :     }
1353   13:   SEQUENCE {
1355    9:     OBJECT IDENTIFIER sha256WithRSAEncryption (1 2 840 113549 1 1 11)
1366    0:     NULL
```

```
        :     }
1368  513:   BIT STRING
        :     54 49 DC F3 76 1F BF 5D 33 B7 78 3A 26 72 4B 2B
        :     50 79 22 70 4A 7E DA EB 8F 26 3C 7F 8D CB 08 8E
        :     96 A6 EB 00 93 5D 82 1D 48 C8 E0 FF C6 1D 69 32
        :     3F E8 F3 FC 7A C7 9C 33 4B 19 FA 13 37 01 7F 54
        :     12 49 A3 51 19 6C 3B 0C 50 F1 D2 97 83 7B CF 4F
        :     58 F4 82 27 98 FB C7 11 97 B8 D7 FC 73 F2 96 41
        :     D1 13 25 07 5A 77 B1 E4 BE 6C 0E BD FA D8 CA 58
        :     5B DC 4B 08 4F EC CC 9F CD E9 E8 9E 7D 43 27 4D
        :             [ Another 384 bytes skipped ]
        :   }
```

Electronic Signature Qualified Root ”InfoCert Qualified Electronic Signature CA 4”

```
  0 1693: SEQUENCE {
  4 1157:   SEQUENCE {
  8    3:     [0] {
 10    1:       INTEGER 2
       :       }
 13    1:     INTEGER 1
 16   13:     SEQUENCE {
 18    9:       OBJECT IDENTIFIER
       :         sha256WithRSAEncryption (1 2 840 113549 1 1 11)
 29    0:       NULL
       :       }
 31  165:     SEQUENCE {
 34   11:       SET {
 36    9:         SEQUENCE {
 38    3:           OBJECT IDENTIFIER countryName (2 5 4 6)
 43    2:           PrintableString 'IT'
       :           }
       :         }
 47   24:       SET {
 49   22:         SEQUENCE {
 51    3:           OBJECT IDENTIFIER organizationName (2 5 4 10)
 56   15:           UTF8String 'InfoCert S.p.A.'
       :           }
       :         }
 73   41:       SET {
 75   39:         SEQUENCE {
 77    3:           OBJECT IDENTIFIER organizationalUnitName (2 5 4 11)
 82   32:           UTF8String 'Qualified Trust Service Provider'
       :           }
       :         }
116   26:       SET {
118   24:         SEQUENCE {
120    3:           OBJECT IDENTIFIER '2 5 4 97'
125   17:           UTF8String 'VATIT-07945211006'
       :           }
       :         }
144   53:       SET {
146   51:         SEQUENCE {
148    3:           OBJECT IDENTIFIER commonName (2 5 4 3)
153   44:           UTF8String
       :             'InfoCert Qualified Electronic Signature CA 4'
       :           }
       :         }
       :       }
199   30:     SEQUENCE {
201   13:       UTCTime 23/03/2020 09:21:16 GMT
216   13:       UTCTime 23/03/2036 10:21:16 GMT
       :       }
231  165:     SEQUENCE {
234   11:       SET {
236    9:         SEQUENCE {
238    3:           OBJECT IDENTIFIER countryName (2 5 4 6)
243    2:           PrintableString 'IT'
       :           }
       :         }
247   24:       SET {
249   22:         SEQUENCE {
251    3:           OBJECT IDENTIFIER organizationName (2 5 4 10)
256   15:           UTF8String 'InfoCert S.p.A.'
```

```
        :           }
        :         }
273   41:       SET {
275   39:         SEQUENCE {
277    3:           OBJECT IDENTIFIER organizationalUnitName (2 5 4 11)
282   32:           UTF8String 'Qualified Trust Service Provider'
        :           }
        :         }
316   26:       SET {
318   24:         SEQUENCE {
320    3:           OBJECT IDENTIFIER '2 5 4 97'
325   17:           UTF8String 'VATIT-07945211006'
        :           }
        :         }
344   53:       SET {
346   51:         SEQUENCE {
348    3:           OBJECT IDENTIFIER commonName (2 5 4 3)
353   44:           UTF8String
        :             'InfoCert Qualified Electronic Signature CA 4'
        :           }
        :         }
        :       }
399  546:     SEQUENCE {
403   13:       SEQUENCE {
405    9:         OBJECT IDENTIFIER rsaEncryption (1 2 840 113549 1 1 1)
416    0:         NULL
        :         }
418  527:       BIT STRING, encapsulates {
423  522:         SEQUENCE {
427  513:           INTEGER
        :             00 B3 F6 00 3B 90 01 2E AC 2A 26 9E CB 03 0C 02
        :             E3 8A C3 14 FE F6 22 6B 6B B5 31 8E 44 8B 01 C2
        :             80 46 B8 E9 3B A6 84 84 4A AB 45 D4 60 D5 67 AF
        :             9D 57 BA DC EC AE AE AF 4F DD 71 4C 63 9E E2 81
        :             AF 71 16 A6 D2 4A C7 EE 7B EB 2B A4 18 14 6E 35
        :             C8 33 C6 BF AD 43 F9 10 90 97 73 A0 5C 87 B0 19
        :             5E 1E 87 E7 45 70 BE 68 19 EB 53 34 56 15 A5 D4
        :             84 57 6A AA 69 25 F0 48 1C 3A 59 B6 2B EF D9 68
        :             E3 CA 7D E6 39 30 BC BE 38 55 6A 08 D9 F7 B5 37
        :             8A ED B6 15 25 D3 E8 95 B3 3B 3F 7D B4 4F C0 EB
        :             D5 44 D4 A0 7E 93 4A 37 84 8D 2D 3B A2 77 44 48
        :             BC 29 F0 AE 98 85 0A 04 BE DD 3E 4A 73 BA 09 9A
        :             F9 9C DE B8 29 0D A2 E9 70 01 68 37 CB 53 36 80
        :             7B 04 C3 71 64 FE 20 91 B2 37 A1 B5 C7 B9 15 68
        :             C8 22 C5 C2 D8 DC 5D 7C F6 92 E7 D6 12 4B AA C6
        :             61 A9 C8 F3 FE E6 6C 89 8E A5 28 8A 20 7D D1 1F
        :             A8 D4 34 A2 C0 24 E5 07 BB E3 1F AF 07 5C 46 AB
        :             1C 05 52 92 7B FE C4 C4 BD 87 66 FE 2F 4D F3 D9
        :             20 08 45 81 6E A0 03 A3 6E F7 38 DB A0 76 DD 8C
        :             D1 1F 0A E8 6E DB 6F 55 F0 EE 19 6D E7 AA 63 5C
        :             32 03 43 D1 F5 6C 08 16 93 DC 2D 00 B7 38 30 2F
        :             92 56 02 69 BA 0C 9E E2 B9 31 29 DB 2D 29 27 BF
        :             B1 94 9D 36 EE 2E 6F 2D E6 E8 43 17 93 E1 79 EB
        :             76 03 EB 30 7D 39 01 B0 6E 92 51 8D 1B 75 A3 7C
        :             E6 07 F2 24 96 DA 91 A6 5A AC 14 14 2D 8C 79 9C
        :             F4 CD 5A 78 A6 6A B2 7A 6D 2D 5C 78 91 D6 F6 D1
        :             0D 6E 24 4B A6 81 35 4C 58 E8 CA 21 B5 FA 7F 6C
        :             9A 03 45 51 DA F8 C8 17 2E 6B 95 3D F3 29 C7 DF
        :             80 AC 6D 59 B8 B9 6C 85 9F 9E EC CC 54 76 B4 94
        :             0A 0C 12 93 19 14 B2 E3 87 1D 9C 25 78 4C 9E 75
        :             70 B0 37 5F A9 EF EC 86 FD F8 5A 9B 5F A7 E6 85
        :             9E 5E DD 4A 98 58 86 8C 61 73 1D FF F0 C2 36 98
        :             99
944    3:           INTEGER 65537
        :           }
        :         }
        :       }
949  213:     [3] {
952  210:       SEQUENCE {
955   15:         SEQUENCE {
957    3:           OBJECT IDENTIFIER basicConstraints (2 5 29 19)
962    1:           BOOLEAN TRUE
965    5:           OCTET STRING, encapsulates {
967    3:             SEQUENCE {
969    1:               BOOLEAN TRUE
        :               }
```

```
        :             }
        :           }
 972   88:         SEQUENCE {
 974    3:           OBJECT IDENTIFIER certificatePolicies (2 5 29 32)
 979   81:           OCTET STRING, encapsulates {
 981   79:             SEQUENCE {
 983   77:               SEQUENCE {
 985    4:                 OBJECT IDENTIFIER anyPolicy (2 5 29 32 0)
 991   69:                 SEQUENCE {
 993   67:                   SEQUENCE {
 995    8:                     OBJECT IDENTIFIER cps (1 3 6 1 5 5 7 2 1)
1005   55:                     IA5String
        :                     'http://www.firma.infocert.it/documentazione/manu'
        :                     'ali.php'
        :                     }
        :                   }
        :                 }
        :               }
        :             }
        :           }
1062   54:         SEQUENCE {
1064    3:           OBJECT IDENTIFIER cRLDistributionPoints (2 5 29 31)
1069   47:           OCTET STRING, encapsulates {
1071   45:             SEQUENCE {
1073   43:               SEQUENCE {
1075   41:                 [0] {
1077   39:                   [0] {
1079   37:                     [6] 'http://crl.ca4.infocert.it/qc/ARL.crl'
        :                     }
        :                   }
        :                 }
        :               }
        :             }
        :           }
1118   14:         SEQUENCE {
1120    3:           OBJECT IDENTIFIER keyUsage (2 5 29 15)
1125    1:           BOOLEAN TRUE
1128    4:           OCTET STRING, encapsulates {
1130    2:             BIT STRING 1 unused bit
        :               '1100000'B
        :             }
        :           }
1134   29:         SEQUENCE {
1136    3:           OBJECT IDENTIFIER subjectKeyIdentifier (2 5 29 14)
1141   22:           OCTET STRING, encapsulates {
1143   20:             OCTET STRING
        :               5D 7C 6B 61 E8 AC 90 EB 5E C9 D7 BE B4 E3 34 2E
        :               5C 2B 1C DF
        :             }
        :           }
        :         }
        :       }
1165   13:   SEQUENCE {
1167    9:     OBJECT IDENTIFIER sha256WithRSAEncryption (1 2 840 113549 1 1 11)
1178    0:     NULL
        :     }
1180  513:   BIT STRING
        :     80 F2 2D 1C 50 0B 6C 38 DE 22 99 D7 69 5B 92 95
        :     99 AE FD FD 7A 3A 4D 06 D0 01 E3 CE 56 DC AF 5B
        :     A6 23 EB CD 35 DB 11 C0 72 27 79 E6 7B 91 E6 4F
        :     D5 77 D6 68 E3 D2 48 B3 E9 49 D6 5B D4 57 3F E0
        :     9E 46 E4 0E F4 CF 66 E6 28 6A 91 F1 BE 3F 42 44
        :     0E 75 EB A8 1A D4 24 2C 65 36 9B D5 1E 82 2B 45
        :     29 18 3A CC 91 51 66 69 7D FE 6E E2 63 94 DA E1
        :     E9 82 AE 9B CE 5E B9 7B 7C E3 08 97 94 DB 57 C9
        :     EC D1 9A 71 2B DE 25 2B 85 77 2B 7F 99 97 16 4D
        :     7B 84 A9 DF DA 75 C6 62 8B 3B 65 B3 C3 D7 5C 42
        :     BA AB FB CE 2D 6B AA B6 EB 6E AD EA 84 52 F1 0F
        :     C8 E0 64 9C A1 07 94 9E CF E0 22 E2 D1 3D 71 DD
        :     B5 90 6B D5 69 5E 86 7A BF 4D 6C 50 B5 EC CF 8F
        :     E4 15 DE 37 C8 5F CE 7A 8A 3E 52 C1 DE AB CF 08
        :     1B E9 8D 1D A0 14 8C A7 67 C0 77 3F A4 55 1C F3
        :     7A E9 CE 7D C1 99 BE D0 32 37 81 F9 39 95 AF 46
        :     EE B8 B3 22 16 9C AA 1D A2 EA F2 B1 67 93 3B 4B
        :     2F 71 80 91 5B CE 7F 0D EF F2 BD 31 73 C2 2A 8F
```

```
:     E3 F1 B3 99 F0 97 10 4F DE 15 C9 B5 89 ED A7 14
:     0B 57 96 70 AF 76 D2 F0 F9 5E 35 19 5E 4D 67 7F
:     1E 23 D3 FA F6 6E CA DF B1 60 DE 35 38 81 08 21
:     FF 7E 4E 06 3C 8E 75 55 78 AC 55 F0 73 40 84 D2
:     76 97 FE 1E FE 42 E7 9D F3 69 5B BD 45 09 89 AF
:     C9 11 A6 12 E0 E6 BB 34 87 51 21 78 38 FA 4B DA
:     B9 57 6C 3A 85 65 01 DB 7D 27 64 89 C3 83 DD 44
:     0B BF 91 46 EC 94 88 0A DB 7D 4F BD 79 5D 5E 2C
:     07 D0 5D E0 87 6B 3E 68 4F 79 CA DF 1F 15 89 60
:     C2 09 B9 4A 5F D6 D3 38 B0 F8 9A 4F 26 A4 34 D6
:     62 9E 2A 7C 50 BF 43 7E AE F0 5C 31 F2 99 BE DD
:     6B 97 12 E6 42 94 45 44 19 C0 01 33 E4 C8 FA 0B
:     E2 BB D1 F2 A3 25 4A B8 58 12 C3 2A E9 BD 9C FF
:     8D 31 41 5C 8D DC 55 9B B3 DB 9A 64 A0 56 14 8A
:   }
```

Certificat qualifié personne physique avec identifiants et clés sémantiques sur QSCD

Field	Value
VERSION:	3
SERIAL:	Allocated automatically by the Issuing CA
INNER SIGNATURE:	
ALG. ID:	id-sha256-with-rsa-encryption
PARAMETER:	0
ISSUER:	
Country Name:	IT
Organization Name:	InfoCert S.p.A.
Organizational Unit Name:	Qualified Trust Service Provider
Organization Identifier:	VATIT-07945211006
Common Name:	InfoCert Qualified Electronic Signature CA 3
VALIDITY:	max 39 month
Not Before:	
Not After:	
SUBJECT:	
Country Name:	*CountryCode (ISO 3166) (mandatory)(*****)*
Organization Name:	*(conditioned presence) (***)*
Organizational Unit	*(conditioned presence) (****)*
Organization Identifier:	*(conditioned presence) (***) as defined in clause 5.1.4 of ETSI EN 319 412-1 (i.e. "**VATIT-**TaxIdentificationNumber", "**NTRIT-**IdentifierNationalTradeRegister")*
GivenName:	*Name (conditioned presence) (*)*
Surname:	*Surname (conditioned presence) (*)*
SerialNumber:	*(conditioned presence) (**) as defined in clause 5.1.3 of ETSI EN 319 412-1 (i.e. "**TINIT-**Codicefiscale", "**PASIT-**PassportNumber", "**IDCIT-**IdentityCardNumber")*
Title	*Holder's specific qualification (optional)*
Locality	*(optional)*
DNQualifier	*Holder's identification code assigned by the Certification Authority, unique within the Certification Authority itself (mandatory)*
Pseudonym:	*(conditioned presence) (*)*
Common Name	*name of the subject (recommended)*
PUBLIC KEY:	(key size is 2048 bits or higher)
ALGORITHM:	

ALG. ID:	id-rsa-encryption
PARAMETER:	0
MODULUS:	
EXPONENT:	
EXTENSIONS:	
Authority Key Identifier:	key identifier (sha1 160 bit) of Issuer Public Key
Key Usage*:	Non-Repudiation (critical)
CRL Distribution Points:	
Distribution Point 1:	
Uniform Resource ID1:	
http://crl.infocert.it/ca3/qc/CRLxx.crl	
Uniform Resource ID2:	
ldap://ldap.infocert.it/cn%3DInfoCert%20Qualified%20Electronic%20Signature%20CA%203%20CRLxx,ou%3DQualified%20Trust%20Service%20Provider,o%3DINFOCERT%20SPA,c%3DIT?certificateRevocationList	
Authority Information Access	
Access Method	1.3.6.1.5.5.7.48.1
Alternative Name	http://ocsp.qc.ca3.infocert.it
Access Method	1.3.6.1.5.5.7.48.2
Alternative Name	http://cert.infocert.it/ca3/qc/CA.crt
Subject Key Identifier:	key identifier (sha1 (160 bit) of public key)
SubjectDirectoryAttributes	
DateOfBirth	
Subject Alternative Name	
RFC822Name	*certificate holder e-mail*
Certificate Policies:	
Policy 1:	
Policy ID:	0.4.0.194112.1.2
Policy 2:	
Policy ID:	• 1.3.76.36.1.1.61 • 1.3.76.36.1.1.62 • 1.3.76.36.1.1.63 • 1.3.76.36.1.1.66
Policy Qualifier ID:	cps (id-qt-cps)
CPS uri:	http://www.firma.infocert.it/documentazione/manuali.php
ETSI extensions: qcStatement-1 (QcCompliance) ::=	

0.4.0.1862.1.1	
ETSI extensions: qcStatement-2 (QcEuLimitValue) ::= 0.4.0.1862.1.2	*(optional)*
ETSI extensions: QCStatement-3 (QcEURetentionPeriod)::= 0.4.0.1862.1.3	20
ETSI extensions: qcStatement-4 (QcSSCD)::= 0.4.0.1862.1.4	
ETSI extensions: qcStatement-5 (QcEuPDS)::= 0.4.0.1862.1.5	*PDS URL and LANGUAGE*
ETSI extensions: qcStatement-6 (QcType)::= 0.4.0.1862.1.6	id-etsi-qct-esign
RFC3739 extensions: qcStatement-2 (pkixQCSyntax-v2)::= 1.3.6.1.5.5.7.0.18.11.2	id-etsi-qcs-semanticsId-Natural (0.4.0.194121.1.1) *(mandatory)* id-etsi-qcs-SemanticsId-Legal (0.4.0.194121.1.2) *(optional)*
SIGNATURE:	
ALG. ID:	id-sha256-with-rsa-encryption
PARAMETER:	0
VALUE:	Ca Signature
***(*)**: the pseudonym attribute shall not be present if the givenName and surname attributes are present*	
***(**)**: if givenName and surname or pseudonym attributes are not sufficient to ensure Subject name uniqueness within the context of the issuer, then the serialNumber attribute shall be present*	
***(***):** when a natural person subject is associated with an organization, the subject attributes may also identify such organization using attributes such as organizationName and organizationIdentifier*	
***(****)**: if the organization attribute is present, it contains more information about the organization itself. This attribute may appear, at most, four times.*	
***(*****)**: if the organization attribute is present, it contains the country where the organization is based, otherwise it contains the country consistent with the legal Jurisidction under which the certificate is issued*	
NB: xx = partitioned revocation list progressive numbering	

Certificat qualifié personne physique SANS identifiant ni clé sémantique sur QSCD délivré par l'AC racine « InfoCert Qualified Electronic Signature CA 3 »

Field	Value
VERSION:	3
SERIAL:	Allocated automatically by the Issuing CA
INNER SIGNATURE:	
ALG. ID:	id-sha256-with-rsa-encryption
PARAMETER:	0
ISSUER:	
Country Name:	IT
Organization Name:	InfoCert S.p.A.
Organizational Unit Name:	Qualified Trust Service Provider
Organization Identifier:	VATIT-07945211006
Common Name:	InfoCert Qualified Electronic Signature CA 3
VALIDITY:	max 39 month
Not Before:	
Not After:	
SUBJECT:	
Country Name:	*CountryCode (ISO 3166) (mandatory)(*****)*
Organization Name:	*(conditioned presence) (***)*
Organization Identifier:	*(conditioned presence) (***)*
Organizational Unit	*(conditioned presence) (****)*
GivenName:	*Name (conditioned presence) (*)*
Surname:	*Surname (conditioned presence) (*)*
SerialNumber:	*(conditioned presence) (**)*
Title	*Holder's specific qualification (optional)*
Locality	*(optional)*
DNQualifier	*Holder's identification code assigned by the Certification Authority, unique within the Certification Authority itself (mandatory)*
Pseudonym:	*(conditioned presence) (*)*
Common Name	*name of the subject (recommended)*
PUBLIC KEY:	(key size is 2048 bits or higher)
ALGORITHM:	
ALG. ID:	id-rsa-encryption
PARAMETER:	0
MODULUS:	
EXPONENT:	
EXTENSIONS:	
Authority Key Identifier:	key identifier (sha1 160 bit) of Issuer Public Key
Key Usage*:	Non-Repudiation (critical)
CRL Distribution Points:	
Distribution Point 1:	
Uniform Resource ID1:	

http://crl.infocert.it/ca3/qc/CRLxx.crl	
Uniform Resource ID2:	
ldap://ldap.infocert.it/cn%3DInfoCert%20Qualified%20Electronic%20Signature%20CA%203%20CRLxx,ou%3DQualified%20Trust%20Service%20Provider,o%3DINFOCERT%20SPA,c%3DIT?certificateRevocationList	
Authority Information Access	
Access Method	1.3.6.1.5.5.7.48.1
Alternative Name	http://ocsp.qc.ca3.infocert.it
Access Method	1.3.6.1.5.5.7.48.2
Alternative Name	http://cert.infocert.it/ca3/qc/CA.crt
Subject Key Identifier:	key identifier (sha1 (160 bit) of public key)
SubjectDirectoryAttributes	
DateOfBirth	
Subject Alternative Name	
RFC822Name	*certificate holder e-mail*
Certificate Policies:	
Policy 1:	
Policy ID:	0.4.0.194112.1.2
Policy 2:	
Policy ID:	• 1.3.76.36.1.1.61 • 1.3.76.36.1.1.62 • 1.3.76.36.1.1.63 • 1.3.76.36.1.1.66
Policy Qualifier ID:	cps (id-qt-cps)
CPS uri:	http://www.firma.infocert.it/documentazione/manuali.php
ETSI extensions: qcStatement-1 (QcCompliance) ::= 0.4.0.1862.1.1	
ETSI extensions: qcStatement-2 (QcEuLimitValue) ::= 0.4.0.1862.1.2	*(optional)*
ETSI extensions: QCStatement-3 (QcEURetentionPeriod)::= 0.4.0.1862.1.3	20
ETSI extensions: qcStatement-4 (QcSSCD)::= 0.4.0.1862.1.4	

ETSI extensions: qcStatement-5 (QcEuPDS)::= 0.4.0.1862.1.5	*PDS URL and LANGUAGE*
ETSI extensions: qcStatement-6 (QcType)::= 0.4.0.1862.1.6	id-etsi-qct-esign
SIGNATURE:	
ALG. ID:	id-sha256-with-rsa-encryption
PARAMETER:	0
VALUE:	Ca Signature
***(*)**: the pseudonym attribute shall not be present if the givenName and surname attributes are present*	
***(**)**: if givenName and surname or pseudonym attributes are not sufficient to ensure Subject name uniqueness within the context of the issuer, then the serialNumber attribute shall be present*	
***(***):** when a natural person subject is associated with an organization, the subject attributes may also identify such organization using attributes such as organizationName and organizationIdentifier*	
***(****)**: if the organization attribute is present, it contains more information about the organization itself. This attribute may appear, at most, four times.*	
***(*****)**:if the organization attribute is present, it contains the country where the organization is based, otherwise it contains the country consistent with the legal Jurisidction under which the certificate is issued*	
NB: xx = partitioned revocation list progressive numbering	

Certificat qualifié personne physique SANS identifiant ni clé sémantique sur QSCD délivré par l'AC racine « InfoCert Firma Qualificata 2 »

Field	Value
VERSION:	3
SERIAL:	Allocated automatically by the Issuing CA
INNER SIGNATURE:	
ALG. ID:	id-sha256-with-rsa-encryption
PARAMETER:	0
ISSUER:	
Country Name:	IT
Organization Name:	INFOCERT SPA
Organizational Unit Name:	Certificatore Accreditato
serialNumber	07945211006
Common Name:	InfoCert Firma Qualificata 2
VALIDITY:	max 39 month
Not Before:	
Not After:	
SUBJECT:	
Country Name:	*CountryCode (ISO 3166) (mandatory)* ***(*****)***
Organization Name:	*(conditioned presence)* ***(***)***
Organization Identifier:	*(conditioned presence)* ***(***)***
Organizational Unit	*(conditioned presence)* ***(****)***
GivenName:	*Name (conditioned presence)* ***(*)***
Surname:	*Surname (conditioned presence)* ***(*)***
SerialNumber:	*(conditioned presence)* ***(**)***
Title	*Holder's specific qualification (optional)*
Locality	*(optional)*
DNQualifier	Holder's identification code assigned by the Certification Authority, unique within the Certification Authority itself (mandatory)
Pseudonym:	*(conditioned presence)* ***(*)***
Common Name	*name of the subject (recommended)*
PUBLIC KEY:	(key size is 2048 bits or higher)
ALGORITHM:	
ALG. ID:	id-rsa-encryption
PARAMETER:	0
MODULUS:	
EXPONENT:	
EXTENSIONS:	
Authority Key Identifier:	key identifier (sha1 160 bit) of Issuer Public Key
Key Usage*:	Non-Repudiation (critical)
CRL Distribution Points:	
Distribution Point 1:	
Uniform Resource ID1:	
http://crl.infocert.it/crls/firma2/CRLxx.crl	

Field	Value
Uniform Resource ID2:	
URI = ldap://ldap.infocert.it/cn%3DInfoCert%20Firma%20Qualificata%202%20CRL05,ou%3DCertificatore%20Accreditato,o%3DINFOCERT%20SPA,c%3DIT?certificateRevocationList	
Authority Information Access	
Access Method	1.3.6.1.5.5.7.48.1
Alternative Name	http://ocsp.sc.infocert.it/
Access Method	1.3.6.1.5.5.7.48.2
Alternative Name	http://cert.infocert.it/ca2/firma2/CA.crt
Subject Key Identifier:	key identifier (sha1 (160 bit) of public key)
SubjectDirectoryAttributes	
DateOfBirth	
Subject Alternative Name	
RFC822Name	*certificate holder e-mail*
Certificate Policies:	
Policy 1:	
Policy ID:	0.4.0.194112.1.2
Policy 2:	
Policy ID:	• 1.3.76.36.1.1.1 (firma qualificata) • 1.3.76.36.1.1.2 (firma qualificata automatica) • 1.3.76.36.1.1.22 (firma qualificata remota) • 1.3.76.36.1.1.32 (firma qualificata CMS)
Policy Qualifier ID:	cps (id-qt-cps)
CPS uri:	http://www.firma.infocert.it/documentazione/manuali.php
ETSI extensions: qcStatement-1 (QcCompliance) ::= 0.4.0.1862.1.1	
ETSI extensions: qcStatement-2 (QcEuLimitValue) ::= 0.4.0.1862.1.2	*(optional)*
ETSI extensions: QCStatement-3 (QcEURetentionPeriod)::= 0.4.0.1862.1.3	20
ETSI extensions: qcStatement-4 (QcSSCD)::= 0.4.0.1862.1.4	

Field	Value
ETSI extensions: qcStatement-5 (QcEuPDS)::= 0.4.0.1862.1.5	*PDS URL and LANGUAGE*
ETSI extensions: qcStatement-6 (QcType)::= 0.4.0.1862.1.6	id-etsi-qct-esign
SIGNATURE:	
ALG. ID:	id-sha256-with-rsa-encryption
PARAMETER:	0
VALUE:	Ca Signature
***(*)**: the pseudonym attribute shall not be present if the givenName and surname attributes are present*	
***(**)**: if givenName and surname or pseudonym attributes are not sufficient to ensure Subject name uniqueness within the context of the issuer, then the serialNumber attribute shall be present*	
***(***):** when a natural person subject is associated with an organization, the subject attributes may also identify such organization using attributes such as organizationName and organizationIdentifier*	
***(****)**: if the organization attribute is present, it contains more information about the organization itself. This attribute may appear, at most, four times.*	
***(*****)**:if the organization attribute is present, it contains the country where the organization is based, otherwise it contains the country consistent with the legal Jurisidction under which the certificate is issued*	
NB: xx = partitioned revocation list progressive numbering	

Certificat qualifié personne physique avec identifiants et clés sémantiques

Field	Value
VERSION:	3
SERIAL:	Allocated automatically by the Issuing CA
INNER SIGNATURE:	
ALG. ID:	id-sha256-with-rsa-encryption
PARAMETER:	0
ISSUER:	
Country Name:	IT
Organization Name:	InfoCert S.p.A.
Organizational Unit Name:	Qualified Trust Service Provider
Organization Identifier:	VATIT-07945211006
Common Name:	InfoCert Qualified Electronic Signature CA 3
VALIDITY:	max 39 month
Not Before:	
Not After:	
SUBJECT:	
Country Name:	*CountryCode (ISO 3166) (mandatory)* ***(*****)***
Organization Name:	*(conditioned presence)* ***(***)***
Organization Identifier:	*(conditioned presence)* ***(***)*** *as defined in clause 5.1.4 of ETSI EN 319 412-1 (i.e. "***VATIT-***TaxIdentificationNumber", "***NTRIT-***IdentifierNationalTradeRegister")*
Organizational Unit	*(conditioned presence)* ***(****)***

GivenName:	*Name (conditioned presence) **(*)***
Surname:	*Surname (conditioned presence) **(*)***
SerialNumber:	*(conditioned presence) **(**)** as defined in clause 5.1.3 of ETSI EN 319 412-1 (i.e. "**TINI**T-Codicefiscale", "**PASIT-**PassportNumber", "**IDCIT-**IdentityCardNumber")*
Title	*Holder's specific qualification (optional)*
Locality	*(optional)*
DNQualifier	Holder's identification code assigned by the Certification Authority, unique within the Certification Authority itself (mandatory)
Pseudonym:	*(conditioned presence) **(*)***
Common Name	*name of the subject (recommended)*
PUBLIC KEY:	(key size is 2048 bits or higher)
ALGORITHM:	
ALG. ID:	id-rsa-encryption
PARAMETER:	0
MODULUS:	
EXPONENT:	
EXTENSIONS:	
Authority Key Identifier:	key identifier (sha1 160 bit) of Issuer Public Key
Key Usage*:	Non-Repudiation (critical)
CRL Distribution Points:	
Distribution Point 1:	
Uniform Resource ID1:	
http://crl.infocert.it/ca3/qc/CRLxx.crl	
Uniform Resource ID2:	
ldap://ldap.infocert.it/cn%3DInfoCert%20Qualified%20Electronic%20Signature%20CA%203%20CRLxx,ou%3DQualified%20Trust%20Service%20Provider,o%3DINFOCERT%20SPA,c%3DIT?certificateRevocationList	
Authority Information Access	
Access Method	1.3.6.1.5.5.7.48.1
Alternative Name	http://ocsp.qc.ca3.infocert.it
Access Method	1.3.6.1.5.5.7.48.2
Alternative Name	http://cert.infocert.it/ca3/qc/CA.crt
Subject Key Identifier:	key identifier (sha1 (160 bit) of public key)
SubjectDirectoryAttributes	
DateOfBirth	
Subject Alternative Name	
RFC822Name	*certificate holder e-mail*
Certificate Policies:	
Policy 1:	
Policy ID:	0.4.0.194112.1.0

Policy 2:	
Policy ID:	1.3.76.36.1.1.48
Policy Qualifier ID:	cps (id-qt-cps)
CPS uri:	http://www.firma.infocert.it/documentazione/manuali.php
ETSI extensions: qcStatement-1 (QcCompliance) ::= 0.4.0.1862.1.1	
ETSI extensions: qcStatement-2 (QcEuLimitValue) ::= 0.4.0.1862.1.2	*(optional)*
ETSI extensions: QCStatement-3 (QcEURetentionPeriod)::= 0.4.0.1862.1.3	20
ETSI extensions: qcStatement-5 (QcEuPDS)::= 0.4.0.1862.1.5	*PDS URL and LANGUAGE*
ETSI extensions: qcStatement-6 (QcType)::= 0.4.0.1862.1.6	id-etsi-qct-esign
RFC3739 extensions: qcStatement-2 (pkixQCSyntax-v2)::= 1.3.6.1.5.5.7.0.18.11.2	id-etsi-qcs-semanticsId-Natural (0.4.0.194121.1.1) *(mandatory)* id-etsi-qcs-SemanticsId-Legal (0.4.0.194121.1.2) *(optional)*
SIGNATURE:	
ALG. ID:	id-sha256-with-rsa-encryption
PARAMETER:	0
VALUE:	Ca Signature
***(*)**: the pseudonym attribute shall not be present if the givenName and surname attributes are present*	
***(**)**: if givenName and surname or pseudonym attributes are not sufficient to ensure Subject name uniqueness within the context of the issuer, then the serialNumber attribute shall be present*	
***(***):** when a natural person subject is associated with an organization, the subject attributes may also identify such organization using attributes such as organizationName and organizationIdentifier*	
***(****)**: if the organization attribute is present, it contains more information about the organization itself. This attribute may appear, at most, four times.*	
***(*****)**:if the organization attribute is present, it contains the country where the organization is based, otherwise it contains the country consistent with the legal Jurisidction under which the certificate is issued*	
NB: xx = partitioned revocation list progressive numbering	

Certificat qualifié personne physique SANS identifiant ni clé sémantique

Field	Value
VERSION:	3
SERIAL:	Allocated automatically by the Issuing CA
INNER SIGNATURE:	
ALG. ID:	id-sha256-with-rsa-encryption
PARAMETER:	0
ISSUER:	
Country Name:	IT
Organization Name:	InfoCert S.p.A.
Organizational Unit Name:	Qualified Trust Service Provider
Organization Identifier:	VATIT-07945211006
Common Name:	InfoCert Qualified Electronic Signature CA 3
VALIDITY:	max 39 month
Not Before:	
Not After:	
SUBJECT:	
Country Name:	*CountryCode (ISO 3166) (mandatory)* ***(*****)***
Organization Name:	*(conditioned presence)* ***(***)***
Organization Identifier:	*(conditioned presence)* ***(***)***
Organizational Unit	*(conditioned presence)* ***(****)***
GivenName:	*Name (conditioned presence)* ***(*)***
Surname:	*Surname (conditioned presence)* ***(*)***
SerialNumber:	*(conditioned presence)* ***(**)***
Title	*Holder's specific qualification (optional)*
Locality	*(optional)*
DNQualifier	Holder's identification code assigned by the Certification Authority, unique within the Certification Authority itself (mandatory)
Pseudonym:	*(conditioned presence)* ***(*)***
Common Name	*name of the subject (recommended)*
PUBLIC KEY:	(key size is 2048 bits or higher)
ALGORITHM:	
ALG. ID:	id-rsa-encryption
PARAMETER:	0
MODULUS:	
EXPONENT:	
EXTENSIONS:	
Authority Key Identifier:	key identifier (sha1 160 bit) of Issuer Public Key
Key Usage*:	Non-Repudiation (critical)
CRL Distribution Points:	
Distribution Point 1:	
Uniform Resource ID1:	
http://crl.infocert.it/ca3/qc/CRLxx.crl	
Uniform Resource	

ID2:	
ldap://ldap.infocert.it/cn%3DInfoCert%20Qualified%20Electronic%20Signature%20CA%203%20CRLxx,ou%3DQualified%20Trust%20Service%20Provider,o%3DINFOCERT%20SPA,c%3DIT?certificateRevocationList	
Authority Information Access	
Access Method	1.3.6.1.5.5.7.48.1
Alternative Name	http://ocsp.qc.ca3.infocert.it
Access Method	1.3.6.1.5.5.7.48.2
Alternative Name	http://cert.infocert.it/ca3/qc/CA.crt
Subject Key Identifier:	key identifier (sha1 (160 bit) of public key)
SubjectDirectoryAttributes	
DateOfBirth	
Subject Alternative Name	
RFC822Name	*certificate holder e-mail*
Certificate Policies:	
Policy 1:	
Policy ID:	0.4.0.194112.1.0
Policy 2:	
Policy ID:	1.3.76.36.1.1.48
Policy Qualifier ID:	cps (id-qt-cps)
CPS uri:	http://www.firma.infocert.it/documentazione/manuali.php
ETSI extensions: qcStatement-1 (QcCompliance) ::= 0.4.0.1862.1.1	
ETSI extensions: qcStatement-2 (QcEuLimitValue) ::= 0.4.0.1862.1.2	*(optional)*
ETSI extensions: QCStatement-3 (QcEURetentionPeriod)::= 0.4.0.1862.1.3	20
ETSI extensions: qcStatement-5 (QcEuPDS)::= 0.4.0.1862.1.5	*PDS URL and LANGUAGE*
ETSI extensions: qcStatement-6 (QcType)::= 0.4.0.1862.1.6	id-etsi-qct-esign
SIGNATURE:	
ALG. ID:	id-sha256-with-rsa-encryption

PARAMETER:	0
VALUE:	Ca Signature
***(*)**: the pseudonym attribute shall not be present if the givenName and surname attributes are present*	
***(**)**: if givenName and surname or pseudonym attributes are not sufficient to ensure Subject name uniqueness within the context of the issuer, then the serialNumber attribute shall be present*	
***(***):** when a natural person subject is associated with an organization, the subject attributes may also identify such organization using attributes such as organizationName and organizationIdentifier*	
***(****)**: if the organization attribute is present, it contains more information about the organization itself. This attribute may appear, at most, four times.*	
***(*****)**:if the organization attribute is present, it contains the country where the organization is based, otherwise it contains the country consistent with the legal Jurisidction under which the certificate is issued*	
NB: xx = partitioned revocation list progressive numbering	

Certificat qualifié personne morale avec identifiants et clés sémantiques

Field	Value
VERSION:	3
SERIAL:	Allocated automatically by the Issuing CA
INNER SIGNATURE:	
ALG. ID:	id-sha256-with-rsa-encryption
PARAMETER:	0
ISSUER:	
Country Name:	IT
Organization Name:	InfoCert S.p.A.
Organizational Unit Name:	Qualified Trust Service Provider
Organization Identifier:	VATIT-07945211006
Common Name:	InfoCert Qualified Electronic Signature CA 3
VALIDITY:	max 3 years
Not Before:	
Not After:	
SUBJECT:	
Country Name:	*CountryCode (ISO 3166) (mandatory)*
Organization Name:	*full registered name of the subject (legal person) (mandatory)*
Organization Identifier:	*as defined in clause 5.1.4 of ETSI EN 319 412-1 (i.e. "**VATIT-**TaxIdentificationNumber", "**NTRIT-**IdentifierNationalTradeRegister") (mandatory)* *if PSD2, as defined in clause 5.2.1 of ETSI TS 119 495 [7] requirements GEN-5.2.1-3 and GEN-5.2.1-4 (i.e. "**PSDIT-BI-**PSPAuthorizationNumber", "**VATIT-**TaxIdentificationNumber", "**NTRIT-**IdentifierNationalTradeRegister") (mandatory)*
Common Name	*name of the subject (legal person) (mandatory)*
StateorProvince Name:	*Verified subject's state or province information (optional)*
Locality Name:	*Verified subject's locality information (optional)*
PUBLIC KEY:	(key size is 2048 bits or higher)
ALGORITHM:	
ALG. ID:	id-rsa-encryption

PARAMETER:	0
MODULUS:	
EXPONENT:	
EXTENSIONS:	
Authority Key Identifier:	key identifier (sha1 160 bit) of Issuer Public Key
Key Usage*:	Digital Signature or Non-Repudiation (critical)
CRL Distribution Points:	
Distribution Point 1:	
Uniform Resource ID1:	
http://crl.infocert.it/ca3/qc/CRLxx.crl	
Uniform Resource ID2:	
ldap://ldap.infocert.it/cn%3DInfoCert%20Qualified%20Electronic%20Signature%20CA%203%20CRLxx,ou%3DQualified%20Trust%20Service%20Provider,o%3DINFOCERT%20SPA,c%3DIT?certificateRevocationList	
Authority Information Access	
Access Method	1.3.6.1.5.5.7.48.1
Alternative Name	http://ocsp.qc.ca3.infocert.it
Access Method	1.3.6.1.5.5.7.48.2
Alternative Name	http://cert.infocert.it/ca3/qc/CA.crt
Subject Key Identifier:	key identifier (sha1 (160 bit) of public key)
SubjectDirectoryAttributes	
DateOfBirth	
Subject Alternative Name	
RFC822Name	*certificate holder e-mail*
Certificate Policies:	
Policy 1:	
Policy ID:	0.4.0.194112.1.1
Policy 2:	
Policy ID:	1.3.76.36.1.1.47
Policy Qualifier ID:	cps (id-qt-cps)
CPS uri:	http://www.firma.infocert.it/documentazione/manuali.php
ETSI extensions: qcStatement-1 (QcCompliance) ::= 0.4.0.1862.1.1	

ETSI extensions: qcStatement-2 (QcEuLimitValue) ::= 0.4.0.1862.1.2	*(optional)*
ETSI extensions: QCStatement-3 (QcEURetentionPeriod)::= 0.4.0.1862.1.3	20
ETSI extensions: qcStatement-5 (QcEuPDS)::= 0.4.0.1862.1.5	*PDS URL and LANGUAGE*
ETSI extensions: qcStatement-6 (QcType)::= 0.4.0.1862.1.6	id-etsi-qct-eseal
RFC3739 extensions: qcStatement-2 (pkixQCSyntax-v2)::= 1.3.6.1.5.5.7.0.18.11.2	id-etsi-qcs-SemanticsId-Legal (0.4.0.194121.1.2)
SIGNATURE:	
ALG. ID:	id-sha256-with-rsa-encryption
PARAMETER:	0
VALUE:	Ca Signature
NB: xx = partitioned revocation list progressive numbering	

Certificat qualifié personne morale SANS identifiant ni clé sémantique

Field	Value
VERSION:	3
SERIAL:	Allocated automatically by the Issuing CA
INNER SIGNATURE:	
ALG. ID:	id-sha256-with-rsa-encryption
PARAMETER:	0
ISSUER:	
Country Name:	IT
Organization Name:	InfoCert S.p.A.
Organizational Unit Name:	Qualified Trust Service Provider
Organization Identifier:	VATIT-07945211006
Common Name:	InfoCert Qualified Electronic Signature CA 3
VALIDITY:	max 3 years
Not Before:	
Not After:	
SUBJECT:	
Country Name:	*CountryCode (ISO 3166) (mandatory)*
Organization Name:	*full registered name of the subject (legal person) (mandatory)*
Organization Identifier:	*identification of the subject organization different from the organization name (mandatory)*
Common Name	*name of the subject (legal person) (mandatory)*
PUBLIC KEY:	(key size is 2048 bits or higher)
ALGORITHM:	
ALG. ID:	id-rsa-encryption
PARAMETER:	0
MODULUS:	
EXPONENT:	
EXTENSIONS:	
Authority Key Identifier:	key identifier (sha1 160 bit) of Issuer Public Key
Key Usage*:	Digital Signature or Non-Repudiation (critical)
CRL Distribution Points:	
Distribution Point 1:	
Uniform Resource ID1:	
http://crl.infocert.it/ca3/qc/CRLxx.crl	
Uniform Resource ID2:	
ldap://ldap.infocert.it/cn%3DInfoCert%20Qualified%20Electronic%20Signature%20CA%203%20CRLxx,ou%3DQualified%20Trust%20Service%20Provider,o%3DINFOCERT%20SPA,c%3DIT?certificateRevocationList	
Authority Information Access	
Access Method	1.3.6.1.5.5.7.48.1

Alternative Name	http://ocsp.qc.ca3.infocert.it
Access Method	1.3.6.1.5.5.7.48.2
Alternative Name	http://cert.infocert.it/ca3/qc/CA.crt
Subject Key Identifier:	key identifier (sha1 (160 bit) of public key)
SubjectDirectoryAttributes	
DateOfBirth	
Subject Alternative Name	
RFC822Name	*certificate holder e-mail*
Certificate Policies:	
Policy 1:	
Policy ID:	0.4.0.194112.1.1
Policy 2:	
Policy ID:	1.3.76.36.1.1.47
Policy Qualifier ID:	cps (id-qt-cps)
CPS uri:	http://www.firma.infocert.it/documentazione/manuali.php
ETSI extensions: qcStatement-1 (QcCompliance) ::= 0.4.0.1862.1.1	
ETSI extensions: qcStatement-2 (QcEuLimitValue) ::= 0.4.0.1862.1.2	*(optional)*
ETSI extensions: QCStatement-3 (QcEURetentionPeriod)::= 0.4.0.1862.1.3	20
ETSI extensions: qcStatement-5 (QcEuPDS)::= 0.4.0.1862.1.5	*PDS URL and LANGUAGE*
ETSI extensions: qcStatement-6 (QcType)::= 0.4.0.1862.1.6	id-etsi-qct-eseal
SIGNATURE:	
ALG. ID:	id-sha256-with-rsa-encryption
PARAMETER:	0
VALUE:	Ca Signature
NB: xx = partitioned revocation list progressive numbering	

Certificat qualifié personne morale avec identifiants et clés sémantiques sur QSCD (QSealC)

Field	Value
VERSION:	3
SERIAL:	Allocated automatically by the Issuing CA
INNER SIGNATURE:	
ALG. ID:	id-sha256-with-rsa-encryption
PARAMETER:	0
ISSUER:	
Country Name:	IT
Organization Name:	InfoCert S.p.A.
Organizational Unit Name:	Qualified Trust Service Provider
Organization Identifier:	VATIT-07945211006
Common Name:	InfoCert Qualified Electronic Signature CA 3
VALIDITY:	max 3 years
Not Before:	
Not After:	
SUBJECT:	
Country Name:	*CountryCode (ISO 3166) (mandatory)*
Organization Name:	*full registered name of the subject (legal person) (mandatory)*
Organization Identifier:	*as defined in clause 5.1.4 of ETSI EN 319 412-1 (i.e. "***VATIT-***TaxIdentificationNumber", "***NTRIT-***IdentifierNationalTradeRegister") (mandatory)*
Common Name	*name of the subject (legal person) (mandatory)*
StateorProvince Name:	*Verified subject's state or province information (optional)*
Locality Name:	*Verified subject's locality information (optional)*
PUBLIC KEY:	(key size is 2048 bits or higher)
ALGORITHM:	
ALG. ID:	id-rsa-encryption
PARAMETER:	0
MODULUS:	
EXPONENT:	
EXTENSIONS:	
Authority Key Identifier:	key identifier (sha1 160 bit) of Issuer Public Key
Key Usage*:	Digital Signature or Non-Repudiation (critical)
CRL Distribution Points:	
Distribution Point 1:	
Uniform Resource ID1:	
http://crl.infocert.it/ca3/qc/CRLxx.crl	
Uniform Resource ID2:	
ldap://ldap.infocert.it/cn%3DInfoCert%20Qualified%20Electronic%20Signature%20CA%203%20CRLxx,ou%3DQualified%20Trust%20Service%20Provider,o%3DINFOCERT%20SPA,c%3DIT?certificateRevocationList	
Authority Information Access	

Access Method	1.3.6.1.5.5.7.48.1
Alternative Name	http://ocsp.qc.ca3.infocert.it
Access Method	1.3.6.1.5.5.7.48.2
Alternative Name	http://cert.infocert.it/ca3/qc/CA.crt
Subject Key Identifier:	key identifier (sha1 (160 bit) of public key)
SubjectDirectoryAttributes	
DateOfBirth	
Subject Alternative Name	
RFC822Name	*certificate holder e-mail*
Certificate Policies:	
Policy 1:	
Policy ID:	0.4.0.194112.1.3
Policy 2:	
Policy ID:	1.3.76.36.1.1.46
Policy Qualifier ID:	cps (id-qt-cps)
CPS uri:	http://www.firma.infocert.it/documentazione/manuali.php
ETSI extensions: qcStatement-1 (QcCompliance) ::= 0.4.0.1862.1.1	
ETSI extensions: qcStatement-2 (QcEuLimitValue) ::= 0.4.0.1862.1.2	*(optional)*
ETSI extensions: QCStatement-3 (QcEURetentionPeriod)::= 0.4.0.1862.1.3	20
ETSI extensions: qcStatement-4 (QcSSCD)::= 0.4.0.1862.1.4	
ETSI extensions: qcStatement-5 (QcEuPDS)::= 0.4.0.1862.1.5	*PDS URL and LANGUAGE*
ETSI extensions: qcStatement-6 (QcType)::= 0.4.0.1862.1.6	id-etsi-qct-eseal
RFC3739 extensions: qcStatement-2 (pkixQCSyntax-v2)::= 1.3.6.1.5.5.7.0.18.11.2	id-etsi-qcs-SemanticsId-Legal (0.4.0.194121.1.2)
SIGNATURE:	

ALG. ID:	id-sha256-with-rsa-encryption
PARAMETER:	0
VALUE:	Ca Signature
NB: xx = partitioned revocation list progressive numbering	

Certificat qualifié personne morale SANS identifiant ni clé sémantique sur QSCD

Field	Value
VERSION:	3
SERIAL:	Allocated automatically by the Issuing CA
INNER SIGNATURE:	
ALG. ID:	id-sha256-with-rsa-encryption
PARAMETER:	0
ISSUER:	
Country Name:	IT
Organization Name:	InfoCert S.p.A.
Organizational Unit Name:	Qualified Trust Service Provider
Organization Identifier:	VATIT-07945211006
Common Name:	InfoCert Qualified Electronic Signature CA 3
VALIDITY:	max 3 years
Not Before:	
Not After:	
SUBJECT:	
Country Name:	*CountryCode (ISO 3166) (mandatory)*
Organization Name:	*full registered name of the subject (legal person) (mandatory)*
Organization Identifier:	*identification of the subject organization different from the organization name (mandatory)*
Common Name	*name of the subject (legal person) (mandatory)*
PUBLIC KEY:	(key size is 2048 bits or higher)
ALGORITHM:	
ALG. ID:	id-rsa-encryption
PARAMETER:	0
MODULUS:	
EXPONENT:	
EXTENSIONS:	
Authority Key Identifier:	key identifier (sha1 160 bit) of Issuer Public Key
Key Usage*:	Digital Signature or Non-Repudiation (critical)
CRL Distribution Points:	
Distribution Point 1:	
Uniform Resource ID1:	
http://crl.infocert.it/ca3/qc/CRLxx.crl	
Uniform Resource ID2:	
ldap://ldap.infocert.it/cn%3DInfoCert%20Qualified%20Electronic%20Signature%20CA%203%20CRLxx,ou%3DQualified%20Trust%20Service%20Provider,o%3DINFOCERT%20SPA,c%3DIT?certificateRevocationList	
Authority Information Access	
Access Method	1.3.6.1.5.5.7.48.1

Alternative Name	http://ocsp.qc.ca3.infocert.it
Access Method	1.3.6.1.5.5.7.48.2
Alternative Name	http://cert.infocert.it/ca3/qc/CA.crt
Subject Key Identifier:	key identifier (sha1 (160 bit) of public key)
SubjectDirectoryAttributes	
DateOfBirth	
Subject Alternative Name	
RFC822Name	*certificate holder e-mail*
Certificate Policies:	
Policy 1:	
Policy ID:	0.4.0.194112.1.3
Policy 2:	
Policy ID:	1.3.76.36.1.1.46
Policy Qualifier ID:	cps (id-qt-cps)
CPS uri:	http://www.firma.infocert.it/documentazione/manuali.php
ETSI extensions: qcStatement-1 (QcCompliance) ::= 0.4.0.1862.1.1	
ETSI extensions: qcStatement-2 (QcEuLimitValue) ::= 0.4.0.1862.1.2	*(optional)*
ETSI extensions: QCStatement-3 (QcEURetentionPeriod)::= 0.4.0.1862.1.3	20
ETSI extensions: qcStatement-4 (QcSSCD)::= 0.4.0.1862.1.4	
ETSI extensions: qcStatement-5 (QcEuPDS)::= 0.4.0.1862.1.5	*PDS URL and LANGUAGE*
ETSI extensions: qcStatement-6 (QcType)::= 0.4.0.1862.1.6	id-etsi-qct-eseal
SIGNATURE:	
ALG. ID:	id-sha256-with-rsa-encryption
PARAMETER:	0
VALUE:	Ca Signature
NB: xx = partitioned revocation list progressive numbering	

Extensions QCStatement pour QSealC DSP2

ETSI extensions: etsi-psd2-qcStatement (QcType)::= 0.4.0.19495.2	*SEQUENCE{* *rolesOfPSP RolesOfPSP,* *nCAName NCAName,* *nCAId NCAId }*
RolesOfPSP	*SEQUENCE{* *roleOfPspOid RoleOfPspOid,* *roleOfPspName RoleOfPspName }*
RoleOfPspOid	itu-t(0) identified-organization(4) etsi(0) psd2(19495) id-roles(1) 1 itu-t(0) identified-organization(4) etsi(0) psd2(19495) id-roles(1) 2 itu-t(0) identified-organization(4) etsi(0) psd2(19495) id-roles(1) 3 itu-t(0) identified-organization(4) etsi(0) psd2(19495) id-roles(1) 4
RoleOfPspName	PSP_AS PSP_PI PSP_AI PSP_IC
NCAName	*plain text name in English of the NCA*
NCAId	• *2 character ISO 3166 country code representing the NCA country;* • *hyphen-minus "-" (0x2D (ASCII), U+002D (UTF-8)); and* • *2-8 character NCA identifier without country code (A-Z uppercase only, no separator).*

Format des LCR et de l'OCSP

Extension	Description
Issuer Signature Algorithm	sha-256WithRSAEncryption [1 2 840 113549 1 1 11]
Issuer Distinguished Name	InfoCert
thisUpdate	Date en format UTC
nextUpdate	Date de la prochaine LCR en format
Revoked Certificates List	Liste des Certificats Révoqués, avec numéro de série et date de révocation/suspension
Issuer's Signature	Signature de l'AC

Valeurs et extensions pour les LCR et l'OCSP

Les LCR ont les extensions suivantes

Extension	Description
Authority Key Identifier	Valeur de hachage 160-bit SHA-1 de l'IssuerPublicKey
CRL number	Numéro unique de la LCR attribuée par l'AC
ExpiredCertsOnCRL	Date en format GeneralizedTime à partir de laquelle les certificats expirés sont conservés dans les LCR. La valeur est fixée à la date de délivrance de l'AC
Issuing Distribution Point	Identifie le point de distribution des LCR et l'objectif : indique si la LCR est générée pour les certificats d'AC uniquement, ou du Sujet (entité finale)
Invalidity Date	Date en format UTC indiquant la date à partir de laquelle le certificat est considéré comme non valable

La demande OCSP contient les champs suivants :

Champ	Description
Hash Algorithm	sha-1 [1 3 14 3 2 26] OR sha-256 [2 16 840 1 101 3 4 2 1]
Issuer Name Hash	Valeur de hachage du DN de l'émetteur
Issuer Key Hash	Valeur de hachage de la clé publique de l'émetteur.
Serial Number	Numéro de série du certificat

La réponse OCSP contient les champs suivants :

Champ	Description
Response Status	Statut de la réponse OCSP
Response Type	id-pkix-ocsp-basic [1 3 6 1 5 5 7 48 1 1]
Responder ID	Subject DN du certificat signataire de la réponse OCSP
Produced at	Date en format GeneralizedTime de la génération de la réponse OCSP

Hash Algorithm	sha-1 [1 3 14 3 2 26] OR sha-256 [2 16 840 1 101 3 4 2 1]
Issuer Name Hash	Valeur de hachage du nom distinctif de l'émetteur
Issuer Key Hash	Valeur de hachage de la clé publique de l'émetteur
Serial Number	Numéro de série du certificat
thisUpdate	Date de vérification de l'état du certificat en format GeneralizedTime
nextUpdate	Date à laquelle le statut du certificat pourrait être mis à jour
Issuer Signature Algorithm	sha-256WithRSAEncryption [1 2 840 113549 1 1 11]
Issuer's Signature	[OCSP response Signature]
Issuer certificate	[OCSP response signing certificate]

La demande OCSP peut contenir les extensions suivantes :

Extension	Description
nonce	Numéro arbitraire qui ne peut être utilisé qu'une seule fois. Il relie cryptographiquement une demande à sa réponse afin d'éviter les attaques de réplication. Dans le cas d'une demande, il figure dans une requestExtensions, tandis que dans le cas d'une réponse, il peut figurer dans une responseExtensions.

Appendice B

Outils et procédures d'apposition et de vérification de la signature numérique

InfoCert met à disposition un produit (ci-après dénommé « Dike ») qui peut être téléchargé gratuitement par les Propriétaires à partir du site www.firma.infocert.it pour permettre :

- de signer numériquement des documents à tous les Sujets en possession d'un certificat délivré par InfoCert ;
- la vérification de la signature apposée sur les documents signés numériquement selon les formats définis par les actes d'application du règlement.

Les environnements dans lesquels Dike fonctionne, les conditions matérielles et logicielles requises ainsi que toutes les instructions pour l'installation du produit sont disponibles à l'adresse web ci-dessus. Les instructions pour l'utilisation du produit sont incluses dans le produit lui-même et peuvent être consultées via la fonction d'aide. Le produit Dike est en mesure de signer tout type de fichier. Le fichier peut être visualisé si le poste de travail de l'utilisateur dispose d'un logiciel de visualisation approprié.

InfoCert peut mettre à disposition d'autres produits ou services de signature et/ou la vérification de signature. Ces produits ou services sont payants et dépendent des accords commerciaux établis au cas par cas avec les AE, les Demandeurs, les Sujets ou les Utilisateurs. Les documents électroniques signés avec des certificats délivrés par InfoCert peuvent également être vérifiés par l'intermédiaire d'autres outils en mesure d'interpréter les formats de signature requis. Ces outils ne relèvent pas de la responsabilité d'InfoCert.

Par exemple, les documents signés à l'aide de certificats délivrés dans le cadre de la présente Déclaration des Pratiques de Certification (*Certificate Practise Statement*), au format PAdES, peuvent également être vérifiés avec l'outil Adobe Reader®.

Avertissement

Certains formats permettent d'insérer du code exécutable (macros ou commandes) à l'intérieur du document sans altérer sa structure binaire, de manière à activer des fonctionnalités pouvant modifier les actes, les faits ou les données représentés dans le document en question. Les fichiers signés numériquement contenant ces structures ne produisent pas les effets visés à l'article 25, alinéa 2, du règlement [1], c'est-à-dire qu'ils ne peuvent être considérés comme équivalents à une signature manuscrite. Il est de la responsabilité du Propriétaire de s'assurer de l'absence de ce code exécutable par le biais des caractéristiques typiques de chaque produit.