InfoCert: *Identitätsnachweis erklärung zur Dienstleistungspraxis*

Dokumentcode	ICERT-INDI-IPSPS
Version	1.1
Datum	10/07/2025

tinexta infocert

1 EINFÜHRUNG

1.1 Übersicht

InfoCert ist ein Anbieter von Vertrauensdiensten, der auch Online-Dienste zur Identitätsprüfung natürlicher Personen anbietet, um die Ausstellung von Zertifikaten zu unterstützen.

Durch Identitätsnachweis und qualifizierte Zertifikatsdienste können Einzelkunden elektronische Signaturen gemäß der Verordnung n legal nutzen. 910/2014 des Europäischen Parlaments und des Rates vom 23. Juli 2014 über elektronische Identifizierung und Vertrauensdienste für elektronische Transaktionen im Binnenmarkt (im Folgenden "eIDAS" oder "eIDAS-Verordnung").

Insbesondere überprüft SelfQ solution die Identität natürlicher Personen gemäß eIDAS, Artikel 24, Absatz 1 d), indem es "andere Identifizierungsmethoden" verwendet, die nach nationalen Vorschriften anerkannt sind und eine gleichwertige Zuverlässigkeit wie die physische Anwesenheit bieten.

Dieses Dokument ist das Trust Service Practice Statement für die SelfQ-Lösung. Es handelt sich nicht um ein vollständiges Certification Practice Statement (CPS) gemäß RFC 3647, da es sich nur auf die Bereitstellung von Identitätsprüfungsdiensten bezieht, nicht aber auf andere Zertifizierungsdienste wie die Ausstellung von Zertifikaten oder Zertifikatsvalidierungsdienste. (Siehe ICERT-INDI-MO für InfoCert-Zertifizierungsdienste [10]).

Dieses Dokument soll als Grundlage für die Einhaltung von eIDAS dienen.

1.2 Name und Identifikation des Dokuments

Dieses Dokument trägt den Titel "*InfoCert: Erklärung zur Praxis des Identitätsnachweisdienstes*" mit der folgenden Dokument-ID: **ICERT-INDI-IPSPS**. Informationen zur Version und zum Versionsstand finden Sie in der Kopfzeile der Seite.

Das Dokument beschreibt die Richtlinien und Verfahren zur Verwaltung des InfoCert Identity Proofing Service in Übereinstimmung mit der eIDAS-Verordnung [1].

Dieses Dokument ist mit einem oder mehreren der unten beschriebenen Object Identifiers (OID) verknüpft.
Der *Object Identifier* (OID), der InfoCert identifiziert, lautet 1.3.76.36.

Nachstehend sind die Richtlinien für die Identifizierungsmethode aufgeführt:

Beschreibung	*OID*
Anwendungsfälle mit einem Identitätsdokument für unbeaufsichtigte Fernzugriffe identitätsprüfung, mit manuellem und automatisiertem Betrieb: SelfQ	1.3.76.36.1.1.5000.34

(In Übereinstimmung mit den Anforderungen der ETSI TS 119 461 in Kapitel 9.2.3.3 "Anwendungsfall für hybriden manuellen und automatischen Betrieb")	
Anwendungsfälle mit einem Identitätsdokument für unbeaufsichtigte Fernzugriffe identitätsprüfung, mit manuellem und automatisiertem Betrieb: SelfQ automatisiert *(In Übereinstimmung mit den Anforderungen von ETSI TS 119 461 in Kapitel 9.2.3.4 "Anwendungsfall für den automatischen Betrieb")*	1.3.76.36.1.1.5000.34

Tabelle 1 - Richtlinien für Identitätsnachweisverfahren

1.3 IPSP-Teilnehmer

IPSP: Anbieter von Identitätsnachweisdiensten

Die vollständigen Angaben zu der Organisation, die als IPSP fungiert, finden Sie im Folgenden:

Name des Unternehmens	**InfoCert S.p.A. - Gesellschaft für Unternehmen Unternehmen unter der Verwaltung und Koordination von Tinexta S.p.a.**
Eingetragener Sitz	**Piazzale Flaminio n.1/B, 00196, Rom, Italien**
Operative Büros	**Über Fernanda Wittgens n. 2, 20123 Mailand (MI) Piazza Luigi da Porto n. 3, 35131 Padua (PD)**
Juristischer Vertreter	**Danilo Cattaneo als geschäftsführender Direktor**
REA-Nummer	**RM – 1064345**
Umsatzsteuer-Identifikationsnummer	**07945211006**
Website	**https://www.infocert.it**

TSP/QTSP: der Dienstanbieter, der den Prozess verwaltet und Zertifikate ausstellt. Es könnte InfoCert sein, das als QTSP auftritt.

Antragsteller oder Subjekt: die Person, die identifiziert werden soll.

Back-Office-Operator: eine geschulte Person, die die Anweisungen des IPSP befolgt und die Validierungsergebnisse überprüft.

1.4 Politik und Praxis Verwaltung

1.4.1 Kontakte

InfoCert ist für die Definition, Aktualisierung und Veröffentlichung dieses Dokuments verantwortlich. Bei Fragen, Beschwerden, Kommentaren und Bitten um Klarstellung zu dieser Erklärung zur Identitätsnachweispraxis wenden Sie sich bitte an:

Name des Unternehmens	**InfoCert - S.p.A Leiter von QTSP Piazza Luigi da Porto n. 3, 35131 Padua (PD)**
Telefonnummer	**+39 06 836691**
Digitale Unterschrift Contact Center	**https://help.infocert.it/contatti/ für weitere Einzelheiten**
Website	**https://www.firma.infocert.it,https://www.infocert.it**
E-Mail	**firma.digitale@legalmail.it**

Die Betroffenen können eine Kopie ihrer persönlichen Unterlagen beantragen, indem sie das auf https://www.firma.infocert.it verfügbare Formular ausfüllen und abschicken und das vorgegebene Verfahren befolgen.

1.4.2 Für die Genehmigung dieses Dokuments zuständige Stellen

Diese Erklärung zur Praxis des Identitätsnachweisdienstes (im Folgenden IPSPS) wurde von der Unternehmensleitung nach einer Überprüfung durch den Leiter der Abteilung Sicherheit und Politik, den Datenschutzbeauftragten, den Leiter der Zertifizierungsdienste, den Leiter der Rechtsabteilung und den Leiter der Abteilung für regulatorische Angelegenheiten genehmigt.

1.4.3 Genehmigungsverfahren

Die Erstellung und Genehmigung dieses Dokuments erfolgt gemäß den im Qualitätsmanagementsystem des Unternehmens ISO 9001:2015 beschriebenen Verfahren.

InfoCert prüft mindestens einmal im Jahr die Einhaltung dieses Identitätsnachweises im Rahmen seines Zertifizierungsdienstprozesses.

1.5 Definitionen und Akronyme

1.5.1 Begriffsbestimmungen

Begriff	*Definition*
Fortschrittliches elektronisches Siegel	Ein elektronisches Siegel, das die in Artikel 36 der eIDAS-Verordnung festgelegten Anforderungen erfüllt (siehe eIDAS [1])
Fortgeschrittene elektronische Signatur	Eine elektronische Signatur, die die Anforderungen von Artikel 26 der eIDAS-Verordnung erfüllt (siehe eIDAS [1]).
Antragsteller	Person (juristisch oder natürlich), deren Identität nachgewiesen werden soll [6].
Audit-Protokoll	Die Menge der automatischen oder manuellen Einträge von Ereignissen, die in den technischen Anforderungen vorgesehen sind.
Für den Antragsteller verbindlich	Teil eines Identitätsnachweisverfahrens, bei dem überprüft wird, ob der Antragsteller die Person ist, die durch die vorgelegten Nachweise identifiziert wird [6].

Konformitätsbewertungsstelle (KBS)	Gemäß der eIDAS-Verordnung akkreditierte Stelle, die für die Bewertung der Konformität eines qualifizierten Vertrauensdiensteanbieters und der von ihm erbrachten qualifizierten Vertrauensdienste zuständig ist. Sie ist für die Ausarbeitung des CAR zuständig.
Konformitätsbewertungsbericht (CAR)	Bericht, in dem die Konformitätsbewertungsstelle bestätigt, dass der qualifizierte Vertrauensdiensteanbieter und seine Vertrauensdienste den Anforderungen der Verordnung entsprechen (siehe eIDAS [1]).
Kunde	Subjekt, mit dem Infocert einen Dienstleistungsvertrag gegen Entgelt abgeschlossen hat.
Digitales Identitätsdokument	Identitätsdokument, das in maschinenverarbeitbarer Form ausgestellt wird, vom Aussteller digital signiert ist und in rein digitaler Form vorliegt [6]
Elektronisches Dokument	Jeder in elektronischer Form gespeicherte Inhalt, insbesondere Text oder Ton-, Bild- oder audiovisuelle Aufzeichnungen (siehe eIDAS [1]).
Elektronische Identifikationsmittel	Eine materielle und/oder immaterielle Einheit, die persönliche Identifikationsdaten enthält und für den Zugang zu Online-Diensten verwendet wird (siehe eIDAS [1]).
Elektronische Identifizierung	Der Prozess der Verwendung von Personenidentifikationsdaten in elektronischer Form, die entweder eine natürliche oder juristische Person oder eine natürliche Person, die eine juristische Person vertritt, eindeutig repräsentieren (siehe eIDAS [1]).
Identität	Attribut oder eine Reihe von Attributen, die eine Person in einem bestimmten Kontext eindeutig identifizieren [6].
Ausweisdokument	Physisches oder digitales Dokument, das von einer autorisierten Quelle ausgestellt wurde und die Identität des Antragstellers bescheinigt [6].
Identitätsnachweis (Prozess)	Verfahren, bei dem die Identität eines Antragstellers anhand von Nachweisen überprüft wird, die die erforderlichen Identitätsmerkmale bescheinigen [6].
Anbieter von Identitätsnachweisdiensten	Ein IPSP (Identity Proofing Service Provider) ist eine spezialisierte Einrichtung, die als Unterauftragnehmer eines Vertrauensdiensteanbieters (TSP) Identitätsnachweise erbringt und eine Komponente des Vertrauensdienstes des TSP liefert**.**
Erkennung des Vorhandenseins	Messung und Analyse anatomischer Merkmale oder unwillkürlicher oder freiwilliger Reaktionen, um festzustellen, ob eine biometrische Probe von einer lebenden Person, die sich am Ort der Erfassung befindet, erfasst wird [6].
Persönliche Identifikationsdaten	Eine Reihe von Daten, die zur Feststellung der Identität einer natürlichen und/oder juristischen Person oder einer natürlichen Person, die eine juristische Person vertritt, verwendet werden (siehe eIDAS [1]
Physische Präsenz	Identitätsnachweis, wenn der Antragsteller am Ort des Identitätsnachweises physisch anwesend sein muss [6].
Präsentation Angriff	Vorlage beim Teilsystem für die Erfassung biometrischer Daten mit dem Ziel, den Betrieb des biometrischen Systems zu stören [5].
Erkennung von Präsentationsangriffen	Automatisierte Bestimmung eines Präsentationsangriffs [6].
Qualifizierte elektronische Signatur	Eine fortgeschrittene elektronische Signatur, die von einer qualifizierten elektronischen Signaturerstellungseinheit erstellt wird und die auf einem qualifizierten elektronischen Signaturzertifikat basiert (siehe eIDAS [1]
Qualifiziertes Zertifikat für elektronische Signaturen	Elektronisches Signaturzertifikat, das von einem qualifizierten Vertrauensdiensteanbieter ausgestellt wird und den Anforderungen des Anhangs I der eIDAS-Verordnung entspricht (siehe eIDAS [1]).
Qualifizierter Treuhanddienst	Ein Vertrauensdienst, der die in der Verordnung festgelegten Anforderungen erfüllt (siehe eIDAS [1]).
Qualifizierter Anbieter von Treuhanddienstleistungen	Ein Anbieter von Treuhanddiensten, der einen oder mehrere qualifizierte Treuhanddienste anbietet. Der qualifizierte Status wird von der Aufsichtsbehörde verliehen (siehe eIDAS [1]).

Verlässliche Partei	Eine natürliche oder juristische Person, die sich auf eine elektronische Identifizierung oder einen Vertrauensdienst (siehe eIDAS [1]).
Thema	Juristische oder natürliche Person, die sich bei einem Treuhanddienst angemeldet hat [6].
Abonnent	eine juristische oder natürliche Person, die durch eine Vereinbarung mit einem Vertrauensdiensteanbieter an irgendwelche Teilnehmerpflichten gebunden ist [6].
Vertrauensdienst	Ein elektronischer Dienst, der in der Regel gegen Entgelt erbracht wird und aus folgenden Leistungen besteht: a) die Erstellung, Überprüfung und Validierung von elektronischen Signaturen, Siegeln oder Zeitstempeln, zertifizierten elektronischen Zustelldiensten und entsprechenden Zertifikaten oder b) die Erstellung, Überprüfung und Validierung von Zertifikaten für die Website-Authentifizierung, oder c) die Aufbewahrung von elektronischen Signaturen, Siegeln oder Zertifikaten im Zusammenhang mit diesen Diensten (siehe eIDAS [1]).
Erklärung zur Dienstleistungspraxis des Trusts	erklärung zu den Praktiken, die ein TSP bei der Erbringung eines Vertrauensdienstes anwendet [3].
Vertrauensdiensteanbieter	Eine natürliche oder juristische Person, die einen oder mehrere Vertrauensdienste entweder als qualifizierter oder als nicht qualifizierter Vertrauensdiensteanbieter erbringt (siehe eIDAS [1]).
Unbeaufsichtigte Remote-Identitätsüberprüfung	Identitätsnachweisverfahren durch Fernverwendung eines Identitätsdokuments, bei dem die Erfassung des Identitätsdokuments (physisches oder digitales Dokument) und das Gesichtsvideo des Antragstellers in einer automatisierten, interaktiven Sitzung ohne menschliche Aufsicht durchgeführt werden [6].
VIZ	Die visuelle Inspektionszone eines ID-Dokuments besteht aus einer Reihe von Textbereichen, die eine Reihe von Basisinformationen enthalten.

1.5.2 Akronyme

Akronym	*Bedeutung*
AgID	Agenzia per l'Italia Digitale: Aufsichtsbehörde für Vertrauensdiensteanbieter
CAB	Konformitätsbewertungsstelle
CAR	Konformitätsbewertungsbericht
DNN	Tiefes neuronales Netzwerk
eMRTD	Elektronisches maschinenlesbares Reisedokument
EIC	Elektronischer Personalausweis
eIDAS	Elektronische Identifizierung, Authentifizierung und Vertrauensdienste [1]
eID	Elektronische Identität
ETSI	Europäisches Institut für Telekommunikationsnormen
GDPR	Allgemeine Datenschutzverordnung [2]
ISO	Internationale Organisation für Normung: Die 1946 gegründete ISO ist eine internationale Organisation, die sich aus nationalen Normungsgremien zusammensetzt
IPSP	Anbieter von Identitätsnachweisdiensten

IPSPS	Praxiserklärung des Identitätsnachweisdienstes
LoA	Grad der Gewissheit
MRZ	Maschinenlesbare Zone
OCR	Optische Zeichenerkennung
OID	Objektidentifikator: eine Zahlenfolge, die nach dem in ISO/IEC 6523 beschriebenen Verfahren registriert wird und auf ein bestimmtes Objekt innerhalb einer Hierarchie verweist
PAD	Erkennung von Präsentationsangriffen
PEC	Posta Elettronica Certificata (Zertifizierte E-Mail)
QTSP	Qualifizierter Anbieter von Treuhanddienstleistungen
TSP	Vertrauensdiensteanbieter
VIZ	Zone für visuelle Inspektion

1.6 Referenzen

1. Verordnung (EU) Nr. 910/2014 des Europäischen Parlaments und des Rates vom 23. Juli 2014 über elektronische Identifizierung und Vertrauensdienste für elektronische Transaktionen im Binnenmarkt und zur Aufhebung der Richtlinie 1999/93/EG, konsolidierte Fassung: 18/10/2024.

2. GDPR (General Data Protection Regulation) EU-Verordnung 679/2016 des Europäischen Parlaments und des Rates vom 27. April 2016 zum Schutz natürlicher Personen bei der Verarbeitung personenbezogener Daten und zum freien Verkehr dieser Daten.

3. ETSI EN 319 401: "Elektronische Signaturen und Vertrauensinfrastrukturen (ESI); Allgemeine Anforderungen an Vertrauensdiensteanbieter".

4. ETSI EN 319 411-1: "Elektronische Signaturen und Infrastrukturen (ESI); Richtlinien und Sicherheitsanforderungen für Vertrauensdiensteanbieter, die Zertifikate ausstellen; Teil 1: Allgemeine Anforderungen".

5. ETSI EN 319 411-2: "Elektronische Signaturen und Infrastrukturen (ESI); Richtlinien und Sicherheitsanforderungen für Vertrauensdiensteanbieter, die Zertifikate ausstellen; Teil 2: Anforderungen an Vertrauensdiensteanbieter, die EU-qualifizierte Zertifikate ausstellen".

6. ETSI TS 119 461: "Elektronische Signaturen und Vertrauensinfrastrukturen (ESI); Richtlinien und Sicherheitsanforderungen für Vertrauensdienstkomponenten, die den Identitätsnachweis von Vertrauensdienstsubjekten erbringen".

7. ICAO Doc 9303 Teil 3: Maschinenlesbare Reisedokumente Achte Ausgabe, 2021 Teil 3: Gemeinsame Spezifikationen für alle MRTDs

8. ICAO Doc 9303 Teil 4: Maschinenlesbare Reisedokumente Achte Ausgabe, 2021 Teil4: Spezifikationen für maschinenlesbare Pässe (MRP) und andere MRTDs der Größe TD3

9. ICAO Doc 9303 Teil 10: "Maschinenlesbares Reisedokument - Teil 10: Logische Datenstruktur (LDS) für die Speicherung von biometrischen und anderen Daten in der kontaktlosen integrierten Schaltung (IC)".

10. InfoCert-Zertifikatsrichtlinie & Erklärung zur Zertifikatspraxis: ICERT-INDI-MO

11. Konservierungshandbuch InfoCert: 01_Handbuch_der_InfoCert_ENG_2023

2 IDENTITÄTSNACHWEISVERFAHREN

2.1 SelfQ Prozessschritte

Der Antragsteller wird durch einen durchgängigen Prozess geführt, der eine unbeaufsichtigte Identifizierung ermöglicht und aus den folgenden Schritten besteht:

Datenerhebung:

Der Antragsteller wird während des gesamten Identitätsnachweisverfahrens automatisch angeleitet, einschließlich der Bedingungen, unter denen das Identitätsnachweisverfahren erfolgreich abgeschlossen werden kann.

Bitte beachten Sie, dass nur digitale eMRT-Ausweisdokumente, die den Anforderungen von ICAO 9303 Teil 10 [9] akzeptiert werden.

- Der Antragsteller erfasst Bilder seines Ausweises über eine geführte mobile App oder eine Webschnittstelle (Uploads sind nicht erlaubt).
- Der SelfQ OCR-Service extrahiert Daten aus dem Ausweisdokument und ermöglicht es dem Antragsteller, kleinere Fehler zu bestätigen oder zu korrigieren.

Identitätsdokumente unterscheiden sich je nach geografischer Region, Version und Verwendung. Sie enthalten in der Regel Informationen sowohl auf der Vorder- als auch auf der Rückseite (es gibt nur wenige Fälle, in denen die Informationen nur auf der Vorderseite zu finden sind). Das ID-Dokument kann durch zwei Arten von Informationen beschrieben werden.

Die erste ist die VIZ**(Visual Inspection Zone)**, in der die Informationen über den Inhaber des Ausweises erscheinen. Sie enthält die folgenden Elemente:

- Gesicht: Foto des Gesichts der Person, die durch dieses Dokument identifiziert wird.
- OCR-Knoten: Sie enthalten die schriftlichen Informationen des Dokuments wie Namen, Nachnamen, Daten, Identifikationsnummer, Unterstützungsnummer, Adressen usw.
- Physische Sicherheitsmerkmale: Physische Sicherheitsmaßnahmen wie OVI-Tinten, Mikroschrift, Kinegramme usw.

MRZ**(Machine Readable Zone**) ist der Bereich des Identitätsdokuments, in dem maschinenlesbare Informationen erscheinen. Er besteht im Allgemeinen aus zwei Zeilen (Reisepass) oder drei Zeilen (Personalausweis). Siehe [7] und [8].

Wie bereits erwähnt, können die aus Identitätsdokumenten extrahierten Datenkategorien je nach Art des Dokuments und seiner Referenzvorlage

unterschiedlich sein. Die extrahierten gemeinsamen Daten können wie folgt wieder aufgenommen werden.

- **Vorname**
- **Nachname**
- **Sex**
- **Steuernummer**
- Geburtsdatum
- Geburtsort
- Nationalität
- Wohnsitz - Adresse
- Nummer des Dokuments
- Ausstellendes Land
- Gültig ab (Datum)
- Gültig bis (Datum)
- Ort der Ausstellung

Validierung der Daten:

- Das System prüft, ob das Ausweisdokument manipuliert wurde, die MRZ- und VIZ-Konsistenz sowie Betrugsbekämpfungsindikatoren (basierend auf Replay- und Print-Attack-Checks).
- Die Informationen aus der MRZ werden extrahiert, validiert und mit den Informationen aus dem sichtbaren Teil des Identitätsdokuments verglichen.

Für den Antragsteller verbindlich:

- Der Antragsteller führt eine kurze Videositzung zur Erkennung von Liveness durch. Während der Videositzung, die ausschließlich zum Zeitpunkt der Identitätsfeststellung durchgeführt wird, wird eine Videoaufnahme gemacht. Wenn alle Qualitätsmerkmale übereinstimmen (Beleuchtung, Position, Auflösung), nimmt das System automatisch die Bilder des Bewerbers aus dem Video auf und die Software bearbeitet sie in Echtzeit, um die korrekte Ausrichtung des Gesichts zu bestimmen.
- Sobald das Bild des Gesichts des Antragstellers extrahiert ist, vergleicht das System es mit dem Bild, das aus dem zuvor erfassten Ausweisdokument extrahiert wurde.

In der Phase zur Erkennung des Lebens des Benutzers muss dessen Anwesenheit und tatsächliche Existenz überprüft werden, indem sein Gesicht mit dem Foto aus seinem Ausweis verglichen wird. Der Dienst ermöglicht es:

- Führen Sie den Benutzer durch den Prozess des Einrahmens seines Gesichts, um ein Selfie zu machen, das optimale Bedingungen für die Aufnahme bietet:
  - Ausrichtung des Gesichts während des Schnappschusses.
  - Qualität des aufgenommenen Bildes.
  - Licht des aufgenommenen Bildes.

- Führen Sie während des Verfahrens eine "Live"-Gesichtserkennung durch.

Das Modul zur Lebendigkeitserkennung stellt sicher, dass sich eine reale Person vor der Kamera befindet und nicht ein Foto oder ein Videostream. InfoCert steuert den gesamten Datenerfassungsprozess und erstellt ein Mini-Video, in dem die Pixel automatisch analysiert und verarbeitet werden, um Betrugsversuche zu verhindern. Die gesamte Technologie stützt sich auf hochentwickelte KI-Komponenten, die aus neuronalen Netzen bestehen, die mit einer Reihe von Koeffizienten trainiert wurden, die den Fehler minimieren und die eingehenden Daten klassifizieren können, die dann für verbindliche Aktivitäten verwendet werden.

Das Modul kann insbesondere Fälschungsversuche auf der Grundlage desselben Selfies erkennen, das für den Gesichtsabgleich ohne Beteiligung des Nutzers verwendet wird, und verwendet eine auf dem so genannten Deep Neural Network (DNN) basierende Methode, die verschiedene Elemente des Bildes untersucht, um Artefakte zu erkennen, die dabei helfen, zwischen dem Foto einer echten Person und einem so genannten "Präsentationsangriff" zu unterscheiden.

Die InfoCert Liveness Detection Komponente wurde in Übereinstimmung mit der ISO/IEC 30107-3:2023 Norm "*Information technology - Biometric presentation attack detection*" evaluiert und erreichte die Stufe "substantial". Es wurden Auswertungen und Tests für Angriffe des Typs 1 (Präsentationsangriffe) und des Typs 2 (Injektionsangriffe) durchgeführt.

Darüber hinaus entspricht die Komponente zur Erkennung von Liveness den Merkmalen, die in den Sicherheitsvorgaben für die wesentliche Evaluationsstufe gemäß CEN TS 18099 und dem zugehörigen CLR-Labs-Testplan für die wesentliche Zertifizierungsstufe spezifiziert sind. Es wurden Tests zur Erkennung von Injektionsangriffen durchgeführt.

Der Videostream wird in eine Umgebung übertragen, die die Authentizität, Integrität und Vertraulichkeit des erzeugten Elements gewährleistet.

Nach Abschluss der Erkennung der Echtheit vergleicht die Komponente für den automatischen Gesichtsabgleich das auf dem Selfie gezeigte Gesicht des Benutzers mit dem aus dem Ausweisdokument extrahierten Foto.

Die optionale Überprüfung durch die Back-Office-Mitarbeiter sorgt für zusätzliche Genauigkeit.

Freigabe des Ergebnisses des Identitätsnachweises:

Wenn alle Prüfungen durch das System mit einem positiven Ergebnis durchgeführt wurden, kann ein qualifiziertes Zertifikat ausgestellt werden.

Die Daten und Nachweise werden von der QTSP für den Zeitraum gemäß den örtlichen Normen und Vorschriften digital aufbewahrt. Handelt es sich bei dem QTSP um InfoCert, werden die Daten und Nachweise 20 (zwanzig) Jahre lang digital aufbewahrt.

3 EINRICHTUNG, VERWALTUNG UND OPERATIVE KONTROLLEN

InfoCert hat ein Informationssicherheitssystem für seine vertrauenswürdigen Dienste eingeführt. Das Sicherheitssystem ist in drei Stufen unterteilt:

- Eine physische Ebene, die darauf abzielt, die Sicherheit von Umgebungen zu gewährleisten, in denen TSP den Dienst verwaltet.
- Eine verfahrenstechnische Ebene mit rein organisatorischem Charakter.
- Eine logische Ebene, die die Bereitstellung von Hardware- und Softwaretechnologie umfasst, um die mit der Art des Dienstes und der verwendeten Infrastruktur verbundenen Probleme und Risiken zu bewältigen.

Mit diesem Sicherheitssystem sollen Risiken vermieden werden, die sich aus der Störung von Systemen, Netzen und Anwendungen sowie aus dem unbefugten Abfangen oder der Veränderung von Daten ergeben.

Ein Auszug aus der InfoCert-Sicherheitspolitik kann per E-Mail angefordert werden unter *infocert@legalmail.it.*

Die Sicherheitsrichtlinien von InfoCert werden mindestens einmal im Jahr überprüft und bei relevanten Änderungen aktualisiert. Jede Überprüfung wird im Dokument selbst nachverfolgt, auch wenn keine Änderungen erforderlich waren.

Physische Sicherheitskontrollen, Standortmanagement, physischer Zugang, Schutz vor Überschwemmungen und Bränden, Lagermanagement und andere Betriebskontrollen für Einrichtungen und Sicherheit werden von InfoCert als QTSP verwaltet und in ICERT-INDI-MO beschrieben [10].

3.1 Personelle Verfahrenskontrollen

3.1.1 Schlüsselrollen

Die Schlüsselpositionen werden von Mitarbeitern besetzt, die über die erforderliche Erfahrung, Professionalität und das technische/juristische Fachwissen verfügen, was durch jährliche Bewertungen ständig überprüft wird.

3.1.2 Qualifikationen, Erfahrung und Sicherheitsanforderungen

Im Anschluss an die jährliche Personalplanung legt der Leiter der Funktion/Organisationsstruktur die Merkmale und Fähigkeiten der einzusetzenden Ressource fest (Stellenprofil). Anschließend werden in Zusammenarbeit mit dem Staff Selection Manager das Such- und Auswahlverfahren eingeleitet. Die ausgewählten Bewerber nehmen am Auswahlverfahren teil, indem sie an einem ersten kognitiv-motivationalen Gespräch mit dem Leiter der Personalauswahl und an einem anschließenden fachlichen Gespräch mit dem Leiter der Funktion/Organisationsstruktur teilnehmen, um die von den Bewerbern angegebenen

Fähigkeiten zu überprüfen. Weitere Überprüfungsinstrumente sind Übungen und Tests.

3.1.3 Anforderungen an die Ausbildung

Um zu verhindern, dass eine einzelne Person die Sicherheit des Gesamtsystems beeinträchtigt oder verändert oder unbefugte Tätigkeiten ausführt, wird das Betriebsmanagement des Systems verschiedenen Ressourcen anvertraut, die jeweils separate und genau definierte Aufgaben haben. Das für die Entwicklung des Identitätsnachweises zuständige Personal wurde aufgrund seiner Erfahrung in der Entwicklung, Implementierung und Verwaltung von IT-Diensten sowie aufgrund seiner Zuverlässigkeit und Vertraulichkeit ausgewählt. In regelmäßigen Abständen werden Schulungen geplant, um das Bewusstsein für die zugewiesenen Aufgaben zu schärfen. Insbesondere werden vor der Eingliederung des Personals in die operativen Tätigkeiten Schulungen durchgeführt, um alle erforderlichen (technischen, organisatorischen und verfahrenstechnischen) Fähigkeiten zur Ausführung der zugewiesenen Aufgaben zu vermitteln.

3.1.4 Häufigkeit der Umschulung

Zu Beginn eines jeden Jahres wird der Schulungsbedarf analysiert, um die im Laufe des Jahres zu veranstaltenden Schulungen festzulegen. Die Analyse basiert auf den folgenden Schritten:

- Treffen mit der Unternehmensleitung, um Daten über den Schulungsbedarf zu sammeln, der zur Erreichung der Unternehmensziele erforderlich ist.
- Feedback von den Bereichsleitern, um den spezifischen Schulungsbedarf der einzelnen Bereiche zu ermitteln.
- Weiterleitung der gesammelten Daten an die Unternehmensleitung zum Abschluss und zur Genehmigung des Ausbildungsplans.

Der einmal festgelegte Ausbildungsplan wird zu Beginn des Jahres an die Mitarbeiter weitergegeben.

3.1.5 Sanktionen für unbefugte Handlungen

Sanktionen werden dem Personal gemäß dem nationalen Arbeitsvertrag für Metallarbeiter und Installateure privater Industrieanlagen ("CCNL Metalmeccanici e installazione impianti industria privata") auferlegt.

3.1.6 Kontrollen des nicht beschäftigten Personals

Der Zugang zu nicht angestelltem Personal wird durch eine spezielle Unternehmensrichtlinie geregelt. Sie nehmen an einer angemessenen Ausbildung teil.

3.1.7 Vom Personal vorzulegende Dokumentation

Bei der Einstellung müssen die Mitarbeiter eine Kopie eines gültigen Personalausweises sowie eine Kopie einer gültigen Gesundheitskarte und ein Passfoto für ihren Zugangsausweis vorlegen. Anschließend müssen sie eine schriftliche Zustimmung zur Verarbeitung personenbezogener Daten und eine Vertraulichkeitsvereinbarung ausfüllen und unterzeichnen sowie den Ethikkodex und die Netiquette von InfoCert lesen.

4 AUDIT-PROTOKOLLIERUNGSVERFAHREN

4.1 Arten von protokollierten Ereignissen

Beweise, Ereignisse und Protokolle des Identitätsprüfungsprozesses werden in Übereinstimmung mit der gewählten Identitätsprüfungsmethode gesammelt und aufbewahrt. In einigen Fällen kann, je nach Kontext, auch der Validierungsnachweis erfasst und aufbewahrt werden.

Die Verfahren für die Verwaltung von Nachweisen, Ereignissen und Protokollen im Zusammenhang mit dem Betrieb des Identitätsnachweisdienstes sind in einem internen Verfahren formalisiert.

Sie werden mit Hilfe automatisierter Ad-hoc-Verfahren erhoben.

4.2 Aufbewahrungsfrist

Alle Nachweise, Protokolle und Ereignisse werden für mindestens 5 (fünf) Jahre aufbewahrt, auch wenn der Identitätsnachweis abgelehnt wurde nach Ablauf der festgelegten Aufbewahrungsfrist werden die Nachweise des Identitätsnachweisverfahrens und alle personenbezogenen Daten des Antragstellers gelöscht.
Der Anbieter des Identitätsnachweises kann die Nachweise und Protokolle über einen längeren Zeitraum auf der Grundlage spezifischer Vereinbarungen mit dem FDA, der den Dienst nutzt, aufbewahren.

4.3 Wie werden die Beweismittel gespeichert?

Der Nachweis des Identitätsnachweises wird temperatursicher aufbewahrt, so dass die Vertraulichkeit der Informationen gewährleistet ist.

Ziel ist es, die Möglichkeit zu gewährleisten, die Ergebnisse des Identitätsnachweises zu suchen, abzurufen und erneut zu überprüfen, um sie auf Anfrage der Strafverfolgungsbehörden oder der betroffenen Person leicht zugänglich zu halten.

Der Nachweis wird im Archivierungssystem InfoCert SAFE LTA gespeichert (siehe 01_Aufbewahrung_Handbuch_von_InfoCert_ENG_2023) [11].

5 SONSTIGE GESCHÄFTLICHE UND RECHTLICHE ANGELEGENHEITEN

5.1 Vergütung

Die Gebühren für die Identitätsprüfungsdienste unterliegen den vertraglichen Vereinbarungen zwischen InfoCert IPSP und seinen Geschäftspartnern.

5.2 Finanzielle Verantwortung

5.2.1 Versicherungsschutz

InfoCert IPSP unterhält eine Berufshaftpflichtversicherung.

5.3 Persönliche Informationen Datenschutz

Sofern nicht ausdrücklich gestattet, sind alle Informationen, die das IPSP im Rahmen seiner routinemäßigen Tätigkeiten erhält, vertraulich und dürfen nicht weitergegeben werden, es sei denn, es handelt sich um Informationen, die speziell für die Öffentlichkeit bestimmt sind. Die Verarbeitung personenbezogener Daten durch das IPSP erfolgt gemäß dem Gesetzesdekret Nr. 196 vom 30. Juni 2003 und der europäischen Verordnung 2016/679 (GDPR), die am 25. Mai 2018 in Kraft getreten ist2].

5.3.1 Plan zum Schutz der Privatsphäre

InfoCert setzt die Richtlinien zum Schutz personenbezogener Daten im Rahmen seines ISO 27001-zertifizierten Managementsystems für Informationssicherheit um und gewährleistet so eine kontinuierliche Verbesserung.

5.3.2 Persönliche Informationen

Personenbezogene Daten im Sinne der geltenden Gesetzgebung [2 sind alle Informationen über eine **natürliche** Person, mit denen diese direkt oder indirekt identifiziert werden kann, einschließlich einer persönlichen Identifikationsnummer.

InfoCert-Mitarbeiter, die mit Informationen umgehen, sind verpflichtet, diese vor Kompromittierung und Weitergabe an Dritte zu schützen.

Sie müssen die italienischen Datenschutzgesetze einhalten.

5.3.3 Verantwortlicher für die personenbezogenen Daten Verarbeitung

Name des Unternehmens	**InfoCert S.p.A**

Eingetragener Sitz	**Piazzale Flaminio n. 1/B** **00196 - Rom**
E-Mail	**richieste.privacy@legalmail.it**

5.3.4 Offenlegung der Privatsphäre und Zustimmung

Die Datenschutzpolitik von InfoCert ist auf der Website www.infocert.it unter dem folgenden Link:

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

InfoCert verarbeitet die Daten in der gesetzlich vorgeschriebenen Weise und Form. Die Verarbeitung erfolgt auf der Grundlage einer geeigneten Rechtsgrundlage, wie in der Datenschutzerklärung beschrieben.

In Fällen, in denen die Identifizierung die Verarbeitung biometrischer Daten erfordert, wird InfoCert vor der Erbringung der Dienstleistung die Zustimmung einholen.

Wird die Verarbeitung von einer anderen juristischen Person im Auftrag von InfoCert durchgeführt, so wird die Datenschutzerklärung von der dritten Partei zur Verfügung gestellt, die gegebenenfalls auch für die Einholung der Zustimmung verantwortlich ist.

5.3.5 Offenlegung aufgrund rechtlicher Anforderungen

InfoCert muss die von den Behörden angeforderten Informationen gemäß den von der jeweiligen Behörde festgelegten Verfahren offenlegen.

5.4 Rechte an geistigem Eigentum

Das Urheberrecht an diesem Dokument liegt bei InfoCert. Alle Rechte vorbehalten.

5.5 Zusicherungen und Garantien

InfoCert bleibt für die Einhaltung seiner Informationssicherheitspolitik verantwortlich, auch wenn bestimmte Funktionen an Dritte ausgelagert werden.

Das Subjekt ist für die Richtigkeit der angegebenen Daten verantwortlich. Verheimlicht die betroffene Person ihre Identität oder gibt sie sich fälschlicherweise als eine andere Person aus, z.B. durch Fälschung oder Veränderung von Dokumenten, so haftet sie für den Schaden, der dem IPSP und/oder Dritten entsteht, und muss das IPSP von allfälligen Schadenersatzforderungen freistellen.

5.6 Gewährleistungsausschluss

Es werden keine Garantien gegeben.

5.7 Haftungsbeschränkung

InfoCert ist nicht verantwortlich für die Überwachung des Inhalts, der Art oder des Formats der vom Subjekt übermittelten Dokumente sowie für die Sicherstellung der Gültigkeit und Nachvollziehbarkeit des Verfahrens, das die tatsächliche Absicht des Subjekts widerspiegelt.

Außer im Falle von Vorsatz oder grober Fahrlässigkeit haftet InfoCert nicht für direkte oder indirekte Schäden, die den Subjekten und/oder Dritten durch die Verwendung oder Nichtverwendung von Abonnementzertifikaten entstehen, die nach dem Identitätsnachweisverfahren ausgestellt wurden.

InfoCert lehnt auch die Verantwortung für direkte und/oder indirekte Schäden ab, die sich ergeben aus: (i) Verlust, (ii) unsachgemäßer Aufbewahrung, (iii) unsachgemäßer Verwendung von Identifizierungs- und Authentifizierungsinstrumenten und/oder (iv) der Nichtbeachtung der oben genannten Empfehlungen durch das Subjekt.

Darüber hinaus haftet InfoCert nicht für Schäden und/oder Verzögerungen aufgrund von System- oder Netzwerkfehlern während des Identitätsprüfungsprozesses.

Außer im Falle von Vorsatz oder grober Fahrlässigkeit haftet InfoCert nicht für direkte oder indirekte Schäden des Subjekts.

5.8 Entschädigungen

InfoCert ist allein verantwortlich für direkte Schäden, die einer natürlichen oder juristischen Person aufgrund der Nichteinhaltung der eIDAS-Vorschriften vorsätzlich oder fahrlässig zugefügt werden [1] und das Versäumnis, geeignete Maßnahmen zur Schadensvermeidung zu ergreifen.

Rückerstattungen werden nicht gewährt, wenn Zugangsprobleme auf eine unsachgemäße Nutzung des Zertifizierungsdienstes, auf Probleme im Telekommunikationsnetz oder auf Ereignisse zurückzuführen sind, die außerhalb des Einflussbereichs von InfoCert liegen, wie z. B. höhere Gewalt, Streiks, Aufstände, Erdbeben, Terrorakte, Volksaufstände, organisierte Sabotage, chemische und/oder bakteriologische Ereignisse, Krieg, Überschwemmungen, behördlich angeordnete Maßnahmen, vom Antragsteller verwendete Hard- und/oder Software.

5.9 Laufzeit und Beendigung

5.9.1 Laufzeits & Bedingungen

Der Antragsteller wird über die Bedingungen & informiert, die er vor Beginn des Identitätsnachweisverfahrens akzeptieren muss. Für die Nutzung des Vertrauensdienstes, für den der Identitätsnachweis erbracht wird, können die Geschäftsbedingungen gelten.

5.9.2 Kündigung

Der Vertrag endet automatisch mit der Unterbrechung der Dienstleistungen bei Nichteinhaltung der Vertragsbedingungen. Die Kündigung erfolgt von Rechts wegen, wenn eine Partei die andere Partei per PEC oder Einschreiben a.r. benachrichtigt. Die Wirkungen des Vertrags bleiben bis zu seiner Beendigung unberührt.

Das Subjekt nimmt zur Kenntnis, dass der Dienst nach der Kündigung nicht mehr verfügbar ist.

Wenn InfoCert beschließt, den SelfQ-Service einzustellen, werden die Kunden innerhalb der vereinbarten Kündigungsfrist benachrichtigt. Die entsprechenden Nachweise werden jedoch von InfoCert für den erforderlichen Zeitraum aufbewahrt.

5.10 Änderungsanträge

Das IPSP behält sich das Recht vor, dieses Dokument aus technischen Gründen oder zur Anpassung an gesetzliche oder regulatorische Änderungen zu ändern. Jede neue Version ersetzt die vorherigen Versionen.

Steigende Versionsnummern von Dokumenten weisen auf Änderungen hin, die sich nicht wesentlich auf die vertrauenden Parteien auswirken, während steigende Versionsnummern von Dokumenten auf Änderungen hinweisen, die sich wesentlich auf die vertrauenden Parteien auswirken (z. B. wesentliche Änderungen der Betriebsverfahren). In jedem Fall wird dieses Dokument unverzüglich veröffentlicht und auf den vorgeschriebenen Wegen zugänglich gemacht.

Größere Änderungen erfordern ein Audit durch eine akkreditierte KBS, die Vorlage des Zertifizierungsberichts (CAR - Conformity Assessment Report) und die Genehmigung der AgID vor der Veröffentlichung.

5.10.1 Geschichte der Änderungen

Informationen	Beschreibung
Version/Freigabe:	1.1
Version/Veröffentlichungsdatum (gg/mm/aaaa):	10/07/2025
Beschreibung der Änderungen:	Bearbeitungen zur Umformulierung § 5.9 Bearbeitungen bei Beendigung des Dienstes
Die Gründe:	aktualisierung des Dokuments

Informationen	Beschreibung
Version/Freigabe:	1.0
Version/Veröffentlichungsdatum (gg/mm/aaaa):	15/03/2025
Beschreibung der Änderungen:	
Die Gründe:	erste Version

6 ANHANG

6.1 Ausgelagerte Technologien

Für einige prozessbezogene Komponenten greift InfoCert auf die Technologien der folgenden Anbieter zurück:

- **VERIDAS DIGITAL AUTHENTICATION SOLUTIONS, S.L.**
  Verfügbar unter folgendem Link: https://veridas.com/en/.
  Veridas bietet alle Komponenten der Daten- und Beweismittelerfassung, -extraktion und -validierung im Zusammenhang mit dem SelfQ-Identifizierungsprozess an.
  Um die Zuverlässigkeit der Beweiserhebung und -validierung zu erhöhen, dürfen nur digitale eMRT-Dokumente verwendet werden, die der ICAO 9303 Teil 10 [9 von der Veridas-Lösung akzeptiert werden.
  Veridas hat die Zertifizierungen ETSI TS 119 461 und ETSI EN 319 401 erhalten, wie unter dem folgenden Link beschrieben https://veridas.com/en/compliance/

  IDrND
  Verfügbar unter folgendem Link: https://www.idrnd.ai/.
  Das InfoCert Liveness Detection Modul wird InfoCert von dem Anbieter ID R&D zur Verfügung gestellt. Die Komponenten des Moduls entsprechen der Norm ISO 30107-3 und sind entsprechend zertifiziert, wie aus dem Bestätigungsschreiben von iBeta hervorgeht (unter folgendem Link abrufbar https://www.ibeta.com/wp-content/uploads/2020/10/200930-ID-RD-PAD-Level-2-Confirmation-Letter.pdf).