InfoCert : *Vérification de l'identité*
déclaration sur les pratiques de service

Code du document	ICERT-INDI-IPSPS
Version	1.1
Date	10/07/2025

tinexta
infocert

1 INTRODUCTION

1.1 Vue d'ensemble

InfoCert est un prestataire de services de confiance qui offre également des services en ligne pour la vérification de l'identité des personnes physiques en vue de la délivrance de certificats.

Grâce aux services de vérification d'identité et de certificats qualifiés, les particuliers peuvent utiliser les signatures électroniques en toute légalité, conformément au règlement n° 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 (ci-après « eIDAS » ou « règlement eIDAS »).

En particulier, la solution SelfQ vérifie l'identité des personnes physiques conformément à l'article 24, paragraphe 1, point d), de l'eIDAS en utilisant « d'autres méthodes d'identification » reconnues par les réglementations nationales qui fournissent une assurance équivalente à la présence physique en termes de fiabilité.

Ce document est la Déclaration des pratiques de service de confiance pour la solution SelfQ. Il ne s'agit pas d'une déclaration de pratiques de certification (CPS - Certification Practice Statement) à part entière selon le RFC 3647, car elle ne concerne que la fourniture de services de vérification de l'identité et n'inclut pas d'autres services de certification tels que la délivrance de certificats ou les services de validation de certificats. (cf. ICERT-INDI-MO pour les services de certification InfoCert [10]).

L'objectif de ce document est de servir de base à la conformité à eIDAS.

1.2 Nom et identification du document

Ce document est intitulé « *InfoCert : Déclaration de pratique du service de vérification de l'identité* », portant l'identifiant de document suivant : **ICERT-INDI-IPSPS**. Pour obtenir des informations sur la version et le niveau de mise à jour, veuillez consulter l'en-tête de la page.

Le document décrit les politiques et les procédures mises en place pour gérer le Service de vérification de l'identité d'InfoCert en conformité avec le règlement eIDAS [1].

Ce document est associé à un ou plusieurs identificateurs d'objets (OID) décrits ci-dessous.
L'*identificateur d'objet* (OID - Object Identifier) qui identifie InfoCert est 1.3.76.36.

Les politiques relatives à la méthode d'identification sont énumérées ci-dessous :

Description	*OID*
Cas d'utilisation d'un document d'identité pour la vérification d'identité à distance sans surveillance, avec un fonctionnement hybride manuel et automatisé : SelfQ *(Conforme aux exigences de l'ETSI TS 119 461 établies au chapitre 9.2.3.3 « Cas d'utilisation pour un fonctionnement hybride manuel*	1.3.76.36.1.1.5000.34

et automatisé (Use case for hybrid manual and automated operation) »)	
Cas d'utilisation d'un document d'identité pour la vérification d'identité à distance sans surveillance, avec un fonctionnement hybride manuel et automatisé : SelfQ automatisé *(Conforme aux exigences de l'ETSI TS 119 461 établies au chapitre 9.2.3.4 « Cas d'utilisation pour un fonctionnement automatisé (Use case for automated operation) »)*	1.3.76.36.1.1.5000.34

Tableau 1 - Politiques relatives à la méthode de vérification de l'identité (Policies for identity proofing method)

1.3 Participants de l'IPSP

IPSP : Identity Proofing Service Provider ou Prestataire de services de vérification de l'identité

Les coordonnées complètes de l'organisation agissant en tant qu'IPSP sont les suivantes :

Nom de l'entreprise	**InfoCert S.p.A. - Société anonyme Société soumise à la gestion et à la coordination de Tinexta S.p.A.**
Siège social	**Piazzale Flaminio n.1/B, 00196, Rome, Italie**
Bureaux opérationnels	**Via Fernanda Wittgens n. 2, 20123 Milan (MI)** **Piazza Luigi da Porto n° 3, 35131 Padoue (PD)**
Représentant légal	**Danilo Cattaneo en tant que directeur général**
Numéro REA	**RM - 1064345**
Numéro de TVA	**07945211006**
Site web	**https://www.infocert.it**

TSP/QTSP : le prestataire de services qui gère le processus et délivre les certificats. Il pourrait s'agir d'InfoCert agissant en tant que QTSP.

Demandeur ou sujet : la personne faisant l'objet d'une identification.

Opérateur de back-office : personne formée qui suit les instructions de l'IPSP et examine les résultats de la validation.

1.4 Politique et Administration des pratiques

1.4.1 Contacts

InfoCert est responsable de la définition, de la mise à jour et de la publication de ce document. Pour toute question, plainte, commentaire ou demande d'éclaircissement concernant la présente déclaration sur les pratiques en matière de vérification de l'identité, veuillez vous adresser à

Nom de l'entreprise	**InfoCert – S.p.A** **Chef du QTSP** **Piazza Luigi da Porto n° 3, 35131 Padoue (PD)**
Numéro de téléphone	**+39 06 836691**
Signature numérique Centre de contact	**https://help.infocert.it/contatti/ pour plus de détails**
Site web	**https://www.firma.infocert.it,https://www.infocert.it**
Courriel	**firma.digitale@legalmail.it**

Les personnes concernées peuvent demander une copie de leur documentation personnelle en remplissant et en envoyant le formulaire disponible sur https://www.firma.infocert.it, et en suivant la procédure indiquée.

1.4.2 Parties responsables de l'approbation du présent document

La présente déclaration des pratiques du service de vérification de l'identité (ci-après dénommé « IPSPS ») a été approuvée par la direction de l'entreprise, après avoir été examinée par le responsable de la sécurité et de la politique, le responsable de la protection de la vie privée, le responsable des services de certification, le responsable du service juridique et le responsable des affaires réglementaires.

1.4.3 Procédures d'approbation

La rédaction et l'approbation de ce document sont effectuées conformément aux procédures décrites dans le système de gestion de la qualité ISO 9001:2015 de l'entreprise.

Au moins une fois par an, InfoCert vérifie la conformité de cette déclaration sur les pratiques en matière de vérification de l'identité avec son processus de service de certification.

1.5 Définitions et acronymes

1.5.1 Définitions

Termes	*Définition*
Cachet électronique avancé	un cachet électronique qui satisfait aux exigences énoncées à l'article 36 du règlement eIDAS (cf. eIDAS [1])
Signature électronique avancée	une signature électronique qui satisfait aux exigences énoncées à l'article 26 du règlement eIDAS (cf. eIDAS [1]).
Demandeur	Personne (morale ou physique) dont l'identité doit être prouvée [6].
Journal d'audit	L'ensemble des entrées automatiques ou manuelles d'événements, prévues dans les exigences techniques.
Contraignant pour le	Partie d'un processus de vérification de l'identité qui vérifie que le demandeur est

demandeur	bien la personne identifiée par la preuve présentée [6].
Organisme d'évaluation de la conformité (OEC)	Organisme accrédité en vertu du règlement eIDAS comme étant compétent pour évaluer la conformité d'un prestataire de services de confiance qualifié et des services de confiance qualifiés qu'il fournit. Il est responsable de la rédaction du CAR.
Rapport d'évaluation de la conformité (CAR - Conformity Assessment Report)	Rapport dans lequel l'organisme d'évaluation de la conformité confirme que le prestataire de services de confiance qualifié et ses services de confiance sont conformes aux exigences du règlement (cf. eIDAS [1]).
Client	Acteur avec lequel Infocert a formalisé un contrat de prestation de services en échange d'une rémunération.
Document d'identité numérique	Document d'identité délivré sous une forme traitable par machine, signé numériquement par l'émetteur et sous une forme purement numérique [6]
Document électronique	Tout contenu conservé sous forme électronique, notamment un texte ou un enregistrement sonore, visuel ou audiovisuel (cf. eIDAS [1]) .
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]).
Identification électronique	le processus consistant à utiliser des données d'identification personnelle sous une forme électronique représentant de manière univoque une personne physique ou morale, ou une personne physique représentant une personne morale (cf. eIDAS [1]).
Identité	Attribut ou ensemble d'attributs permettant d'identifier de manière unique une personne dans un contexte donné [6].
Document d'identité	Document physique ou numérique délivré par une source faisant autorité et attestant de l'identité du demandeur [6].
Vérification de l'identité (processus)	Processus par lequel l'identité d'un demandeur est vérifiée par l'utilisation de preuves attestant des attributs d'identité requis [6].
Identity Proofing Service Provider ou Prestataire de services de vérification de l'identité	Un IPSP (Identity Proofing Service Provider ou Prestataire de services de vérification d'identité) est une entité spécialisée qui fournit une preuve d'identité en tant que sous-traitant d'un Prestataire de services de confiance (TSP - Trust Service Provider), en fournissant un composant du service de confiance du TSP**.**
Détection du vivant	Mesure et analyse de caractéristiques anatomiques ou de réactions involontaires ou volontaires, afin de déterminer si un échantillon biométrique est prélevé sur un sujet vivant présent au point de prélèvement [6].
Données d'identification personnelle	Ensemble de données utilisées pour déterminer l'identité d'une personne physique et/ou morale ou d'une personne physique représentant une personne morale (cf. eIDAS [1]
Présence physique	Vérification de l'identité lorsque le demandeur est tenu d'être physiquement présent sur le lieu de la vérification de l'identité [6].
Attaque de présentation	Présentation au sous-système de saisie des données biométriques dans le but d'interférer avec le fonctionnement du système biométrique [5].
Détection d'attaque de présentation	Détermination automatisée d'une attaque de présentation [6].
Signature électronique qualifiée	Une signature électronique avancée qui est créée à l'aide d'un dispositif de création de signature électronique qualifiée et qui repose sur un certificat qualifié de signature électronique (cf. eIDAS [1]
Certificat qualifié de signature électronique	un certificat de signature électronique, qui est délivré par un prestataire de services de confiance qualifié et qui satisfait aux exigences fixées à l'annexe I du règlement eIDAS (cf. eIDAS [1]).
Service de confiance qualifié	Un service de confiance qui satisfait aux exigences applicables du règlement (cf. eIDAS [1]).
Qualified Trust Service Provider ou Prestataire de	Un prestataire de services de confiance qui fournit un ou plusieurs services de confiance qualifiés. Il a obtenu de l'organe de contrôle le statut qualifié (cf. eIDAS

services de confiance qualifié	[1]).
Partie utilisatrice	une personne physique ou morale qui se fie à une identification électronique ou à un service de confiance (cf. eIDAS [1]) .
Personne concernée	Personne morale ou physique inscrite auprès d'un service de confiance [6].
Abonné	personne physique ou morale liée par un accord avec un prestataire de services de confiance à toute obligation de l'abonné [6].
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 site internet ; ou c) en la conservation de signatures électroniques, de cachets électroniques ou des certificats relatifs à ces services (cf. eIDAS [1]) .
Déclaration des pratiques des services de confiance	déclaration des pratiques qu'un TSP emploie pour fournir un service de confiance [3].
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]) .
Vérification d'identité à distance sans surveillance	Processus de vérification de l'identité par l'utilisation à distance d'un document d'identité, dans lequel la capture du document d'identité (document physique ou numérique) et la vidéo du visage du demandeur sont effectuées dans le cadre d'une session automatisée et interactive, sans supervision humaine [6].
VIZ	La zone d'inspection visuelle du document d'identité est constituée d'un ensemble de zones de texte qui contiennent un ensemble prédéterminé d'informations de base.

1.5.2 Acronymes

Acronyme	*Signification*
AgID	Agenzia per l'Italia Digitale : Autorité de surveillance des prestataires de services de confiance
OEC	Organisme d'évaluation de la conformité
CAR	Conformity Assessment Report ou Rapport d'évaluation de la conformité
DNN	Deep Neural Network ou Réseau neuronal profond
eMRTD	Electronic Machine-Readable Travel Document ou Document de voyage électronique lisible à la machine
EIC	Electronic Identity Card ou Carte d'identité électronique
eIDAS	Electronic Identification, Authentication and Trust Services ou Services d'identification, d'authentification et de confiance électroniques [1]
eID	Electronic Identity ou Identité électronique
ETSI	European Telecommunications Standards Institute ou Institut européen de normalisation des télécommunications
RGPD	Règlement général sur la protection des données [2]
ISO	Organisation internationale de normalisation : Créée en 1946, l'ISO est une organisation internationale composée d'organismes nationaux de normalisation

IPSP	Identity Proofing Service Provider ou Prestataire de services de vérification de l'identité
IPSPS	Identity Proofing Service Practice Statement ou Déclaration des pratiques du service de vérification de l'identité
LoA	Level of Assurance ou Niveau d'assurance
MRZ	Machine Readable Zone ou Zone lisible par machine
OCR	Optical Character Recognition ou Reconnaissance optique de caractères
OID	Identificateur d'objet : une séquence de nombres enregistrés selon la procédure décrite dans la norme ISO/IEC 6523, qui fait référence à un objet spécifique au sein d'une hiérarchie
PAD	Presentation Attack Detection ou Détection d'attaques de présentation
PEC	Posta Elettronica Certificata (Courrier électronique certifié)
QTSP	Qualified Trust Service Provider ou Prestataire de services de confiance qualifié
TSP	Trust Service Provider ou Prestataire de services de confiance
VIZ	Visual Inspection Zone ou Zone d'inspection visuelle

1.6 Références

1. Règlement (UE) n° 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, version consolidée : 18/10/2024.

2. RGPD (Règlement général sur la protection des données) Règlement UE 679/2016 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.

3. ETSI EN 319 401 : « Signatures électroniques et infrastructures de confiance (ESI) ; exigences de politique générale pour les prestataires de services de confiance ».

4. ETSI EN 319 411-1 : « Signatures électroniques et infrastructures (ESI) ; exigences en matière de politique et de sécurité pour les prestataires de services de confiance délivrant des certificats ; partie 1 : Exigences générales".

5. ETSI EN 319 411-2 : « Signatures électroniques et infrastructures (ESI) ; exigences en matière de politique et de sécurité pour les prestataires de services de confiance délivrant des certificats ; partie 2 : Exigences applicables aux prestataires de services de confiance délivrant des certificats qualifiés de l'UE ».

6. ETSI TS 119 461 : « Signatures électroniques et infrastructures de confiance (ESI) ; exigences en matière de politique et de sécurité pour les composants de services de confiance fournissant une preuve d'identité des opérateurs de services de confiance ».

7. OACI Doc 9303, partie 3 : Documents de voyage lisibles à la machine Huitième édition, 2021 Partie 3 : Spécifications communes à tous les MRTD

8. OACI Doc 9303, partie 4 : Documents de voyage lisibles à la machine Huitième édition, 2021 Partie 4 : Spécifications pour les passeports lisibles à la machine (MRP) et autres MRTD de format TD3

9. OACI Doc 9303, partie 10 : « Document de voyage lisible à la machine - Partie 10 : Structure de données logiques (LDS) pour le stockage des données biométriques et autres dans le circuit intégré sans contact ».

10. InfoCert Politique de certification & Déclaration de pratiques de certification : ICERT-INDI-MO

11. Manuel de conservation InfoCert : 01_Preservation_Manual_of_InfoCert_ENG_2023

2 PROCESSUS DE VÉRIFICATION D'IDENTITÉ

2.1 Étapes du processus SelfQ

Le Demandeur est guidé tout au long d'un processus de bout en bout fournissant une identification sans surveillance, et composé des étapes suivantes :

Collecte des données :

Le Demandeur reçoit des conseils automatisés tout au long du processus de vérification d'identité, y compris les conditions permettant de mener à bien le processus de vérification d'identité.

Veuillez noter que seuls les documents d'identité numériques eMRT, conformes à la norme OACI 9303, partie 10 [9] sont acceptés.

- Le Demandeur capture des images de son document d'identité via une application mobile guidée ou une interface web (les téléchargements ne sont pas autorisés).
- Le service SelfQ OCR extrait les données du document d'identité, ce qui permet au Demandeur de confirmer ou de corriger des erreurs mineures.

Les documents d'identité varient en fonction des régions géographiques, des versions et de leur utilisation. Ils contiennent généralement des informations au recto et au verso (il existe peu de cas où les informations ne figurent qu'au recto). Le document d'identité peut être décrit par deux types d'informations.

Le premier, VIZ (**Visual Inspection Zone)**, contient des informations sur le propriétaire du document d'identité. Il contient les éléments suivants :

- Visage : Photographie du visage de la personne identifiée par ce document.
- Nœuds OCR : Ils contiennent les informations écrites du document telles que les noms, prénoms, dates, numéro d'identification, numéro de support, adresses, etc.
- Éléments de sécurité physique : Mesures de sécurité physique telles que les encres OVI, les micro-écritures, les kinégrammes, etc.

La MRZ **(Machine Readable Zone**) est la zone du document d'identité dans laquelle apparaissent les informations adaptées à la lecture par une machine. Elle comprend généralement deux lignes (passeport) ou trois lignes (cartes d'identité). cf. [7] et [8].

Comme prévu ci-dessus, les catégories de données extraites des documents d'identité peuvent varier en fonction du type de document et de son modèle de référence. Les données communes extraites peuvent être reprises comme suit.

- **Prénom**
- **Nom de famille**
- **Sexe**
- **Numéro d'identification fiscale**
- Date de naissance
- Lieu de naissance
- Nationalité
- Domicile
- Numéro du document
- Pays d'émission
- Valable à partir de (date)
- Valable jusqu'au (date)
- Lieu de délivrance

Validation des données :

- Le système vérifie si le document d'identité a été falsifié, la cohérence MRZ et VIZ, et les indicateurs antifraude (basés sur des contrôles de relecture et d'attaque à l'impression).
- Les informations de la MRZ sont extraites, validées et comparées aux informations de la partie visible du document d'identité.

Contraignante pour le Demandeur :

- Le Demandeur effectue une brève session vidéo pour la détection du vivant. Au cours de la session vidéo, exclusivement réalisée au moment du processus de vérification de l'identité, une capture vidéo est réalisée. Lorsque toutes les caractéristiques de qualité sont réunies (éclairage, position, résolution), le système prend automatiquement les photos du demandeur à partir de la vidéo et le logiciel les élabore en temps réel, en déterminant l'alignement correct du visage.
- Une fois l'image du visage du demandeur extraite, le système la compare à l'image extraite du document d'identité précédemment collecté.

La phase de détection du vivant répond au besoin de vérifier la présence et l'existence réelle de l'utilisateur, qui soumet son visage à la vérification par rapport à la photo extraite de son document d'identité. Le service permet de :

- Guider l'utilisateur dans le processus de cadrage de son visage pour prendre un selfie dans des conditions optimales :
  - Alignement du visage pendant la prise de vue.
  - Qualité de l'image capturée.
  - Lumière de l'image capturée.
- Effectuer une reconnaissance faciale « en direct » pendant la procédure.

Le module de détection du vivant permet de s'assurer qu'une personne réelle, et non une photo ou une vidéo en continu, se trouve devant l'appareil. InfoCert guide l'ensemble du processus

de collecte des données et crée une mini-vidéo dans laquelle les pixels sont analysés et traités automatiquement afin de prévenir les tentatives de fraude. Toutes les technologies reposent sur des composants d'IA très sophistiqués, consistant en des réseaux neuronaux, correctement entraînés avec un ensemble de coefficients qui minimisent les erreurs et permettent de classer les données entrantes. Ces données sont ensuite utilisées pour des activités de liaison.

Plus précisément, le module peut identifier les tentatives d'usurpation d'identité basées sur le même selfie que celui utilisé pour la comparaison des visages sans la participation de l'utilisateur et utilise une méthode basée sur le réseau neuronal profond (DNN), qui examine divers éléments de l'image pour détecter les artefacts aidant à faire la distinction entre la photo d'une personne en chair et en os et une attaque dite « de présentation ».

Le composant de détection du vivant d'InfoCert a été évalué en conformité avec la norme ISO/IEC 30107-3:2023, « *Information technology - Biometric presentation attack detection* » (Technologies de l'information — Détection d'attaque de présentation en biométrie) atteignant le niveau « substantial ». Des évaluations et des tests ont été pratiqués pour des attaques de type 1 (attaques de présentation) et de type 2 (attaques par injection).

En outre, le composant de détection du vivant est conforme aux caractéristiques spécifiées dans son objectif de sécurité pour le niveau d'évaluation substantiel tel que défini dans la norme CEN TS 18099 et le plan de test CLR Labs associé au niveau de certification Substantiel. Des tests ont été pratiqués sur les fonctions de détection des attaques par injection.

Le flux vidéo est transmis à un environnement qui garantit l'authenticité, l'intégrité et la confidentialité de l'élément produit.

Une fois la détection du vivant terminée, le composant de mise en correspondance automatique des visages compare le visage de l'utilisateur montré dans le selfie avec la photographie extraite du document d'identité.

La révision facultative des opérateurs de back-office garantit une précision accrue.

Publication du Résultat de la vérification d'identité :

Une fois que le système a effectué tous les contrôles et que le résultat est probant, un certificat qualifié peut être délivré.

Les données et les preuves sont conservées numériquement par le QTSP pendant la période prévue par les normes et réglementations locales. Si le QTSP est InfoCert, ces données et preuves sont conservées numériquement pendant 20 (vingt) ans.

3 CONTRÔLES DES INSTALLATIONS, DE LA GESTION ET DES OPÉRATIONS

InfoCert a mis en place un système de sécurité de l'information pour ses services de confiance. Le système de sécurité est divisé en trois niveaux :

- Niveau physique visant à garantir la sécurité des environnements dans lesquels le TSP gère le service.
- Un niveau procédural de nature strictement organisationnelle.
- Un niveau logique impliquant la fourniture de technologies matérielles et logicielles pour résoudre les problèmes et les risques associés au type de service et à l'infrastructure utilisée.

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

Un extrait de la politique de sécurité d'InfoCert peut être demandé par courrier électronique à l'adresse suivante *infocert@legalmail.it*.

Les politiques de sécurité d'InfoCert sont révisées au moins une fois par an et sont mises à jour pour tenir compte de tout changement pertinent. Chaque révision fait l'objet d'un suivi dans le document lui-même, même si aucune modification n'a été nécessaire.

Les contrôles de sécurité physique, la gestion des sites, l'accès physique, la prévention et la protection contre les inondations et les incendies, la gestion du stockage et d'autres contrôles opérationnels des installations et de la sécurité sont gérés par InfoCert agissant en tant que QTSP et décrits dans ICERT-INDI-MO [10].

3.1 Contrôles procéduraux du personnel

3.1.1 Rôles clés

Les rôles clés sont occupés par du personnel possédant l'expérience, le professionnalisme et l'expertise technique/juridique nécessaires, lesquels sont constamment vérifiés par des évaluations annuelles.

3.1.2 Qualifications, expérience et exigences en matière d'habilitation

À la suite de 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 de poste). Ensuite, en collaboration avec le Responsable de la Sélection du personnel, le processus de recherche et de sélection est déclenché. Les candidats sélectionnés participent au processus de sélection en prenant part à un premier entretien cognitif et motivationnel avec le Responsable de la Sélection du personnel puis à un entretien technique avec le Responsable de la fonction/structure organisationnelle, afin de vérifier les compétences déclarées par le candidat. Les exercices et les tests constituent des outils de vérification supplémentaires.

3.1.3 Exigences en matière de formation

Afin d'empêcher toute personne d'affecter ou d'altérer individuellement la sécurité globale du système ou d'effectuer des activités non autorisées, la gestion opérationnelle du système est confiée à différentes ressources, ayant chacune des tâches distinctes bien définies. Le

personnel chargé de la conception du service de vérification d'identité a été sélectionné pour son expérience dans la conception, la mise en œuvre et la gestion de services informatiques et pour ses caractéristiques de fiabilité et de confidentialité. Des sessions de formation sont prévues périodiquement pour sensibiliser aux tâches assignées. En particulier, avant l'intégration du personnel dans les activités opérationnelles, des cours de formation sont organisés pour fournir toutes les compétences (techniques, organisationnelles et procédurales) nécessaires à l'exécution des tâches assignées.

3.1.4 Fréquence de recyclage

Chaque début d'année, les besoins en formation sont analysés afin de définir les formations à organiser au cours de l'année. L'analyse est basée sur les étapes suivantes :

- Réunion avec la direction de l'entreprise pour recueillir des données sur les besoins de formation nécessaires afin d'atteindre les objectifs de l'entreprise.
- Retour d'information de la part des responsables de secteur afin d'identifier les besoins spécifiques de chaque secteur en matière de formation.
- Transmission des données collectées à la direction de l'entreprise pour la clôture et l'approbation du Plan de formation.

Une fois défini, le Plan de formation est communiqué au personnel en début d'année.

3.1.5 Sanctions pour les actions non autorisées

Des sanctions sont imposées aux employés conformément au Contrat national de travail des métallurgistes et installation d'établissements industriels privés (« CCNL Metalmeccanici e installazione impianti industria privata »).

3.1.6 Contrôles du personnel non salarié

L'accès au personnel non employé est régi par une politique spécifique de l'entreprise. Ce personnel participe à une formation adéquate.

3.1.7 Documentation à fournir par le personnel

Lors de leur recrutement, les employés doivent fournir une copie d'une pièce d'identité et d'une carte de santé en cours de validité et une photo d'identité pour leur badge d'accès. Ils devront ensuite remplir et signer un consentement écrit au traitement des données à caractère personnel et un accord de confidentialité, puis prendre connaissance du code de déontologie et de la politique en matière de nétiquette d'InfoCert.

4 LES PROCÉDURES D'ENREGISTREMENT DES AUDITS

4.1 Types d'événements enregistrés

Les preuves, les événements et les journaux du processus de vérification d'identité sont rassemblés et conservés conformément à la méthode de vérification d'identité choisie. Dans certains cas, selon le contexte, la preuve de validation peut également être recueillie et conservée.

Les procédures de gestion des preuves, des événements et des journaux liés au fonctionnement du service de vérification d'identité sont formalisées dans une procédure interne.

Elles sont collectées au moyen de procédures automatisées ad hoc.

4.2 Durée de conservation

Toutes les preuves, tous les journaux et tous les événements sont conservés pendant au moins 5 (cinq) ans, même si la vérification d'identité a été rejetée ; à la fin de la période de conservation définie, les preuves du processus de vérification d'identité et toutes les données à caractère personnel concernant le demandeur seront supprimées.
Le prestataire de vérification d'identité peut conserver les preuves et les journaux pendant une période plus longue sur la base d'accords spécifiques avec le TSP qui utilise le service.

4.3 Comment les preuves sont-elles conservées ?

Les preuves du processus de vérification d'identité sont conservées à l'abri de la chaleur, ce qui garantit la confidentialité des informations.

L'objectif est de garantir la possibilité de rechercher, d'extraire et de revérifier les résultats de la vérification d'identité, afin qu'ils soient facilement accessibles à la demande des autorités en charge de l'application des lois ou de la Personne concernée.

La preuve est stockée dans le système d'archivage InfoCert SAFE LTA (cf. 01_Preservation_Manual_of_InfoCert_ENG_2023) [11].

5 AUTRES QUESTIONS COMMERCIALES ET JURIDIQUES

5.1 Honoraires

Les frais des services de vérification d'identité sont soumis à des accords contractuels entre l'IPSP InfoCert et ses partenaires commerciaux.

5.2 Responsabilité financière

5.2.1 Couverture d'assurance

L'IPSP InfoCert dispose d'une assurance responsabilité civile professionnelle.

5.3 Informations personnelles Vie privée

Sauf autorisation expresse, toute information acquise par l'IPSP dans le cadre de ses activités courantes est confidentielle et non divulgable, à l'exception des informations spécifiquement destinées à un usage public. Les données personnelles sont traitées par l'IPSP conformément au décret législatif n° 196 du 30 juin 2003 et au règlement européen 2016/679 (RGPD) en vigueur depuis le 25 mai 2018 [2].

5.3.1 Plan de protection de la vie privée

InfoCert met en œuvre des politiques de protection des données à caractère personnel dans le cadre de son système certifié de gestion de la sécurité de l'information ISO 27001, gage d'une amélioration continue.

5.3.2 Informations personnelles

Les données à caractère personnel telles que définies par la législation applicable [2] désignent toute information concernant une personne **physique** et permettant de l'identifier, directement ou indirectement, y compris un numéro d'identification personnel.

Les employés d'InfoCert qui traitent des informations sont tenus de les protéger contre la compromission et la divulgation à des tiers.

Ils doivent respecter les lois italiennes relatives à la protection de la vie privée.

5.3.3 Responsable du traitement des données à caractère personnel

Nom de l'entreprise	**InfoCert S.p.A**
Siège social	**Piazzale Flaminio, 1/B**

	00196 Rome
Adresse électronique	**richieste.privacy@legalmail.it**

5.3.4 Divulgation de la vie privée et consentement

La politique de confidentialité d'InfoCert est disponible sur le site web www.infocert.it au lien suivant :

https://www.infocert.it/informative-privacy.

InfoCert traitera les données de la manière et sous la forme requises par la loi. Le traitement sera basé sur un fondement juridique approprié, décrit dans la politique de confidentialité.

Dans les cas où l'identification nécessite le traitement de données biométriques, InfoCert demandera le consentement avant de fournir le service.

Si le traitement est effectué par une autre entité juridique au nom d'InfoCert, la politique de confidentialité sera mise à disposition par le tiers, qui sera également responsable, si nécessaire, de l'obtention du consentement.

5.3.5 Divulgation à la suite d'une demande légale

InfoCert doit divulguer les informations demandées par les autorités, en suivant les procédures établies par l'autorité concernée.

5.4 Droits de propriété intellectuelle

Les droits d'auteur de ce document sont détenus par InfoCert. Tous droits réservés.

5.5 Déclarations et garanties

InfoCert reste responsable du respect de sa politique de sécurité de l'information, même lorsque certaines fonctions sont confiées à des tiers.

La Personne concernée est responsable de l'exactitude des données fournies. Si la Personne concernée dissimule son identité ou prétend faussement être quelqu'un d'autre par des méthodes telles que la falsification ou l'altération de documents, elle est responsable de tout dommage causé à l'IPSP et/ou à des tiers et doit indemniser l'IPSP de toute demande de dédommagement.

5.6 Exclusion de garantie

Aucune garantie n'est fournie.

5.7 Limitation de la responsabilité

InfoCert n'est pas responsable du contrôle du contenu, du type ou du format des documents transmis par la Personne concernée, ni de la validité et de la traçabilité de la procédure reflétant

l'intention réelle de la Personne concernée.

Sauf en cas de faute intentionnelle ou de négligence grave, InfoCert n'est pas responsable des dommages directs ou indirects causés aux Personnes concernées et/ou aux tiers en raison de l'utilisation ou de la non-utilisation des certificats d'abonnement délivrés après le processus de vérification d'identité.

InfoCert décline également toute responsabilité pour les dommages directs et/ou indirects découlant : (i) de la perte, (ii) du stockage incorrect, (iii) de l'utilisation incorrecte des outils d'identification et d'authentification et/ou (iv) du non-respect par la Personne concernée des recommandations susmentionnées.

En outre, InfoCert n'est pas responsable des dommages et/ou des retards dus à un dysfonctionnement du système ou du réseau pendant le processus de vérification d'identité.

Hormis en cas de faute intentionnelle ou de négligence grave , InfoCert n'est pas responsable des dommages directs ou indirects subis par la Personne concernée.

5.8 Indemnités

InfoCert est seul responsable des dommages directs, causés intentionnellement ou par négligence, à toute personne physique ou morale, en raison du non-respect de la réglementation eIDAS [1] et de l'absence de mise en œuvre de mesures appropriées pour prévenir les dommages.

Aucun remboursement ne sera accordé si les problèmes d'accès sont dus à une mauvaise utilisation du service de certification, à des problèmes de réseau de télécommunication ou à des événements indépendants de la volonté d'InfoCert, tels que la force majeure, les grèves, révoltes, tremblements de terre, actes de terrorisme, émeutes populaires, le sabotage organisé, les événements chimiques et/ou bactériologiques, guerres, inondations, mesures imposées par le gouvernement, matériel et/ou logiciel utilisé par le Demandeur.

5.9 Durée et résiliation

5.9.1 Termes et conditions

Le Demandeur est informé des termes et conditions, qui doivent être acceptés avant d'entamer le processus de vérification d'identité. Les termes et conditions peuvent s'appliquer à l'utilisation du service de confiance pour lequel la vérification d'identité est effectuée.

5.9.2 Résiliation

Le Contrat prend fin automatiquement avec l'interruption des services en cas de non-respect des conditions contractuelles. La résiliation intervient de plein droit lorsqu'une partie en informe l'autre partie par PEC ou par lettre recommandée a.r. Les effets du Contrat demeurent inchangés jusqu'à sa résiliation.

La Personne concernée admet qu'après la résiliation, le Service ne sera plus disponible.

Si InfoCert décide d'interrompre le service SelfQ, les clients en seront informés dans le délai de préavis convenu. Les preuves correspondantes seront toutefois conservées par InfoCert pendant la période requise.

5.10 Modifications

L'IPSP se réserve le droit de modifier ce document pour des raisons techniques ou pour se conformer à des changements légaux ou réglementaires. Chaque nouvelle version remplace les versions précédentes.

L'augmentation des numéros de publication du document indique des modifications qui n'ont pas d'impact significatif sur les parties utilisatrices, tandis que l'augmentation des numéros de version du document indique des modifications qui ont un impact significatif sur les parties utilisatrices (telles que des changements significatifs affectant les procédures d'exploitation). En tout état de cause, ce document sera rapidement publié et mis à disposition selon les modalités prescrites.

Les changements majeurs nécessitent un audit par un OEC accrédité, la soumission du rapport de certification (CAR - Conformity Assessment Report) et l'approbation de l'AgID avant la publication.

5.10.1 Historique des modifications

Informations	Description
Version/Publication :	1.1
Version/Date de publication (jj/mm/aaaa) :	10/07/2025
Description des changements :	Modifications de la formulation § 5.9 Modifications en cas de cessation du service
Raisons :	mise à jour du document

Informations	Description
Version/Publication :	1.0
Version/Date de publication (jj/mm/aaaa) :	15/03/2025
Description des changements :	
Raisons :	première version

6 ANNEXE

6.1 Technologies externalisées

Pour certains composants liés aux processus, InfoCert s'appuie sur les technologies fournies par les fournisseurs suivants :

- **VERIDAS DIGITAL AUTHENTICATION SOLUTIONS, S.L.**
  Disponible sur le lien suivant : https://veridas.com/en/.
  Veridas est le fournisseur de tous les éléments de collecte, d'extraction et de validation des données et des preuves, liés au processus d'identification de SelfQ.
  Pour renforcer la fiabilité du processus de collecte et de validation des preuves, seuls les documents d'identité numériques eMRT conformes à la partie 10 de l'OACI 9303 [9] sont acceptés par la solution Veridas.
  Veridas a obtenu les certifications ETSI TS 119 461 et ETSI EN 319 401, comme décrit sur le lien suivant https://veridas.com/en/compliance/

  IDrND
  Disponible sur le lien suivant : https://www.idrnd.ai/.
  Le module de détection du vivant d'InfoCert est mis à la disposition d'InfoCert par la R&D ID du prestataire. Ses composants sont conformes à la norme ISO 30107-3 et certifiés, comme indiqué dans la lettre de confirmation d'iBeta ci-dessous (disponible sur le lien suivant https://www.ibeta.com/wp-content/uploads/2020/10/200930-ID-RD-PAD-Level-2-Confirmation-Letter.pdf).