Beschreibung der Zertifizierungspraxis

Certificate Policy
Certificate Practice Statement

DOKUMENTEN-CODE	ICERT-INDI-MO*
VERSION	4.4
DATUM	10.02.2021

* Ab Version 4.0 sind die Unterlagen ICERT-INDI-MO und ICERT-INDI-MO-ENT in dieses Dokument aufgenommen worden

InfoCert
TINEXTA GROUP

INHALTSVERZEICHNIS

VERZEICHNIS DER ABBILDUNGEN

1 EINLEITUNG

1.1 Allgemeines

Ein Zertifikat verknüpft den öffentlichen Schlüssel mit Gesamtinformationen, die die Person identifizieren, die den entsprechenden privaten Schlüssel besitzt: Diese natürliche oder juristische Person ist der **Zertifikatsinhaber**. Das Zertifikat wird von anderen Personen benutzt, um den mit dem Zertifikat verteilten öffentlichen Schlüssel abzurufen und die qualifizierte elektronische Signatur zu prüfen, die auf einem Dokument angebracht oder mit ihm verbunden ist. Das Zertifikat garantiert die Zuordnung des öffentlichen Schlüssels zu dem Zertifikatsinhaber. Die Zuverlässigkeitsstufe dieser Verknüpfung ist mit verschiedenen Faktoren verbunden: die Verfahrensweise, mit der die Certification Authority (Zertifizierungsstelle) das Zertifikat ausgestellt hat, die Sicherheitsmaßnahmen, die von dem Zertifikatsinhaber übernommenen Pflichten für den Schutz seines privaten Schlüssels, die angebotenen Garantien.
Bei diesem Dokument handelt es sich um die Beschreibung der Zertifizierungspraxis des **Vertrauensdiensteanbieters InfoCert** (*Trust Service Provider*) der als Vertrauensdienste auch qualifizierte elektronische Signaturen bereitstellt. Die Beschreibung enthält die Richtlinien und die Vorgehensweisen, die in dem Identifizierungsverfahren und bei der Erstellung des qualifizierten Zertifikats befolgt werden, die ergriffenen Sicherheitsmaßnahmen, die Pflichten, die Garantien und die Haftung und allgemein alles, was ein qualifiziertes Zertifikat vertrauenswürdig macht, in Übereinstimmung mit den geltenden Rechtsvorschriften über Vertrauensdienste, qualifizierte elektronische Signaturen und Siegel und digitale Signaturen.
Mit der Veröffentlichung einer solchen Beschreibung der Zertifizierungspraxis und mit Aufnahme der Verweisungen auf ein solches Dokument in die Zertifikate ist es den Nutzern möglich, die Eigenschaften und die Zuverlässigkeit des Zertifizierungsdienstes, also die Verknüpfung zwischen Schlüsseln und Zertifikatsinhaber, zu beurteilen.
Der Inhalt basiert auf die zum Ausstellungsdatum geltenden Rechtsvorschriften und setzt die Empfehlungen des Dokuments „Request for Comments: 3647 – Internet X.509 Public Key Infrastructure Certificate Policy and Certification Practices Framework" © Internet Society 2003, um.

Diese Beschreibung der Zertifizierungspraxis enthält außerdem die Richtlinien und die Vorgehensweisen, die InfoCert bei der Prüfung der Anträge, der Identifizierung der Antragsteller und der Ausstellung der Zertifikate für die Website-Authentifizierung lt. Art 34 der delegierten Verordnung (EU) 2018/389 [12] zur Umsetzung der Richtlinie (EU) 2015/2366 (PSD2) [11] entsprechend den durch den Standard ETSI TS 119 495 festgelegten Anforderungen befolgt (nachstehend „PSD2-Zertifikate").

1.2 Name und Kennung des Dokuments

Dieses Dokument heißt „Vertrauensdiensteanbieter InfoCert – Beschreibung der Zertifizierungspraxis " und besitzt folgenden Dokumenten-Code: **ICERT-INDI-MO**. Die Version und der Stand finden sich in der Kopfzeile jeder Seite.

Die Version 4.0 dieses Dokuments ist die aktuelle Version und ersetzt die vorherigen Beschreibungen der Zertifizierungspraxis mit den Bezeichnungen:

- ICERT-INDI-MO, Version 3.5 vom 30.11.2018 für die Ausstellung von qualifizierten Zertifikaten an eine natürliche und juristische Person über ein CMS.
- ICERT-INDI-MO-ENT, Version 3.5 vom 30.11.2018 für die Ausstellung von qualifizierten LongTerm- und OneShot-Zertifikaten an eine natürliche Person.

Dabei werden in einem einzigen Dokument die Richtlinien und Verfahren für die Verwaltung der qualifizierten Zertifikate gemäß der eIDAS-Verordnung [1] beschrieben.

Dem Dokument sind die nachfolgend erläuterten Object Identifier (OID) zugeordnet, auf die je nach ihrer bestimmungsgemäßen Verwendung in der CertificatePolicy-Erweiterung der Zertifikate verwiesen wird. Die Bedeutung der OID ist folgende:

Der *Object Identifier* (OID), der InfoCert identifiziert, ist 1.3.76.36.

Die Policies für qualifzierte Zertifikate:

Beschreibung der Zertifizierungspraxis -qualifiziertes Zertifikat ausgestellt für natürliche Person	1.3.76.36.1.1.48.1 gemäß der Policy QCP-n-qscd 0.4.0.194112.1.0
Beschreibung der Zertifizierungspraxis -qualifiziertes Zertifikat ausgestellt für natürliche Person und Schlüssel auf Einheit (SSCD)	1.3.76.36.1.1.48.2 gemäß der Policy QCP-n-qscd 0.4.0.194112.1.0
Beschreibung der Zertifizierungspraxis -qualifiziertes Zertifikat ausgestellt für juristische Person, auch auf qualifizierter Einheit Auch verfügbar für PSD2 (QSealC)	1.3.76.36.1.1.47 gemäß der Policy QCP-n-qscd 0.4.0.194112.1.1

Die Policies für qualifzierte Zertifikate auf qualifizierter Einheit:

Beschreibung der Zertifizierungspraxis -qualifiziertes Zertifikat ausgestellt für natürliche Person und Schlüssel auf qualifizierter Einheit (SSCD)	1.3.76.36.1.1.1/1.3.76.36.1.1.61 gemäß der Policy QCP-n-qscd 0.4.0.194112.1.2
Beschreibung der Zertifizierungspraxis -qualifiziertes Zertifikat ausgestellt für natürliche Person für automatischen Fernsignatur auf Einheit (QSCD)	1.3.76.36.1.1.2/1.3.76.36.1.1.62 gemäß der Policy QCP-n-qscd 0.4.0.194112.1.2
Beschreibung der Zertifizierungspraxis -qualifiziertes Zertifikat ausgestellt für natürliche Person für Fernsignatur auf Einheit (QSCD)	1.3.76.36.1.1.22/1.3.76.36.1.1.63 gemäß der Policy QCP-n-qscd 0.4.0.194112.1.2
Beschreibung der Zertifizierungspraxis -qualifiziertes Zertifikat ausgestellt für natürliche Person über CMS auf (QSCD)	1.3.76.36.1.1.32/1.3.76.36.1.1.66 gemäß der Policy QCP-n-qscd 0.4.0.194112.1.2
Beschreibung der Zertifizierungspraxis -qualifiziertes Zertifikat ausgestellt für juristische Person auf Einheit (QSCD)	1.3.76.36.1.1.46 gemäß der Policy QCP-n-qscd 0.4.0.194112.1.3

Auch verfügbar für PSD2 (QSealC)	
Beschreibung der Zertifizierungspraxis für qualifizierte Zertifikate ausgestellt für natürliche Personen für Fernsignatur auf einer qualifizierten Einheit	1.3.76.36.1.1.35/1.3.76.36.1.1.65 gemäß Policy QCP-n-qscd 0.4.0.194112.1.2
Beschreibung der Zertifizierungspraxis für qualifizierte Zertifikate ausgestellt für natürliche Personen für Fernsignatur auf qualifizierter Einheit Typ One-Shot	1.3.76.36.1.1.34/1.3.76.36.1.1.64 gemäß Policy QCP-n-qscd 0.4.0.194112.1.2

In dem Zertifikat können zusätzliche OID vorhanden sein, um das Vorliegen von Verwendungsbeschränkungen anzugeben. Diese OID sind in § 4.5.3aufgelistet. Bestehende Verwendungsbeschränkungen ändern keinesfalls die übrigen Regeln der Beschreibung der Zertifizierungspraxis.
Darüber hinaus enthalten ab dem 5. Juli 2019 alle Zertifikate, die den Empfehlungen der Entscheidung AgID Nr. 121/2019 entsprechen, ein weiteres PolicyIdentifier-Element mit dem Wert agIDcert (OID 1.3.76.16.6) im Feld CertificatePolicies (OID 2.5.29.32).[1] Dieses Dokument ist in elektronischer Form auf der Website des Vertrauensdiensteanbieters veröffentlicht: http://www.firma.infocert.it, Bereich „Documentazione“.

1.3 Teilnehmer und Haftung

1.3.1 Certification Authority – Zertifizierungsstelle

Die **Certification Authority** ist die dritte und vertrauenswürdige Person, die die qualifizierten Zertifikate für qualifizierte elektronische Signaturen durch deren Signatur mit ihrem eigenen privaten Schlüssel, genannt CA- oder Root-Schlüssel, erstellt.
InfoCert ist die Certification Authority (**CA**), die die qualifizierten Zertifikate ausstellt, im Verzeichnis veröffentlicht und widerruft. Sie handelt dabei gemäß den technischen Vorschriften der Aufsichtsbehörde sowie den Vorgaben der eIDAS-Verordnung [1] und des Codice dell’Amministrazione Digitale (italienischer Kodex der digitalen Verwaltung – CAD) [2].

Die vollständigen Daten der Organisation, die die CA-Funktion ausübt, sind folgende:

Firma	**InfoCert – Società per azioni** **Gesellschaft, die der Leitung und Koordinierung der Tinexta S.p.A. unterliegt.**
Sitz	Piazza Sallustio n.9, 00187, Roma (RM)
Betriebsstätte	Via Marco e Marcelliano n.45, 00147, Roma (RM)
Gesetzlicher Vertreter	Danilo Cattaneo als geschäftsführendes Verwaltungsratsmitglied

[1] Das Fehlen des besagten OID kann eine Unangemessenheit der angebotenen Netzdienste in Italien zur Folge haben. Ein Beispiel in diesem Zusammenhang ist die mangelnde Verpflichtung, im qualifizierten Zertifikat für die Signaturerstellung die Steuernummer des Inhabers anzugeben, ein unerlässliches Element für verschiedene italienische Behörden.

Telefon	06 836691
HR-Nummer	Steuernummer 07945211006
USt-Nr.	07945211006
Website	https://www.infocert.it

1.3.2 Registration Authority – Registrierungsstelle (RA)

Die **Registration Authorities oder Registrierungsstellen** sind Personen, denen die CA einen spezifischen Auftrag mit Vertretung erteilt hat und mit dem sie die Durchführung einer oder mehrerer Tätigkeiten des Registrierungsverfahrens überträgt. Hierzu gehören zum Beispiel:

- die Identifizierung des Zertifikatsinhabers oder des Antragstellers,
- die Registrierung der Daten des Zertifikatsinhabers,
- die Weiterleitung der Daten des Zertifikatsinhabers an die Systeme der CA,
- die Entgegennahme des Antrags für das qualifizierte Zertifikat,
- die Verteilung und/oder Initialisierung der sicheren Signatureinheit, soweit vorhanden,
- die Aktivierung des Zertifizierungsverfahrens des öffentlichen Schlüssels,
- die Bereitstellung von Support an den Zertifikatsinhaber, den Antragsteller und die CA in den etwaigen Phasen der Erneuerung, des Widerrufs und der Suspendierung der Zertifikate.

Die Registration Authority führt im Wesentlichen alle Schnittstellentätigkeiten zwischen der Certification Authority und dem Zertifikatsinhaber oder dem Antragsteller auf Grundlage der getroffenen Vereinbarungen aus. Der Vertretungsauftrag, „RAO-Vereinbarung“ genannt, regelt die Art der Tätigkeiten, die die CA der RA anvertraut, sowie die operative Durchführung.
Die RA werden von der CA nach einer angemessenen Schulung des zuständigen Personals aktiviert. Die CA überprüft, ob die verwendeten Verfahren den Bestimmungen dieser Beschreibung entsprechen.

1.3.2.1 Der Registrierungsbeauftragte (RB)

Die RA kann unter Verwendung eigens dafür bestimmter Formulare natürliche oder juristische Personen benennen, denen die Durchführung der Identifizierung des Zertifikatsinhabers überantwortet wird. Die **Registrierungsbeauftragten** sind auf Grundlage der Anweisungen tätig, die sie von der RA erhalten, der sie unterstehen und die die Aufgabe besitzt, die Ordnungsmäßigkeit der Vorgehensweise zu überwachen.

1.3.3 Zertifikatsinhaber

Der **Zertifikatsinhaber** ist die natürliche oder juristische Person, die Inhaber des qualifizierten Zertifikats ist, in dem die wesentlichen zur Identifizierung dienden Daten enthalten sind. Der Zertifikatsinhaber kann in einigen Teilen der Beschreibung und in einigen Verwendungsbeschränkungen auch als Inhaber definiert sein.

1.3.4 Nutzer

Es handelt sich um die Person, die ein mit dem digitalen Zertifikat des Zertifikatsinhabers signiertes elektronisches Dokument erhält und sich auf die Gültigkeit dieses Zertifikats (und/oder der dort

vorhandenen elektronischen Signatur) stützende um die Ordnungsmäßigkeit und die Gültigkeit des Dokuments in dem Kontext beurteilt, in dem es benutzt wird.

1.3.5 Antragsteller

Es handelt sich um die natürliche oder juristische Person, die bei der CA die Ausstellung von digitalen Zertifikaten für einen Zertifikatsinhaber unter eventueller Übernahme der Kosten beantragt sowie die Befugnis besitzt, diese Zertifikate zu suspendieren oder zu widerrufen. Diese eventuell vorhandene Rolle kann auch von der RA übernommen werden.
Im Einzelnen handelt es sich um die folgenden Fälle:

- Er kann mit dem Zertifikatsinhaber identisch sein, wenn dieser eine natürliche Person ist;
- Er kann die natürliche Person sein, die zur Beantragung eines Zertifikats für eine juristische Person berechtigt ist;
- Er kann mit der juristischen Person identisch sein, die das Zertifikat für natürliche Personen beantragt, die mit ihm durch Geschäftsbeziehungen oder im Rahmen von Organisationen verbunden sind;
- Er kann im Fall einer minderjährigen Person über 14 Jahre ein Elternteil oder ein Erziehungsberechtigter sein.

Der Antragsteller kann die natürliche oder juristische Person sein, von der die Signaturbefuggnisse oder die Rolle des Zertifikatsinhabers stammen. In diesem Fall, wo der Antragsteller auch als *betroffener Dritter* definiert wird, enthält das Zertifikat die Angabe der Organisation, mit der der Zertifikatsinhaber verbunden ist und/oder bei der er eine Rolle innehat.
Sofern in der Vertragsdokumentation nichts anders bestimmt, sind der Antragsteller und der Zertifikatsinhaber identisch.

1.3.6 Behörde

1.3.6.1 Agenzia per l'Italia Digitale – AgID

Die Agenzia per l'Italia Digitale (**AgID**) ist eine Aufsichtsstelle für Vertrauensdiensteanbieter im Sinne von Artikel 17 der eIDAS-Verordnung. Die AgID übt in dieser Eigenschaft die Aufsicht über die in Italien niedergelassenen qualifizierten Vertrauensdiensteanbieter aus, um zu gewährleisten, dass diese die von der Verordnung festgelegten Anforderungen erfüllen.

1.3.6.2 Conformity Assessment Body – Konformitätsbewertungsstelle

Die Konformitätsbewertungsstelle (**CAB**, das Akronym für Conformity Assessment Body) ist eine nach der eIDAS-Verordnung eine akkreditierte Stelle, die dafür zuständig ist, die Konformität des qualifizierten Vertrauensdiensteanbieters und der von ihm erbrachten qualifizierten Vertrauensdienste mit den geltenden Rechtsvorschriften und Normen zu bewerten.

1.3.6.3 Zuständige nationale Behörde (NCA)

In Sachen PSD2[11] ist die nationale Aufsichtsbehörde der Finanzintermediäre die für die Autorisierung der PSPs zuständige Stelle jedes Mitgliedstaates. Nach Erteilung der Autorisierung stellt die NCA eine Autorisierungsnummer aus und veröffentlicht besagte Information in ihren öffentlichen Registern.

1.3.6.4 Europäische Bankaufsichtsbehörde (EBA)

Die europäische Bankaufsichtsbehörde (**EBA**) trägt dazu bei, ein gleichförmiges Regulierungs- und Aufsichtsniveau im europäischen Bankwesen sicherzustellen. In Sachen PSD2[11] beaufsichtigt und garantiert sie die Transparenz der Tätigkeit der von den für jeden Mitgliedstaat zuständigen NCA autorisierten Zahlungsdienstleister (PSP). Die Behörde entwickelt und führt ein „elektronisches zentrales Register", in dem jede NCA das Verzeichnis der Namen und die Angaben der autorisierten Personen veröffentlichen muss.

1.4 Verwendung des Zertifikats

1.4.1 Zulässige Verwendung

Die Zertifikate, die von der CA InfoCert gemäß den in dieser Beschreibung der Zertifizierungspraxis erläuterten Verfahrensweisen erstellt werden, sind qualifizierte Zertifikate im Sinne des CAD und der eIDAS-Verordnung.

Das von der CA erstellte Zertifikat wird zur Überprüfung der qualifizierten Signatur oder des elektronischen Siegels des Zertifikatsinhabers verwendet, dem das Zertifikat gehört.

Die CA InfoCert stellt zur Überprüfung der Signaturen die auf der Website InfoCert verfügbaren Produkte bereit. Auf dem Markt können andere Überprüfungsprodukte mit Funktionen und Beschränkungen gemäß den Angaben des Lieferanten verfügbar sein.

1.4.2 Unzulässige Verwendung

Es ist nicht erlaubt, das Zertifikat außerhalb des begrenzten Bereichs und der Kontexte, die in der Beschreibung der Zertifizierungspraxis und in den Verträgen im Einzelnen genannt sind, bzw. unter Verstoß gegen die in dem Zertifikat definierten Nutzungs- und Wertbeschränkungen (*key usage*, *extended key usage, user notice*) zu verwenden.

1.5 Verwaltung der Beschreibung der Zertifizierungspraxis

1.5.1 Kontakte

InfoCert ist für die Definition, Veröffentlichung und Aktualisierung dieses Dokuments verantwortlich. Fragen, Beschwerden, Hinweise oder Ersuchen um Klärungen in Bezug auf diese Beschreibung der Zertifizierungspraxis sind an die folgende Adresse und Person zu richten:

InfoCert S.p.A.
Responsabile del Servizio di Certificazione Digitale
Piazza Luigi da Porto 3
35131 Padova
Telefon: 06 836691
Fax: 049 0978914
Callcenter: 06 54641489
Web: https://www.firma.infocert.it
E-Mail: firma.digitale@legalmail.it

Der Zertifikatsinhaber oder der Antragsteller können eine Kopie der sie betreffenden Dokumentation anfordern. Hierzu ist das auf der Website www.firma.infocert.it bereitgestellte Formular unter Befolgung des dort erläuterten Verfahrens auszufüllen und zuzusenden. Die Dokumentation wird auf elektronischem Weg an die im Formular angegebene E-Mail-Adresse übermittelt.

1.5.2 Verantwortliche Personen für die Genehmigung der Beschreibung der Zertifizierungspraxis

Diese Beschreibung der Zertifizierungspraxis wird vom Leiter der Sicherheit und der Richtlinien, dem Leiter für Datenschutz, dem Leiter des Servicebereichs Zertifizierungen, der Rechtsabteilung und der Beratungsabteilung geprüft und vom Management des Unternehmens genehmigt.

1.5.3 Genehmigungsprozess

Die Abfassung und Genehmigung der Beschreibung der Zertifizierungspraxis erfolgen gemäß den Prozessen der Qualitätsmanagement-Norm ISO 9001:2015.
Der Vertrauensdiensteanbieter führt ein Mal im Jahr eine Konformitätsprüfung dieser Beschreibung der Zertifizierungspraxis im Hinblick auf ihre Verfahren bei der Erbringung des Zertifizierungsdienstes durch.

1.6 Definitionen und Akronyme

1.6.1 Definitionen

Es folgen die Definitionen, die bei der Erstellung dieses Dokuments verwendet wurden. Für die von der eIDAS-Verordnung [1] und dem CAD [2] definierten Begriffe wird auf die dortigen Begriffsbestimmungen verwiesen. Wo es zweckmäßig ist, wird der entsprechende englische Begriff, der allgemein in der Publizistik, den Normen und in technischen Unterlagen verwendet wird, in eckige Klammern gesetzt.

Vertragsende	Definition
Selbstzertifizierung	Es ist die persönliche Erklärung der Person, die Zertifikatsinhaber des digitalen Zertifikats sein wird, gegenüber der CA durch Unterzeichnung des Vorliegens von Ständen, Fakten, Qualitäten mit Übernahme der gesetzlich vorgesehenen Haftungen.
CAB – Conformity Assessment Body (Konformitätsbewertungsstelle)	Eine Stelle, die gemäß der eIDAS-Verordnung als zur Durchführung der Konformitätsbewertung qualifizierter Vertrauensdiensteanbieter und der von ihnen erbrachten qualifizierten Vertrauensdienste befähigte Stelle akkreditiert worden ist. Abfassung des CAR.
CAR – Conformity Assessment Report (Konformitätsbewertungsbericht)	Bericht, mit dem die Konformitätsbewertungsstelle bestätigt, dass der qualifizierte Vertrauensdiensteanbieter und die Vertrauensdienste den Anforderungen der Verordnung genügen (vgl. eIDAS [1]).
Card Management System (CMS)	Instrument zur Authentifizierung, Identitätsprüfung, Erhebung und Speicherung von Daten über die Zertifikatsinhaber oder die Antragsteller.

Vertragsende	Definition
Zertifikat für elektronische Signaturen	Eine elektronische Bescheinigung, die elektronische Signaturvalidierungsdaten mit einer natürlichen Person verknüpft und die mindestens den Namen oder das Pseudonym dieser Person bestätigt. (vgl. eIDAS [1]).
Zertifikat für elektronische Siegel	Eine elektronische Bescheinigung, die elektronische Siegelvalidierungsdaten mit einer juristischen Person verknüpft und die den Namen dieser Person bestätigt (vgl. eIDAS [1]).
Qualifiziertes Zertifikat für elektronische Signaturen	Ein von einem qualifizierten Vertrauensdiensteanbieter ausgestelltes Zertifikat für elektronische Signaturen, das die Anforderungen von Anhang I der eIDAS- Verordnung erfüllt (vgl. eIDAS [1]).
Qualifiziertes Zertifikat für elektronische Siegel (QSealC)	Ein von einem qualifizierten Vertrauensdiensteanbieter ausgestelltes Zertifikat für elektronische Siegel, das die Anforderungen von Anhang III der eIDAS-Verordnung erfüllt (vgl. eIDAS [1]).
Qualifiziertes Zertifikat für elektronische Siegel für PSD2 (QSealC PSD2)	QSealC lt. Art 34 der delegierten Verordnung (EU) 2018/389 [12] zur Umsetzung der Richtlinie (EU) 2015/2366 (PSD2) [11] entsprechend den durch den Standard ETSI TS 119 495 festgelegten Anforderungen (nachstehend "QSealC PSD2")
LongTerm-Zertifikat	Qualifiziertes Zertifikat für elektronische Signaturen für Fernverfahren. Die Verwendung dieses Zertifikats beschränkt sich ausschließlich auf eine Domain, für die das Zertifikat ausgestellt wurde.
One-Shot-Zertifikat	Dies ist ein qualifiziertes Zertifikat für qualifizierte elektronische Signaturen für Fernverfahren, das in dieser Beschreibung der Zertifizierungspraxis geregelt ist und dessen Schlüssel nach ihrer Generierung nur im Bereich einer Domain und ausschließlich für die Signaturtransaktionen verfügbar ist, für die das Zertifikat erstellt wurde. Der private Schlüssel wird sofort nach seiner Verwendung zerstört
Zertifizierungsschlüssel oder Root-Schlüssel	Ein kryptografisches Schlüsselpaar, das die CA zur Signatur der Zertifikate und der Listen der widerrufenen oder suspendierten Zertifikate verwendet.
Privater Schlüssel	Das vom Zertifikatsinhaber verwendete Element des asymmetrischen Schlüsselpaars, über das die qualifizierte elektronische Signatur auf das elektronische Dokument angebracht wird (vgl. CAD [2]).
Öffentlicher Schlüssel	Das Element des asymmetrischen Schlüsselpaars, das zu Veröffentlichung bestimmt ist und mit dem die qualifizierte elektronische Signatur geprüft wird, die der Zertifikatsinhaber auf das elektronische Dokument angebracht hat (vgl. CAD [2]).
Notfallcode (ERC)	Sicherheitscode, der dem Zertifikatsinhaber für die Übermittlung des Antrags auf Suspendierung eines Zertifikats auf den Portalen des Vertrauensdiensteanbieters übergeben wird.
Validierung	Der Prozess der Überprüfung und Bestätigung der Gültigkeit einer elektronischen Signatur (vgl. eIDAS [1]).
Signaturvalidierungsdaten	Daten, die zur Validierung einer elektronischen Signatur verwendet werden (vgl. eIDAS [1]).
Personenidentifizierungsdaten	Ein Datensatz, der es ermöglicht, die Identität einer natürlichen oder juristischen Person oder einer natürlichen Person, die eine juristische Person vertritt, festzustellen (vgl. eIDAS [1]).
Elektronische Signaturerstellungsdaten	Die eindeutigen Daten, die vom Unterzeichner zum Erstellen einer elektronischen Signatur verwendet werden (vgl. eIDAS [1]).

Vertragsende	Definition
Elektronische Signaturerstellungseinheit (SSCD Secure System Creation Device)	Eine konfigurierte Software oder Hardware, die zum Erstellen einer elektronischen Signatur verwendet wird. (vgl. eIDAS [1]).
Qualifizierte elektronische Signaturerstellungseinheit QSCD)	Eine elektronische Signaturerstellungseinheit, die die Anforderungen von Anhang II der eIDAS-Verordnung erfüllt (vgl. eIDAS [1]).
Elektronisches Dokument	Jeder in elektronischer Form, insbesondere als Text-, Ton-, Bild- oder audiovisuelle Aufzeichnung gespeicherte Inhalt (vgl. eIDAS [1]).
Domain	Sie identifiziert sich mit den Anwendungen, über die das qualifizierte Zertifikat an den Zertifikatsinhaber ausgestellt wird und in denen der Zertifikatsinhaber das Zertifikat zur Unterzeichnung elektronischer Dokumente verwenden kann. Die Anwendungen können direkt vom Zertifizierungsanbieter oder vom Antragsteller verwaltet werden und zudem, je nach dem für die Ausstellung des qualifizierten Zertifikats angewandten Identifizierungsverfahren besondere zusätzliche Bestimmungen enthalten.
Automatische Signatur	Ein besonderes rechnergestütztes Verfahren für elektronische Signaturen, das nach vorheriger Autorisierung des Unterzeichners durchgeführt wird, wobei Letzterer die alleinige Kontrolle über seine Signaturschlüssel behält, ohne dass diese regelmäßig und ständig kontrolliert werden müssen.
Digitale Signatur (digital signature)	Eine besondere Art fortgeschrittener elektronischer Signatur, die auf einem qualifizierten Zertifikat und auf einem System miteinander verknüpfter kryptografischer Schlüssel – einem öffentlichen und einem privaten – beruht, das dem Zertifikatsinhaber über den privaten Schlüssel und dem Empfänger über den öffentlichen Schlüssel ermöglicht, die Herkunft und die Integrität eines elektronischen Dokuments oder einer Gesamtheit von elektronischen Dokumenten zu bestätigen bzw. zu überprüfen (vgl. CAD [2]).
Elektronische Signatur	Daten in elektronischer Form, die anderen elektronischen Daten beigefügt oder logisch mit ihnen verbunden werden und die der Unterzeichner zum Unterzeichnen verwendet (vgl. eIDAS [1]).
Fortgeschrittene elektronische Signatur	Eine elektronische Signatur, die die Anforderungen von Artikel 26 der eIDAS-Verordnung erfüllt (vgl. eIDAS [1]).
Qualifizierte elektronische Signatur	Eine fortgeschrittene elektronische Signatur, die von einer qualifizierten elektronischen Signaturerstellungseinheit erstellt wurde und auf einem qualifizierten Zertifikat für elektronische Signaturen beruht (vgl. eIDAS [1]).
Fernsignatur	Besonderes Verfahren für qualifizierte elektronische bzw. digitale Signaturen, die mit einem HSM generiert werden, das die alleinige Kontrolle der privaten Schlüssel durch deren Inhaber sicherstellt
Unterzeichner	Eine natürliche Person, die eine elektronische Signatur erstellt (vgl. eIDAS [1]).
Überwachungsprotokoll	Das Überwachungsprotokoll besteht aus der Gesamtheit der automatisch oder manuell durchgeführten Einträge der von den Technischen Regeln genannten Ereignisse [9].
Elektronische Identifizierung	Der Prozess bei dem Personenidentifizierungsdaten in elektronischer Form verwendet werden, die eine natürliche oder juristische Person oder eine natürliche Person, die eine juristische Person vertritt, eindeutig repräsentieren. (vgl. eIDAS [1]).

Vertragsende	Definition
Sperrliste [Certificate Revocation List – CRL]	Es handelt sich um eine Liste der Zertifikate, die vor Ablauf ihrer Gültigkeitsdauer für „ungültig“ erklärt wurden. Der Vorgang nennt sich Widerruf, wenn die Ungültigkeit endgültig ist, und Suspendierung, wenn sie nur vorübergehend ist. Bei Widerruf oder Suspendierung eines Zertifikats wird seine Seriennummer in die CRL eingetragen, die dann im öffentlichen Register veröffentlicht wird.
Beschreibung der Zertifizierungspraxis [Certificate Practice Statement]	Die Beschreibung der Zertifizierungspraxis bestimmt die von der CA bei der Erbringung des Dienstes angewandten Verfahren. Bei der Abfassung der Beschreibung wurden die erteilten Hinweise der Aufsichtsbehörde und der internationalen Literatur befolgt.
Elektronische Identifizierungsmittel	Eine materielle und/oder immaterielle Einheit, die Personenidentifizierungsdaten enthält und zur Authentifizierung bei Online-Diensten verwendet wird (vgl. eIDAS [1]).
Online Certificate Status Protocol (OCSP)	Von der Internet Engineering Task Force (IETF) in dem RFC 6960 definiertes Protokoll, das es den Anwendungen ermöglicht, die Gültigkeit des Zertifikats schneller und gründlicher zu überprüfen als die CRL, auf deren Daten der Zugriff gewährleistet ist.
OTP - One-Time Password:	Ein One-Time Password (Einmalpasswort) ist ein Passwort, das nur für eine einzelne Transaktion gültig ist. Das OTP wird unmittelbar vor dem Anbringen der qualifizierten elektronischen Signatur generiert und dem Zertifikatsinhaber zur Verfügung gestellt. Es kann auf Hardwaregeräten oder auf Softwareprozessen beruhen.
Vertrauende Partei	Eine natürliche oder juristische Person, die auf eine elektronische Identifizierung oder einen Vertrauensdienst vertraut (vgl. eIDAS [1]).
Vertrauensdiensteanbieter	Eine natürliche oder juristische Person, die einen oder mehrere Vertrauensdienste als qualifizierter oder nichtqualifizierter Vertrauensdiensteanbieter erbringt (vgl. eIDAS [1]).
Qualifizierter Vertrauensdiensteanbieter	Ein Vertrauensdiensteanbieter, der einen oder mehrere qualifizierte Vertrauensdienste erbringt und dem von der Aufsichtsstelle der Status eines qualifizierten Anbieters verliehen wurde (vgl. eIDAS [1]).
Produkt	Eine Hardware, Software oder deren spezifische Komponenten, die zur Erbringung von Vertrauensdiensten bestimmt sind (vgl. eIDAS [1]).
Amtsperson	Person, die im Rahmen der ausgeübten Tätigkeiten auf Grundlage des einschlägigen Gesetzes zur Bescheinigung der Identität natürlicher Personen berechtigt ist.
Öffentliches Register [Directory]	Das öffentliche Register ist ein Archiv, das Folgendes enthält: ▪ alle von der CA ausgestellten Zertifikate, für die der Zertifikatsinhaber die Veröffentlichung verlangt hat ▪ die Sperrliste (CRL)
Widerruf oder Suspendierung eines Zertifikats	Es handelt sich um den Vorgang, mit dem die CA die Gültigkeit des Zertifikats vor dem Ablauf seiner Gültigkeitsdauer aufhebt.
Rolle	Der Begriff Rolle meint allgemein den Inhaber und/oder die Eignung zur Berufsausübung im Besitz des Zertifikatsinhabers beziehungsweise die eventuelle Vertretungsbefugnis natürlicher Personen oder privatrechtlicher oder öffentlich-rechtlichen Einrichtungen beziehungsweise die Zugehörigkeit zu diesen Einrichtungen sowie die Ausübung öffentlicher Funktionen.

Vertragsende	Definition
Vertrauensdienst	Ein elektronischer Dienst, der in der Regel gegen Entgelt erbracht wird und aus folgenden Elementen besteht: a) Erstellung, Überprüfung und Validierung von elektronischen Signaturen, elektronischen Siegeln oder elektronischen Zeitstempeln, Dienste für die Zustellung elektronischer Einschreiben und Zertifikate in Bezug auf solche Dienste; oder b) Erstellung, Überprüfung und Validierung von Zertifikaten für die Website-Authentifizierung; oder c) Bewahrung von diese Dienste betreffenden elektronischen Signaturen, Siegeln oder Zertifikaten (vgl. eIDAS [1]).
Qualifizierter Vertrauensdienst	Ein Vertrauensdienst, der die einschlägigen Anforderungen dieser Verordnung erfüllt (vgl. eIDAS [1]).
Elektronische Siegel	Daten in elektronischer Form, die anderen elektronischen Daten beigefügt oder mit diesen logisch verbunden werden und die die Herkunft und die Integrität dieser Daten garantieren (vgl. eIDAS [1]).
Fortgeschrittenes elektronisches Siegel	Ein elektronisches Siegel, das die Anforderungen von Artikel 36 der eIDAS-Verordnung erfüllt (vgl. eIDAS [1]).
Qualifiziertes elektronisches Siegel	Ein fortgeschrittenes elektronisches Siegel, das von einer qualifizierten elektronischen Siegelerstellungseinheit erstellt wird und auf einem qualifizierten Zertifikat für elektronische Siegel beruht (vgl. eIDAS [1]).
Mitgliedstaat	Mitgliedstaat der Europäischen Union
Koordinierte Weltzeit [Coordinated Universal Time]:	Zeitskala mit Sekundengenauigkeit gemäß Definition in der Empfehlung der internationalen Fernmeldeunion ITU-R TF.460-5.
Elektronischer Zeitstempel	Daten in elektronischer Form, die andere Daten in elektronischer Form mit einem bestimmten Zeitpunkt verknüpfen und dadurch Nachweis erbringen, dass diese anderen Daten zu diesem Zeitpunkt vorhanden waren (vgl. eIDAS [1]).
Qualifizierter elektronischer Zeitstempel	Ein elektronischer Zeitstempel, der die Anforderungen von Artikel 42 der eIDAS-Verordnung erfüllt (vgl. eIDAS [1]).
WebCam	Kleine Videokamera, die Bilder per Streaming mittels Internet überträgt und Fotos aufnimmt. Sie ist mit einem PC verbunden oder in einem Mobilgerät eingebaut und wird für Videochats oder Videokonferenzen verwendet.

1.6.2 Akronyme und Abkürzungen

Akronym	
AgID	Agenzia per l'Italia Digitale: Aufsichtsbehörde für Vertrauensdiensteanbieter
CA	Certification Authority
CAB	Conformity Assessment Body – Konformitätsbewertungsstelle
CAD	Codice dell'Amministrazione Digitale (Kodex der digitalen Verwaltung)
CAR	Conformity Assessment Report – Konformitätsbewertungsbericht
CC	Common Criteria
CIE	Elektronischer Personalausweis
CMS	Card Management System
CNS – TS-CNS	(ital.) Bürgerkarte

Akronym	
	Krankenversicherungskarte – Bürgerkarte
CRL	Certificate Revocation List
DMZ	Demilitarized Zone
DN	Distinguish Name
EAL	Evaluation Assurance Level
EBA	European Banking Authority
eID	Electronic Identity
eIDAS	Electronic Identification and Signature Regulation
ERC	Emergency Request Code
ETSI	European Telecommunications Standards Institute
FIPS	Federal Information Processing Standard
HSM	Hardware Secure Module: Es ist ein Sicherheitsmodul für die Signaturerstellung mit ähnlichen Funktionen wie die der Smartcard, jedoch mit besseren Speicher- und Leistungsmerkmalen;
HTTP	HyperText Transfer Protocol
IETF	Internet Engineering Task Force
RB	Registrierungsbeauftragter
ISO	Internationale Organisation für Normung: Die 1946 gegründete internationale Organisation ISO besteht aus nationalen Organen für die Normierung
ITU	Internationale Fernmeldeunion: Diese 1865 gegründete internationale Organisation definiert die Telekommunikationsstandards.
IUT	Individuelle Inhaberkennung: Es ist ein Code, der dem Zertifikatsinhaber zugeordnet ist und ihn bei der CA eindeutig identifiziert. Der Zertifikatsinhaber besitzt für jedes Zertifikat verschiedene Codes
LDAP	Lightweight Directory Access Protocol: Protokoll, das für den Zugriff auf das Zertifikatsregister verwendet wird
LoA	Level of Assurance
NCA	National Competent Authority
NTR Code	National Trade Register Code
OID	Object Identifier: Er setzt sich aus einer Nummernfolge zusammen, die gemäß dem Verfahren in der Norm ISO/IEC 6523 registriert wird und ein bestimmtes Objekt innerhalb einer Hierarchie identifiziert
OTP	One-Time Password
PEC	Zertifizierte E-Mail-Adresse
PIN	Personal Identification Number: Ein Code, der mit einer sicheren Signatureinheit verknüpft ist und mit dem der Zertifikatsinhaber Zugriff auf die Funktionen dieser Einheit hat
PKCS	Public-Key Cryptography Standards
PKI	Public Key Infrastructure (Infrastruktur mit öffentlichem Schlüssel): Die Gesamtheit der Quellen, Prozesse und technischen Mittel, die dritten

Akronym	
	vertrauenswürdigen Parteien ermöglichen, die Identität einer Person zu überprüfen und/oder für sie zu garantieren sowie einen öffentlichen Schlüssel mit einer Person zu verknüpfen
PSD2	Payment Services Directive 2
PSP	Service Payment Provider (Zahlungsdienstleister)
QSealC	Qualified electronic Seal Certificate
RA	Registration Authority – Registrierungsstelle
RFC	Request for Comment: Ein Dokument, das Informationen oder Spezifikationen über neue Forschungen, Innovationen und Methoden im IT-Bereich enthält, das von den Autoren der Gemeinschaft zur Beurteilung unterbreitet wird
RSA	Aus den Initialen der Erfinder des Algorithmus zusammengesetzter Name: River, Shamir, Adleman
ISMS	Managementsystem für die Informationssicherheit
SPID	Öffentliches System für digitale Identität
SSCD - QSSCD	Secure Signature Creation Device: Signaturerstellungseinheit Qualified Secure Signature Creation Device: Qualifizierte Signaturerstellungseinheit
TIN	Steuer-Identifikationsnummer
UUID	Universally unique identifier
URL	Uniform Resource Locator
VAT Code	Umsatzsteuernummer
X500	ITU-T-Standard für LDAP- und Verzeichnisdienste
X509	ITU-T-Standard für PKI

2 VERÖFFENTLICHUNG UND ARCHIVIERUNG

2.1 Archivierung

Die veröffentlichten Zertifikate, die CRLs und die Beschreibungen der Zertifizierungspraxis werden veröffentlicht und sind rund um die Uhr, 7 Tage die Woche verfügbar.

2.2 Veröffentlichung der Informationen über die Zertifizierung

2.2.1 Veröffentlichung der Beschreibung der Zertifizierungspraxis

Diese Beschreibung der Zertifizierungspraxis, das Zertifikatsverzeichnis der Zertifizierungsschlüssel und die anderen gesetzlich vorgeschriebenen Informationen über die CA sind in dem Verzeichnis der Zertifizierungsanbieter (unter dem Link https://eidas.agid.gov.it/TL/TSL-IT.xml) und auf veröffentlicht 1.5.1).

2.2.2 Veröffentlichung von Zertifikaten

Der Zertifikatsinhaber oder der Antragsteller, als gesetzlicher Vertreter der juristischen Person, der sein Zertifikat veröffentlichen lassen will, kann dies durch Zusendung an InfoCert des eigens dafür (auf der Website www.firma.infocert.it) vorgesehenen, ausgefüllten Formulars beantragen, das mit dem Schlüssel digital signiert ist, das dem zu veröffentlichenden Zertifikat zugrunde liegt. Der Antrag ist per E-Mail an richiesta.pubblicazione@cert.legalmail.itunter Befolgung des auf der Website erläuterten Verfahrens zuzusenden. Diese Möglichkeit ist für die LongTerm- und OneShot-Zertifikate nicht gegeben.

2.2.3 Veröffentlichung der Sperrlisten

Die Sperrlisten sind im öffentlichen Zertifikatsregister veröffentlicht, das mit LDAP-Protokoll oder mit dem HTTP-Protokoll auf der im Attribut „CRL Distribution Points“ des Zertifikats angegebenen Seite abgerufen werden kann. Der Zugriff kann über die von der CA bereitgestellten Softwares erfolgen und/oder über die Funktionen in marktgängigen Produkten, die das LDAP und/oder HTTP interpretieren.

Die CA kann neben der genannten Verfahrensweise auch andere zum Abrufen des Verzeichnisses der veröffentlichten Zertifikate und ihrer Gültigkeit bereitstellen.

2.3 Zeitraum oder Häufigkeit der Veröffentlichung

2.3.1 Häufigkeit der Veröffentlichung der Beschreibung der Zertifizierungspraxis

Die Beschreibung der Zertifizierungspraxis wird mit veränderlicher Häufigkeit bei Eintreten von Änderungen veröffentlicht. Bei wichtigen Änderungen muss sich die CA einer Prüfung durch eine akkreditierte CAB unterziehen, den Konformitätsbewertungsbericht (*CAR – Conformity Assessment Report*) und die Beschreibung der Zertifizierungspraxis der Aufsichtsbehörde (AgID) vorlegen und auf die Erlaubnis für die Veröffentlichung warten.

2.3.2 Häufigkeit der Veröffentlichung der Sperrlisten

Die CRL werden jede Stunde veröffentlicht.

2.4 Kontrolle des Zugriffs auf die öffentlichen Archive

Die Informationen über veröffentlichte Zertifikate, die CRL und die Beschreibungen der Zertifizierungspraxis sind öffentlich. Die CA hat den Zugriff im Lesemodus nicht beschränkt und hat sämtliche Gegenmaßnahmen ergriffen, um unzulässige Änderungen/Löschungen abzuwehren.

3 IDENTIFIZIERUNG UND AUTHENTIFIZIERUNG

3.1 Bezeichnung

3.1.1 Namensformen

Die Person im Zertifikat wird mit dem vergebenen Distinguished Name (DN) identifiziert, ein Attribut, das also einen Wert enthalten und dem Standard X500 entsprechen muss. Die Zertifikate werden gemäß den Bestimmungen der Spezifikation RFC-5280 und der Standards ETSI EN 319 412 von 1 bis 5 sowie gemäß den Angaben der Entscheidung AgID 121/2019 [13] ausgestellt

3.1.2 Notwendigkeit der Bedeutung des Namens

Die Vergabe des zertifizierten Distinguished Name (DN) identifiziert eindeutig die Person, für die das Zertifikat ausgestellt wurde.

3.1.3 Anonymität und Pseudonymität der Antragsteller

Der Zertifikatsinhaber kann nur bei einer Identitätsprüfung gemäß dem Verfahren 1_LiveID (siehe § 3.2.3.1) von der CA verlangen, dass das Zertifikat ein Pseudonym anstelle seiner realen Daten enthält. Diese Möglichkeit ist für die LongTerm- und OneShot-Zertifikate nicht gegeben.

Da es sich um ein qualifiziertes Zertifikat handelt, speichert die CA die Daten über die wirkliche Identität der Person für zwanzig (20) Jahre ab der Zertifikatsausstellung.

3.1.4 Auslegungsregeln der Namensformen

InfoCert hält sich an den Standard X500.

3.1.5 Eindeutigkeit der Namen

Zertifikatsinhaber natürliche Person:
Um die Eindeutigkeit des Zertifikatsinhabers zu garantieren, müssen im Zertifikat der Vor- und Nachname sowie eine eindeutige Identifikationsnummer angegeben werden
In der Regel wird die Tax Identification Number (TIN) verwendet. Die TIN wird von den Behörden des Landes zugeteilt, dessen Bürger der Zertifikatsinhaber ist, oder von dem Land, in dem die Organisation, bei der er arbeitet, ihren Sitz hat. Für italienische Bürger ist die eindeutige Identifikationsnummer die Steuernummer.
Bei fehlender TIN oder Steuernummer kann im Zertifikat Folgendes angegeben werden:

- eine Idenfikationsnummer eines gültigen Ausweisdokuments, das im Rahmen des Identitätsprüfverfahrens verwendet wird. Das Format ist im Standard ETSI 319 412-1 vorgesehen

- eine von der CA festgelegte Identifikationsnummer. In diesem Fall wird das in RFC4122 beschriebene UUID-Format (Universally Unique Identifier) Version 4 verwendet.
- eine eindeutige Identifikationsnummer lt. eiDAS eID Profile im Rahmen von eiDAS Cooperation Network. Das Bezugsdokument ist "eIDAS SAML AttributeProfileVersion" Ver 1.2. (https://ec.europa.eu/cefdigital/wiki/display/CEFDIGITAL/eIDAS+eID+Profile)

Da allerdings die Steuernummer von allen italienischen Behörden zur Identifikation der Bürger und Steuerpflichtigen verwendet wird, hat das Fehlen der Steuernummer im Signaturzertifikat dessen Unangemessenheit gegenüber den italienischen Behörden zur Folge.

Zertifikatsinhaber juristische Person:
Bei einer juristischen Person muss zur Sicherstellung der Eindeutigkeit der Person im Zertifikat der Name der Organisation sowie wahlweise eine der nachfolgenden eindeutigen Identifikationsnummern angegeben sein:

- VAT (Umsatzsteuernummer)
- NTR (Handelsregisternummer)

Bei einer italienischen juristischen Person die Umsatzsteuernummer oder die Handelsregisternummer verwenden. Sollte die Organisation weder über eine Umsatzsteuernummer noch eine Handelsregisternummer verfügen, sondern nur über eine Steuernummer, können die zwei Zeichen „CF" gefolgt von „:IT-" verwendet werden (zum Beispiel: CF:IT- 97735020584), wie in der Entscheidung AgID 121/2019 [13] vorgesehen.
.

3.1.6 Identitätsprüfung, Authentifizierung und Rolle von eingetragenen Marken

Der Zertifikatsinhaber und der Antragsteller garantieren bei der Beantragung eines CA-Zertifikats unter strikter Einhaltung der nationalen und internationalen Rechtsvorschriften über das geistige Eigentum zu handeln.

Die CA nimmt keine Überprüfungen über die Markennutzung vor und kann die Erstellung eines Zertifikats ablehnen oder den Widerruf eines Zertifikats beantragen, das Gegenstand einer Auseinandersetzung ist.

3.2 Erste Validierung der Identität

Dieses Kapitel beschreibt die Verfahren für die Identifizierung des Zertifikatsinhabers oder des Antragstellers bei der Beantragung der Ausstellung des qualifizierten Zertifikats.

Mit dem Identifizierungsverfahren wird der Zertifikatsinhaber von der CA, auch über die RA oder einen ihrer Beauftragten, anerkannt. Dabei wird die Identität über eine der in der Beschreibung der Zertifizierungspraxis festgelegten Verfahrensweisen überprüft.

3.2.1 Verfahren für den Besitznachweis des privaten Schlüssels

InfoCert legt fest, dass der Antragsteller über den privaten Schlüssel, der dem zu zertifizierenden öffentlichen Schlüssel entspricht, den Besitz oder die Kontrolle hat und überprüft dabei die Signatur

des Zertifikatsantrags über den privaten Schlüssel, der dem zu zertifizierenden öffentlich Schlüssel entspricht.

3.2.2 Authentifizierung der Identität von Organisationen

s. § 3.2.4

3.2.3 Identifizierung einer natürlichen Person

Unbeschadet der Haftung der CA kann die Identität des Zertifikatsinhabers von Personen, die zur Durchführung der Identifizierung berechtigt sind, mit den folgenden Verfahrensweisen entsprechend Art. 24 der eiDAS-Verordnung festgestellt werden:

Verfahrensweisen	Zur Identifizierung berechtigte Personen	Authentifizierungsmittel für die Identifizierungsphase
1 LiveID	• Certification Authority (CA) • Registration Authority (RA) • Registrierungsbeauftragter • Amtsperson • Arbeitgeber für die Identifizierung seiner Arbeitnehmer, Mitarbeiter, Handelsvertreter	o. A.
2 AMLID	• Personen, denen die Verpflichtungen zur Bekämpfung der Geldwäsche gemäß der Umsetzungsvorschriften der Richtlinie 2005/60/EG des Europäischen Parlaments und des Rates zur Verhinderung der Nutzung des Finanzsystems zum Zwecke der Geldwäsche und der Terrorismusfinanzierung und der späteren gemeinschaftsrechtlichen Durchführungsbestimmungen obliegen.	o. A.
3 SignID	• Certification Authority (CA) • Registration Authority (RA) • Registrierungsbeauftragter	Verwendung einer qualifizierten elektronischen Signatur, die von einem qualifizierten Vertrauensdiensteanbieter ausgestellt wurde.
4 AutID	• Certification Authority (CA) • Registration Authority (RA) • Registrierungsbeauftragter	Verwendung eines bereits vorhandenen elektronischen Identifizierungsmittels

Verfahrensweisen	Zur Identifizierung berechtigte Personen	Authentifizierungsmittel für die Identifizierungsphase
5.1 VideoID mit Assistenz (attended)	• Certification Authority (CA) • Registration Authority (RA) • Registrierungsbeauftragter	o. A.
5.2 VideoID ohne Assistenz (unattended)	• Certification Authority (CA) • Registration Authority (RA) • Registrierungsbeauftragter	o. A.
6 eDocId	• Certification Authority (CA) • Registration Authority (RA) • Registrierungsbeauftragter	Verwendung eines bereits vorhandenen elektronischen Identifizierungsmittels

3.2.3.1 Identitätsprüfung nach dem Verfahren 1 - LiveID

Das Identifizierungsverfahren **LiveID** sieht ein persönliches Treffen des Zertifikatsinhabers und einer zur Durchführung der Identitätsprüfung berechtigten Personen vor.
Der Zertifikatsinhaber legt dem eigens geschulten CA-Beauftragten ein oder mehrere gültige Ausweise im Original vor, die in der Liste der anerkannten Dokumente enthalten sind, die auf der Website der CA veröffentlicht ist[2].
Um die Eindeutigkeit des Zertifikatsinhabers und seines Namens zu garantieren, muss dieser auch die eindeutige Identifikationsnummer nach § 3.1.5besitzen. Die zur Durchführung der Identitätsprüfung berechtigte Person kann die Vorlage einer Dokumentation verlangen, die den Besitz der eindeutigen Identifikationsnummer nachweist.
InfoCert kann die RAs, die im Ausland tätig sind oder jedenfalls Personen mit Wohnsitz im Ausland identifizieren, dazu autorisieren, Ausweise zu akzeptieren, die von Behörden von Ländern ausgestellt wurden, die zur Europäischen Union gehören, und die in der auf der Website der CA veröffentlichten Liste der anerkannten Dokumente.
Die Identifizierung kann auch durch eine Amtsperson auf Grundlage der einschlägigen Rechtsbestimmungen über deren Tätigkeiten erfolgen. Der Zertifikatsinhaber füllt den Zertifikatsantrag aus, unterzeichnet ihn vor einer Amtsperson und lässt seine Unterschrift gemäß den geltenden Rechtsvorschriften beglaubigen. Der Antrag wird dann bei der CA bei einer der vertragsgebundenen Registrierungsstellen eingereicht.
Die bereits vom Arbeitgeber für den Abschluss des Arbeitsvertrages erfolgte Identifizierung wird von der CA gemäß dem folgenden Identitätsprüfungsverfahren (Employee_ ID) nach einer vorherigen Überprüfung der operativen Identifizierungs- und Authentifizierungsverfahren als gültig erachtet. Als ebenso gültig gilt gemäß dem folgenden Identitätsprüfungsverfahren und nach vorheriger Überprüfung der operativen Identifizierungs- und Authentifizierungsverfahren die Identifizierung, die der Arbeitgeber im Rahmen der Aufnahme von Handelsvertreterbeziehungen durchführt.

[2] Die Liste der anerkannten Ausweisdokumente wird von der CA nach vorheriger Prüfung der Dokumente und ihrer objektiven Eigenschaften im Hinblick auf die Gewissheit der Identität und die Sicherheit in dem Ausstellungsverfahren der ausstellenden Behörde erstellt. Die Liste wird der AgID gemeldet und bei jeder Änderung aktualisiert.

Dieses Identifizierungsverfahren sieht vor, dass die CA dem Arbeitgeber einen Auftrag mit Vertretungsmacht erteilt, der somit als RA handelt[3]. Die mit diesem Identifizierungsverfahren ausgestellten Zertifikate können nur für die Arbeitszwecke benutzt werden, für die sie erteilt wurden, und enthalten eine spezifische Nutzungsbeschränkung.
Die CA bewahrt die Registrierungsdaten für das LiveID-Identifizierungsverfahren in analoger oder elektronsicher Form auf.

3.2.3.2 Identitätsprüfung nach dem Verfahren 2 – AMLID

Bei der **Verfahrensweise 2 - AMLID** bedient sich die CA der Identifizierung, die von einer der Personen durchgeführt wurde, denen die Identifizierungs- und Sorgfaltspflichten im Sinne der jeweils geltenden Rechtsvorschriften, der Umsetzungsvorschriften der Richtlinie 2005/60/EG des Europäischen Parlaments und des Rates zur Verhinderung der Nutzung des Finanzsystems zum Zwecke der Geldwäsche und der Terrorismusfinanzierung und der späteren weiteren gemeinschaftsrechtlichen Aktualisierungs- und Durchführungsbestimmungen obliegen.
Mit besonderem Bezug auf Italien werden die für die Identitätsprüfung verwendeten Daten von dem Zertifikatsinhaber gemäß GvD 231/2007 i. d. g. F. übermittelt, wonach die Kunden in eigener Verantwortung verpflichtet sind, alle notwendigen und aktualisierten Informationen bereitzustellen, um den Personen, denen die Verpflichtungen obliegen, die Erfüllung ihrer Pflichten der Identifizierung der Kunden zu ermöglichen.
Dieses Identifizierungsverfahren sieht vor, dass die CA der Person, der die Pflichten obliegen, einen Auftrag mit Vertretungsmacht erteilt, sodass diese als RA handelt. Die CA speichert die bei der Identitätsprüfung erhobenen Identifizierungsdaten des Zertifikatsinhabers üblicherweise in elektronischer Form. Es ist jedoch auch eine analoge Aufbewahrung möglich.

3.2.3.3 Identitätsprüfung nach dem Verfahren 3 – SignID

Bei der **Verfahrensweise 3 SignID** stützt sich die CA InfoCert auf die bereits erfolgte Identitätsprüfung durch eine CA, die qualifizierte Zertifikate ausstellt (QTSP)**.** Der Zertifikatsinhaber besitzt bereits ein qualifiziertes und noch gültiges Zertifikat, das er gegenüber InfoCert verwendet. Die Registrierungsdaten werden in diesem Fall ausschließlich elektronisch gespeichert.

3.2.3.4 Identitätsprüfung nach dem Verfahren 4 – AUTID

Bei der **Verfahrensweise 4 AutID** stützt sich die CA auf ein bereits vorhandenes elektronischen Identifizierungsmittel:

- das vom Mitgliedstaat gemäß Artikel 9 der eIDAS-Verordnung notifiziert wurde und ein *hohes* Niveau besitzt;
- das vom Mitgliedstaat gemäß Artikel 9 der eIDAS-Verordnung notifiziert wurde und ein *substanzielles* Niveau besitzt, unter der Voraussetzung, dass es unter dem Gesichtspunkt der Zuverlässigkeit eine mit der körperlichen Anwesenheit gleichwertige Sicherheit gewährleistet;
- das nicht notifiziert und von einer öffentlichen Verwaltung oder einer Privatperson ausgestellt wurde, unter der Voraussetzung, dass es unter dem Gesichtspunkt der

[3] Die CA führt vor der Erteilung des Auftrags eine gründliche Beurteilung der Sicherheit der Verfahren zur Identifizierung des Arbeitnehmers sowie der Bedingungen der Zuteilung und Verwaltung der Mittel zur persönlichen Identifizierung bei den IT-Systemen durch, auf die der Arbeitnehmer (oder der Handelsvertreter oder der Arbeitnehmer in Rente) zur Beantragung des CA-Zertifikats für digitale Signaturen zugreift. Diese Fälle werden der Aufsichtsbehörde mitgeteilt.

Zuverlässigkeit eine Sicherheit liefert, die mit der körperlichen Anwesenheit gleichwertig ist, und diese von einer Konformitätsbewertungsstelle bestätigt wurde.

Unter ausdrücklichem Hinweis auf den Interoperabilitätsrahmen gemäß Artikel 12 der eIDAS-Verordnung gilt die vom EIDAS-Knoten angesichts der Nutzung eines notifizierten nationalen Identifizierungssystems, das mindestens ein bedeutendes Niveau aufweist, übermittelte Nachricht als ausreichend, um ein qualifiziertes Zertifikat auszustellen. Wie von CEF-Spezifikation (Connecting Europe Facility) im Rahmen des Programms CEF eID[4] vorgesehen, wird die SAML-Nachricht vom Betreiber des nationalen Knotens bzw. von einer der zur Nutzung des Knotens berechtigten Person an die CA gesendet. Die CA überprüft die Integrität der empfangenen SAML-Nachricht und sieht die Person aufgrund der in der Nachricht enthaltenen Daten als identifiziert an.

Mit besonderem Bezug auf Italien gelten als elektronische Identifizierungsmittel die CNS-Karte (Bürgerkarte) oder TS-CNS (Krankenversicherungskarte – Bürgerkarte), die CIE (elektronischer Personalausweis), der elektronische Aufenthaltstitel und die im Zusammenhang mit dem SPID-System ausgestellten Identitäten.

Die von der CA und den RA verwendeten elektronischen Identifizierungsmittel sind in der auf der Website der CA veröffentlichten und der AgID gemeldeten Liste aufgeführt.
InfoCert erwägt die Möglichkeit, Identifizierungen von Anbietern einzusetzen, die über eine durch eine die Konformität des verwendeten Identifizierungsverfahrens mit Art. 24 Buchstabe d) der eIDAS-Verordnung bescheinigende CAB ausgestellte Zertifizierung verfügen.

3.2.3.5 Identitätsprüfung nach dem Verfahren 5 – VideoID

Bei der **Verfahrensweise 5 VideoID** muss der Zertifikatsinhaber ein internetfähiges Gerät (PC, Smartphone, Tablet usw.), eine Webcam und ein funktionierendes Audiosystem besitzen.
Der entsprechend geschulte Registrierungsbeauftragte überprüft die Identität des Zertifikatsinhabers oder des Antragstellers anhand von einem oder mehreren gültigen Ausweisdokumenten, die ein aktuelles und erkennbares Foto aufweisen und die in der Liste der anerkannten Dokumente enthalten sind, die auf der Website der CA veröffentlicht ist[5].

Das Identifizierungsverfahren 5 - VideoID kann alternativ erfolgen:

5.1. bei gleichzeitiger Teilnahme des Registrierungsbeauftragten und des Zertifikatsinhabers oder des Antragstellers an derselben Audio-/Videositzung (VideoID mit Assistenz);

5.2. ohne gleichzeitige Teilnahme des Registrierungsbeauftragten und des Zertifikatsinhabers oder des Antragstellers an der Audio-/Videositzung. Bei diesem Verfahren führt der Zertifikatsinhaber die Audio-/Videositzung eigenständig aus und sendet darüber hinaus als Bestätigung seiner Identität eine Banktransaktion von einem auf seinen Namen lautenden oder gemeinschaftlich geführten Girokonto, wobei er als Grund der Transaktion die von der

[4] Diese Spezifikationen finden sich unter folgendem Link https://ec.europa.eu/cefdigital/wiki/display/CEFDIGITAL/eIDAS+eID+Profile

[5] Die Liste der anerkannten Ausweisdokumente wird von der CA nach vorheriger Prüfung der Dokumente und ihrer objektiven Eigenschaften im Hinblick auf die Gewissheit der Identität und die Sicherheit in dem Ausstellungsverfahren der ausstellenden Behörde erstellt. Die Liste wird der AgID gemeldet und bei jeder Änderung aktualisiert. Aus Sicherheitsgründen und zur Betrugsbekämpfung ist die Art der von dieser Verfahrensweise anerkannten Dokumente auf die am weitesten verbreiteten Ausweise beschränkt.

CA oder RA bereitgestellte Korrelationskennung angibt. In einer anschließenden Backoffice-Phase prüft der Registrierungsbeauftragte die Audio-/Videositzung, die Entsprechung zwischen dem Aussteller des Überweisungsauftrags und den Daten des Zertifikatsinhabers sowie die Richtigkeit der Korrelationskennung. Bei erfolgreicher Prüfung validiert der Beauftragte dann die Identität (VideoID ohne Assistenz).

InfoCert kann die RA, die im Ausland tätig sind oder die Zertifikatsinhaber mit Wohnsitz im Ausland identifizieren, nach vorheriger Prüfung der Dokumente und ihrer objektiven Eigenschaften im Hinblick auf die Gewissheit der Identität und die Sicherheit in dem Ausstellungsverfahren der ausstellenden Behörde sowie einer spezifischen Schulung dazu autorisieren, Ausweise, die von Behörden von Ländern ausgestellt wurden, die zur Europäischen Union gehören, zu akzeptieren[6].
Der Registrierungsbeauftragte kann die Zulässigkeit des vom Zertifikatsinhaber oder vom Antragsteller verwendeten Dokuments ausschließen, wenn es seiner Meinung nach die aufgeführten Eigenschaften nicht besitzt. Die aus elektronischen Audio-Videodateien und Metadaten bestehenden Registrierungsdaten werden in geschützter Form gespeichert.

3.2.3.6 Identitätsprüfung nach dem Verfahren 6 - eDocID

Bei der Verfahrensweise 6 eDocID besitzt der Zertifikatsinhaber ein mit Internet verbundenes Gerät mit Webcam und berührungslosem Leser und legt zwecks Identifizierung ein maschinenlesbares Ausweisdokument für die biometrische Identifizierung vor[7].
Indem der Zertifikatsinhaber das Dokument mit der Kamera scannt oder an den berührungslosen Leser heranführt, erlaubt er den Zugriff auf den elektronischen Chip-Speicher, aus dem die Identifizierungsdaten und das Foto gewonnen werden. Der Zertifikatsinhaber wird darüber hinaus in einem automatischen Verfahren zur Gesichtsaufnahme (das sogenannte „Selfie-Video“) geführt, während der er zufällige verstärkende Aktionen nach den von der CA bereitgestellten Verfahrensanleitungen ausführt.
Die CA überprüft die Authentizität der digitalen Signatur auf den aus dem Ausweisdokument gewonnenen Daten und Foto und stellt die effektive Zugehörigkeit zur Person mithilfe einer oder mehrerer biometrischer Vergleichstechnologien zwischen dem gewonnenen Foto und dem aufgenommenen Selfie-Video fest. Falls der Kompatibilitätsindex (das sogenannte „Scoring“) keine zufriedenstellenden Werte erreicht, nimmt ein Registrierungsbeauftragter im Backoffice eine nachträgliche Identitätsprüfung vor.
Die aus elektronischen Audio-Videodateien und Metadaten bestehenden Registrierungsdaten werden in geschützter Form gespeichert.

3.2.4 Identifizierung einer juristischen Person

Der Zertifikatsantrag für eine juristische Person muss von einer natürlichen Person gestellt werden, die gemäß einer der oben beschriebenen Verfahren identifiziert wurde (vgl. § 3.2.3).
Es ist zudem die Dokumentation über die juristische Person sowie die Dokumentation vorzulegen, die die Befugnis bescheinigt, den Antrag für die juristische Person stellen zu können.

[6] Diese Fälle werden der Aufsichtsbehörde mitgeteilt.

[7] Es handelt sich Dokumente nach ICAO-Anforderungen mit MRZ oder mit damit vergleichbaren Sicherheitseigenschaften

Die juristische Person kann ein Zahlungsdienstleister (PSP) sein, der der PSD2-Richtlinie unterliegt.

3.2.5 Nicht überprüfte Informationen des Zertifikatsinhabers oder des Antragstellers

Der Zertifikatsinhaber kann direkt oder mit der Zustimmung des eventuell betroffenen Dritten folgende Daten ins Zertifikat aufnehmen lassen:

- Titel und/oder Berufsbefähigungen;
- Vertretungsbefugnis natürlicher Personen;
- Vertretungsbefugnis juristischer Personen oder Zugehörigkeit zu diesen;
- Ausübung öffentlicher Funktionen, Vertretungsbefugnis von Organisationen und öffentlich-rechtlichen Einrichtungen oder Zugehörigkeit zu diesen.

Das Zertifikat mit der **Rolle** entspricht den Angaben in der Entscheidung AgID 121/2019 [13].

Der Zertifikatsinhaber muss eine Erklärung vorlegen, die das tatsächliche Bestehen der spezifischen Rolle nachweist. Dies kann auch über eine Selbstzertifizierung erfolgen[8]. Die CA übernimmt mit Ausnahme von Fällen schuldhaften Handelns keine Haftung in Bezug auf die Aufnahme der vom Zertifikatsinhaber selbst zertifizierten Daten ins Zertifikat.

Im Zertifikat werden dagegen die Bezeichnung oder der Name und die Identifikationsnummer der **Organisation** genannt, wenn diese die Ausstellung des Zertifikats an den Zertifikatsinhaber genehmigt hat, auch ohne ausdrückliche Angabe einer Rolle. In diesem Fall führt die CA eine Prüfung der formalen Ordnungsmäßigkeit der vom Zertifikatsinhaber eingereichten Dokumentation durch. Die Beantragung von Zertifikaten mit Angabe der Rolle und/oder der Organisation ist nur für Organisationen möglich, die eine definierte Rechtsform besitzen.

3.2.6 Validierung der Behörde

Die CA bzw. die RA überprüft die für die Identifizierung erforderlichen, in § 3.2.3, 3.2.4 und 325 definierten Informationen und validiert den Antrag.
Soweit vorgesehen und erforderlich, kann die CA oder die RA zur Validierung der vom Antragsteller bereitgestellten Informationen auf öffentliche Datenbanken zurückgreifen.

Im Fall eines QSealC-PSD2-Antrags überprüft die CA oder die RA die vom Antragsteller bereitgestellten Attribute (Autorisierungsnummer, Name und Staat der NCA, Rolle des PSP), indem sie die von der EBA in ihrem zentralen Register oder gegebenenfalls in den von den NCA jedes Mitgliedstaates verfügbar gemachten Registern bereitgestellten authentischen Informationen verwendet.

Hat die nationale NCA Regeln zur Validierung besagter Attribute vorgegeben, so wendet der Vertrauensdiensteanbieter diese Regeln an.

3.3 Identifizierung und Authentifizierung für die Erneuerung der Schlüssel und der

[8] Erfolgt der Antrag auf Aufnahme der Rolle ins Zertifikat nur über die Selbstzertifizierung des Zertifikatsinhabers, enthält das Zertifikat keine Angaben im Zusammenhang mit der Organisation, mit der diese Rolle eventuell verbunden sein könnte.

Zertifikate

3.3.1 Identifizierung und Authentifizierung für die Erneuerung der Schlüssel und der Zertifikate

Dieser Abschnitt beschreibt die Verfahren für die Authentifizierung und Identifizierung des Zertifikatsinhabers bei einer Erneuerung des qualifizierten Zertifikats für elektronische Signaturen.

Das Zertifikat enthält die Angabe des Gültigkeitszeitraums in dem Feld „Gültigkeit“ (validity) mit dem Attribut „gültig ab“ (*not before*) und „gültig bis“ (*not after*). Das Zertifikat ist außerhalb dieses Datumintervalls, einschließlich der Stunden, Minuten und Sekunden, nicht gültig.

Der Zertifikatsinhaber kann es jedoch vor seinem Ablauf über die von der CA bereitgestellten Mittel erneuern. Diese bestehen aus einem Erneuerungsantrag, der mit dem privaten Schlüssel signiert wird, der dem öffentlichen Schlüssel in dem zu erneuernden Zertifikat entspricht. Nach dem Widerruf oder dem Ablauf des Zertifikats ist die Erneuerung des Zertifikats ist nicht möglich, weshalb eine neue Ausstellung notwendig wird.

3.4 Identifizierung und Authentifizierung für Anträge auf Widerruf oder Suspendierung

Der Widerruf oder die Suspendierung des Zertifikats kann auf authentifiziertes Verlangen des Zertifikatsinhabers oder des Antragstellers (betroffener Dritter in dem Fall, dass der Letztgenannte seine Zustimmung zur Aufnahme der Rolle erteilt hat) bzw. auf Initiative der CA erfolgen.

3.4.1 Beantragung durch den Zertifikatsinhaber

Der Zertifikatsinhaber kann den Widerruf oder die Suspendierung durch Ausfüllen und Unterzeichnung, auch digital, des auf der Website der CA zur Verfügung bereitstehenden Formulars beantragen (s. § 4.9).

Der Antrag auf Suspendierung kann über ein Internet-Formular erfolgen. Der Zertifikatsinhaber authentifiziert sich in einem solchen Fall durch Mitteilung des bei Ausstellung des Zertifikats erhaltenen Notfallcodes oder mit einem anderen Authentifizierungssystem, das in der bei der Registrierung übergebenen Vertragsdokumentation erläutert ist.

Der Zertifikatsinhaber im Besitz einer Fernsignatur kann den Widerruf auch über seinen privaten Bereich beantragen, auf den er durch ein Zwei-Faktor-Authentifizierungssystem zugreift (§ 4.2.2)

Bei Beantragung über die Registration Authority erfolgt die Authentifizierung mit den für die Identifizierung vorgesehenen Verfahren.

Handelt es sich bei dem Zertifikatsinhaber um eine juristische Person, muss der Suspendierungs- oder Widerrufsantrag durch einen gesetzlichen Vertreter oder eine Person gestellt werden, die mit einer dazu bestimmten Vollmacht ausgestattet ist.

3.4.2 Beantragung durch den Antragsteller

Der Antragsteller oder ein betroffener Dritter, der den Widerruf oder die Suspendierung des Zertifikats des Zertifikatsinhabers verlangt, authentifiziert sich durch Unterzeichnung des dafür

vorgesehenen und von der CA zur Verfügung gestellten Formulars für die Beantragung eines Widerrufs oder einer Suspendierung. Der Antrag ist mit den in dem § 4.9.3 oder 4.9.15.2 genannten Verfahren zu übermitteln. Die CA behält sich vor, weitere Verfahrensweisen für die Übermittlung des Widerrufs- oder Suspendierungsantrags des Antragstellers in eigens hierfür abzuschließenden Vereinbarungen mit Letzterem zu bestimmen.

4 FUNKTIONSWEISE

4.1 Beantragung des Zertifikats

4.1.1 Wer kann ein Zertifikat beantragen?

Das qualifizierte Zertifikat für eine natürliche Person kann von folgenden Personen beantragt werden:

- dem Zertifikatsinhaber,
  - der sich hierfür über die Website www.firma.infocert.itdirekt an die CA wendet oder
  - der sich hierfür an eine Registration Authority wendet
- dem Antragsteller für den Zertifikatsinhaber,
  - der sich hierfür über die Website www.firma.infocert.it direkt an die CA wendet oder mit der CA eine Geschäftsvereinbarung abschließt
  - der sich hierfür an eine Registration Authority wendet
  - der hierfür einen Auftrag mit Vertretungsmacht mit der CA unterzeichnet und somit eine Registration Authority innerhalb einer Domain wird.

Das qualifizierte Zertifikat für eine juristische Person kann von folgenden Personen beantragt werden:

- dem Antragsteller, der die juristische Person vertritt,
  - der sich hierfür über die Website www.firma.infocert.it direkt an die CA wendet oder mit der CA eine Geschäftsvereinbarung abschließt
  - der sich hierfür an spezifische Registration Authorities wendet, die eigens für die Ausstellung von Zertifikaten dieser Art ausgebildet sind.

4.1.2 Registrierungsverfahren und Haftung

Das Registrierungsverfahren umfasst: den Antrag des Zertifikatsinhabers, die Generierung des Schlüsselpaars, den Antrag der Zertifizierung des öffentlichen Schlüssels und die Unterzeichnung der Verträge, jedoch nicht unbedingt in dieser Reihenfolge.

In dem Verfahren haben die verschiedenen Akteure unterschiedliche Verantwortungen und tragen zusammen zu der erfolgreichen Ausstellung bei:

- Der Zertifikatsinhaber ist dafür verantwortlich, richtige und wahrheitsgemäße Angaben über seine Identität zu machen, das von der CA auch über die RA zur Verfügung gestellte Material aufmerksam zu lesen, die Anweisungen der CA und/oder der RA während der Bearbeitung des Antrags für das qualifizierte Zertifikat zu befolgen; Handelt es sich bei dem Zertifikatsinhaber um eine juristische Person, obliegt diese Verantwortung dem gesetzlichen Vertreter oder der mit einer dazu bestimmten Vollmacht ausgestatteten Person, die das qualifizierte Zertifikat beantragt.
- Der eventuelle Antragsteller ist dafür verantwortlich, den Zertifikatsinhaber, für den er das Zertifikat beantragt, über die sich im Zusammenhang mit dem Zertifikat ergebenden Pflichten zu informieren, richtige und wahrheitsgemäße Angaben über die Identität des

Zertifikatsinhabers zu machen, die Verfahren und die Anweisungen der CA und/oder der RA zu befolgen;

- Die eventuelle Registration Authority ist, auch über den Registrierungsbeauftragten, dafür verantwortlich, den Zertifikatsinhaber und den Antragsteller eindeutig zu identifizieren, die verschiedenen Personen über die sich im Zusammenhang mit dem Zertifikat ergebenden Pflichten zu informieren und die von der CA definierten Verfahren genau zu befolgen;
- Die Certification Authority ist der letztendliche Verantwortliche für die Identifizierung des Zertifikatsinhabers und für den erfolgreichen Abschluss des Verfahrens für die Eintragung des qualifizierten Zertifikats.

Handelt es sich bei dem Zertifikatsinhaber um eine juristische Person, muss der Antragsteller, wenn die Schlüssel in einer Einheit des Zertifikatsinhabers generiert werden, auch den von ihm selbst unterzeichneten Antrag im Format PKCS#10 zusenden.

4.2 Bearbeitung des Antrags

Für den Erhalt eines Signaturzertifikats hat der Zertifikatsinhaber und/oder der Antragsteller:

- die Vertragsdokumentation und die eventuell weiteren Informationsunterlagen durchzusehen;
- die von der Certification Authority angewandten und in § 3.2.3 erläuterten Identifizierungsverfahren zu befolgen;
- alle für die Identifizierung notwendigen Angaben bereitstellen, die auf Verlangen mit der geeigneten Dokumentation ausgestattet sein müssen;
- den Registrierungs- und Zertifizierungsantrag unter Annahme der Vertragsbedingungen, die die Bereitstellung des Dienstes regeln, auf den von der CA erstellten analogen oder elektronischen Formularen zu unterzeichnen.

4.2.1 Vom Zertifikatsinhaber zu liefernde Angaben

4.2.1.1 Natürliche Person

Für die Beantragung eines qualifizierten Signaturzertifikats hat der Zertifikatsinhaber oder der Antragsteller, der das Zertifikat der natürlichen Person beantragt, zwingend die folgenden Informationen anzugeben:

- Nachname und Vorname;
- Geburtsdatum und Geburtsort;
- TIN-Code (in Italien die Steuernummer) oder falls dieser nicht vorhanden sein sollte eine entsprechenden Identifikationsnummer, wie z. B. die Personalausweisnummer; sollte die Richtlinie des jeweiligen Landes die öffentliche Verwendung dieser Informationen nicht gestatten, nimmt sie InfoCert nicht im Zertifikat auf.
- Daten des Personalausweises, der für die Identitätsprüfung vorgelegt wird, wie Art, Nummer, Ausstellungsbehörde und -datum;
- Mindestens eine der folgenden Kontaktdaten für die Zusendung der Mitteilungen von der CA an den Zertifikatsinhaber
  - Wohnsitzanschrift
  - E-Mail-Adresse;
- Mobiltelefonnummer für Kontaktnahme bei Notfällen und die Übertragung des OTP, sofern

dies die angewandte OTP-Technologie ist.

Die der RA mitgeteilte E-Mail-Adresse und Mobiltelefonnummer müssen gültig sein und den Zertifikatsinhaber eindeutig identifizieren. Die E-Mail-Adresse wird für etwaige Kommunikationen der CA sowie zum Senden der Notfallcodes (ERC) und der Fälligkeitsanzeigen verwendet. Dieser Sachverhalt trifft nicht auf die LongTerm- und OneShot-Zertifikate zu.

Der Zertifikatsinhaber (oder der Antragsteller) kann wahlweise einen anderen Namen liefern, unter dem er allgemein bekannt ist. Dieser Name wird in ein eigenes Feld mit dem Namen commonName (allgemeiner Name) des SubjectDN des Zertifikats aufgenommen. Liefert der Zertifikatsinhaber oder der Antragsteller keinen weiteren Namen, wird im Feld commonName der Vor- und Nachname des Zertifikatsinhabers valorisiert.

4.2.1.2 Juristische Person

Für die Beantragung eines qualifizierten Zertifikats für eine juristische Person ist der Antragsteller, in Person des gesetzlichen Vertreters oder einer bevollmächtigten natürlichen Person, zur Bereitstellung folgender Angaben verpflichtet:

- Nachname und Vorname des Antragstellers;
- TIN-Code oder eine entsprechende Identifikationsnummer des Antragstellers (in Italien die Steuernummer);
- Daten des Ausweisdokuments, das für die Identitätsprüfung des Antragstellers vorgelegt wird, wie Art, Nummer, Ausstellungsbehörde und -datum;
- E-Mail Adresse für die Zusendung der Mitteilungen von der CA an den Antragsteller;
- Name des Zertifikatsinhabers juristische Person;
- VAT Code oder NTR (Umsatzsteuernummer oder Handelsregisternummer für italienische Zertifikatsinhaber).

Möchte die juristische Person ihre eigenen Schlüsselpaare zertifizieren, hat der Antragsteller auch die Datei im Format PKCS#10 des von ihm selbst unterzeichneten Antrags zu liefern.
Die mitgeteilten Informationen sind in den Archiven der CA gespeichert (Registrierungsphase) und bilden die Grundlage für die Erzeugung des qualifizierten Zertifikats.

Bei Beantragung eines QSealC PSD2 Zertifikats ist der Zahlungsdienstleister (PSP), in Person des gesetzlichen Vertreters oder einer bevollmächtigten natürlichen Person, **zur Bereitstellung folgender weiterer Angaben verpflichtet:**

- Autorisierungsnummer, die den Zahlungsdienstleister (PSP) eindeutig identifiziert;
- Rolle der/des Zahlungsdienstleister/s (PSP);
- Name und Staat der zuständigen nationalen Behörde (NCA), die den Zahlungsdienstleister (PSP) autorisiert und die die Autorisierungsnummer ausgestellt hat.

4.2.2 Durchführung der Identifizierungs- und Authentifizierungsfunktionen

Während der ersten Registrierung und des Einholens des Registrierungs- und Zertifizierungsantrags werden dem Zertifikatsinhaber oder dem Antragsteller, gesetzlicher Vertreter der juristischen

Person, die Sicherheitscodes übergeben, mit denen er die Signatureinheit aktivieren oder das eventuelle Fernsignaturverfahren bzw. den eventuellen Antrag auf Suspendierung des Zertifikats beantragen kann (ERC-Code oder entsprechender Code, sofern vom Vertrag vorgesehen). Diese Sicherheitscodes werden auf elektronischem Weg in verschlüsselten Dateien übermittelt.
Von der Vergabe der in einem verschlossenen Umschlag übergebenen Sicherheitscodes wird nach und nach Abstand genommen. Die Verwendung wird lediglich auf die Fälle beschränkt sein, in denen eine elektronische Übermittlung nicht möglich ist.
Die CA kann vorsehen, dass der Zertifikatsinhaber oder der Antragsteller, gesetzlicher Vertreter der juristischen Person, die Signatur-PIN selbst wählt. In diesen Fällen obliegt es dem Zertifikatsinhaber oder dem Antragsteller, sich die PIN zu merken.
Die CA kann zudem dafür sorgen, dass das Signaturzertifikat für Fernverfahren über ein Authentifizierungssystem verwendet werden kann, das die RA bereitstellt und das mindestens ein substanzielles oder hohes Sicherheitsniveau aufweist, nach einer vorherigen Prüfung seiner Eigenschaften im Rahmen des Zertifizierungsumfangs der sicheren Signatureinheit. Das Authentifizierungssystem kann in diesen Fällen auch für den eventuellen Antrag auf Suspendierung und Widerruf des Zertifikats angewandt werden.

4.2.3 Annahme oder Ablehnung des Zertifikatsantrags

Nach der ersten Registrierung kann die CA oder die RA bei fehlenden oder unvollständigen Angaben, Überprüfungen der Übereinstimmung und des Umfangs der übermittelten Angaben, Überprüfungen im Hinblick auf die Betrugsbekämpfung, Zweifel über die Identität des Zertifikatsinhabers oder des Antragstellers usw. die Ausstellung des Signaturzertifikats ablehnen.

4.2.4 Maximal zulässige Bearbeitungsdauer des Zertifikatsantrags

Der Zeitraum ab dem Registrierungsantrag bis zur Ausstellung des Zertifikats hängt von dem vom Zertifikatsinhaber (oder vom Antragsteller) gewählten Antragsverfahren ab sowie von der eventuellen Notwendigkeit, weitere Informationen einzuholen oder die Einheit körperlich zu übergeben.

4.3 Ausstellung des Zertifikats

4.3.1 Handlungen der CA bei der Ausstellung des Zertifikats

4.3.1.1 Ausstellung des Zertifikats auf einer Signatureinheit (Smartcard oder Token)

Das kryptografische Schlüsselpaar wird nach vorheriger sicherer Authentifizierung von der RA direkt auf den sicheren Signatureinheiten unter Verwendung der von der CA bereitgestellten Anwendungen generiert.

Die RA übersendet der Certification Authority den Zertifikatsantrag des öffentlichen Schlüssels im PKCS#10-Format, der mit dem für diesen Zweck spezifisch genehmigten qualifizierten Signaturzertifikat digital signiert ist.

Nachdem die Certification Authority die Gültigkeit der Signatur auf dem PKCS#10 sowie die Berechtigung der Person zur Übermittlung des Antrags geprüft hat, erzeugt sie das qualifizierte Zertifikat, das über einen sicheren Kanal in die Einheit gesandt wird.

4.3.1.2 Ausstellung des Zertifikats mithilfe eines Fernsignaturmoduls (HSM)

Der Zertifikatsinhaber oder der Antragsteller authentifiziert sich gegenüber den Diensten oder den Anwendungen, die die RA zu Verfügung gestellten hat.

Die RA generiert das kryptografische Schlüsselpaar direkt auf der HSM. Die RA übersendet dann der Certification Authority den Zertifikatsantrag des öffentlichen Schlüssels im PKCS#10-Format, der mit dem für diesen Zweck spezifisch genehmigten qualifizierten Signaturzertifikat für automatische Verfahren digital signiert ist.

Nachdem die Certification Authority die Gültigkeit der Signatur auf dem PKCS#10 sowie die Berechtigung der Person zur Übermittlung des Antrags geprüft hat, erzeugt sie das qualifizierte Zertifikat, das auf dem HSM gespeichert wird.

4.3.1.3 Ausstellung des Zertifikats über ein Card Management System

Die RA generiert das kryptografische Schlüsselpaar direkt auf den Einheiten unter Nutzung eines authentisierten Card Management Systems. Das System verwaltet den ganzen Lebenszyklus der kryptografischen Einheit und sendet der Certification Authority über einen authentifizierten sicheren Kanal den Zertifikatsantrag des öffentlichen Schlüssels im Format PKCS#10.

Nachdem die Certification Authority die Gültigkeit der Signatur auf dem PKCS#10 sowie die Berechtigung der Person zur Übermittlung des Antrags geprüft hat, erzeugt sie das qualifizierte Zertifikat, das über einen sicheren Kanal in die Einheit gesandt wird.

4.3.1.4 Ausstellung des Zertifikats an eine juristische Person

Die RA generiert das kryptografische Schlüsselpaar direkt auf der HSM. Die RA übersendet dann der Certification Authority den Zertifikatsantrag des öffentlichen Schlüssels im PKCS#10-Format, der mit dem für diesen Zweck spezifisch genehmigten qualifizierten Signaturzertifikat für automatische Verfahren digital signiert ist.

Nachdem die Certification Authority die Gültigkeit der Signatur auf dem PKCS#10 sowie die Berechtigung der Person zur Übermittlung des Antrags geprüft hat, erzeugt sie das qualifizierte Zertifikat, das auf dem HSM gespeichert wird.

Wird das Schlüsselpaar in der HSM-Einheit des Zertifikatsinhabers generiert, muss dieser das signierte PKCS#10 zusenden. Nach Prüfung der Gültigkeit der Signatur auf dem PKCS#10 und Berechtigung der Person zur Zusendung des Antrags erzeugt die Certification Authority das qualifizierte Zertifikat, das auf der HSM gespeichert wird.

4.3.1.5 Zertifikatsausstellung für Testzwecke

Zuweilen müssen Zertifikate zur Durchführung von Tests im Rahmen der Produktion verwendet werden.
In diesen Fällen ist vor Ausstellung des Zertifikats die Registrierung der Daten erforderlich. Diese Registrierung muss vom Verantwortlichen der CA genehmigt werden.
In den vorgesehenen Fällen muss die Registrierungsstelle die von InfoCert für die internen Ausstellungen verwendete Stelle oder die für den Kunden des Testverfahrens konfigurierte Stelle sein.
Die zur Registrierung verwendeten Daten müssen unmissverständlich im Subject darauf hinweisen, dass es sich um ein Testzertifikat und nicht um ein reguläres Zertifikat handelt.

Dieses Verfahren kann nicht für Belastungstests oder zyklische Testsitzungen für Registrierungen und Ausstellungen eingesetzt werden.
Zum Zeitpunkt, an dem das Zertifikat beispielsweise nach Abschluss der spezifischen Testsitzung nicht mehr benötigt wird, muss es von Amts wegen widerrufen werden.

4.3.2 Benachrichtigung der Antragsteller über die erfolgte Ausstellung des Zertifikats

Bei Ausstellung auf einer kryptografischen Einheit benötigt der Zertifikatsinhaber (oder der Antragsteller) keine Benachrichtigung, da das Zertifikat in der erhaltenen Einheit vorhanden ist.
Bei LongTerm- und OneShot-Zertifikaten benachrichtigt die CA den Antragsteller mit einem automatisierten Verfahren über die Ausstellung des Zertifikats des Zertifikatsinhabers. Der Antragsteller informiert den Zertifikatsinhaber in der vertraglich vorgesehenen Art und Weise.
In den anderen Fällen erhält der Zertifikatsinhaber die Benachrichtigung über die E-Mail-Adresse, die er bei der Eintragung angegeben hat. Diese Information kann auch mit dem Antragsteller geteilt werden

4.3.3 Aktivierung

4.3.3.1 Aktivierung der Signatureinheit (Smartcard oder Token)

Nach Erhalt der Einheit aktiviert der Zertifikatsinhaber unter Nutzung der vertraulich erhaltenen Aktivierungscodes und der eigens von der CA bereitgestellten Software die Einheit und wählt gleichzeitig die Signatur-PIN, wobei die Aufbewahrung und der Schutz dieser vertraulichen Sicherheitsdaten ausschließlich dem Zertifikatsinhaber selbst obliegt.

4.3.3.2 Aktivierung der Fernsignatureinheit (HSM)

Der Zertifikatsinhaber oder der Antragsteller im Fall einer juristischen Person, wählt nach der Authentifizierung auf den CA-Portalen über die vertraulich erhaltenen Aktivierungscodes die Signatur-PIN, eine vertrauliche Sicherheitseinheit, wobei die Aufbewahrung und der Schutz dieser vertraulichen Sicherheitsdaten ausschließlich dem Zertifikatsinhaber selbst obliegt. Diese PIN wird mit der Eingabe des per SMS erhaltenen oder vom Token bzw. von der mit dem Zertifikat verbundenen Token-App generierten One-Time-Passwords bestätigt.
In einigen Fällen kann das Zertifikat bereits aktiviert und einsatzbereit ausgestellt werden.

4.4 Zertifikatsakzeptanz

4.4.1 Schlüssiges Handeln beim Akzeptieren des Zertifikats

o. A.

4.4.2 Veröffentlichung des Zertifikats durch die Certification Authority

Nach erfolgreichem Abschluss des Zertifizierungsverfahrens wird das Zertifikat in dem betreffenden Zertifikatsregister eingetragen und nicht veröffentlicht. Will der Zertifikatsinhaber sein Zertifikat veröffentlichen, kann er dies über das in § 2.2.2. beschriebene Verfahren beantragen. Der Antrag wird innerhalb von drei Arbeitstagen bearbeitet. Diese Möglichkeit ist für die LongTerm- und

OneShot-Zertifikate nicht gegeben.

4.4.3 Benachrichtigung anderer Personen über die erfolgte Veröffentlichung des Zertifikats

o. A.

4.5 Verwendung des Schlüsselpaars und des Zertifikats

4.5.1 Verwendung des privater Schlüssels und des Zertifikats durch den Zertifikatsinhaber

Der Zertifikatsinhaber hat die eventuell vorhandene Signatureinheit bzw. die Authentifizierungsmittel für die Fernsignatur sicher zu verwahren. Die Daten für die Freischaltung des privaten Schlüssels sind getrennt von der eventuell vorhandenen Einheit oder von den Mitteln bzw. den Authentifizierungscodes aufzubewahren. Er hat den Geheimhaltungsschutz und die Aufbewahrung des für die Suspendierung des Zertifikats erforderlichen Notfallcodes, sofern vorhanden, sicherzustellen. Er darf das Zertifikat nur für die von der Beschreibung der Zertifizierungspraxis und den geltenden nationalen und internationalen Gesetzen vorgesehenen Verfahren verwenden. Er hat darüber hinaus das LongTerm- und OneShot-Zertifikat im Rahmen des lt. Vertrags definierten Rahmens zu verwenden.
Er darf keine elektronischen Signaturen unter Inanspruchnahme privater Schlüssel setzen, für die das Zertifikat widerrufen oder ausgesetzt wurde, und er darf keine elektronischen Signaturen unter Inanspruchnahme eines von einer widerrufenen CA ausgestellten Zertifikats setzen .

4.5.2 Verwendung des öffentlichen Schlüssels und des Zertifikats durch Endnutzer

Der Endnutzer muss den Nutzungsbereich des Zertifikats, der in der Beschreibung der Zertifizierungspraxis und im Zertifikat genannt ist, kennen. Er hat vor Verwendung des im Zertifikat enthaltenen öffentlichen Schlüssels zu überprüfen, ob das Zertifikat gültig ist und nicht suspendiert oder widerrufen wurde, und dafür die betreffenden Listen in dem Zertifikatsregister zu kontrollieren. Zudem hat er das Bestehen und den Inhalt eventueller Verwendungsbeschränkungen des Schlüsselpaars, Vertretungsbefugnisse und Berufsbefähigungen zu überprüfen.

4.5.3 Nutzungs- und Wertbeschränkungen

Von der RA kann nach Vorlage unterstützender Unterlagen die Aufnahme in das qualifizierte Signaturzertifikat der von AgID festgelegten Nutzungsbeschränkungen verlangt werden

- Die Inhaber dürfen das Zertifikat nur für jene Arbeitszwecke nutzen, für die es ausgestellt wurde. The certificate holder must use the certificate only for the purposes for which it is

issued.

- Die Nutzung des Zertifikats ist auf die Beziehungen mit [Person, mit dem das Zertifikat verwendet werden kann] beschränkt. The certificate may be used only for relations with the [the subject with which the certificate can be used]

Die qualifizierten Signaturzertifikate **für automatische Verfahren** enthalten die von AgID definierte Nutzungsbeschränkung:

- Dieses Zertifikat ist nur für Signaturen gültig, die mit automatischen Verfahren gesetzt wurden. Diese Erklärung stellt den Nachweis der Anwendung eines solchen Verfahrens für die signierten Dokumente dar.
- The certificate may be used only for automatic procedure signature purposes

Die auf Grundlage der **4-AutID-Identifizierung über den eIDAS-Knoten oder auf Grundlage der eDocID-Identifizierung** ausgestellten Zertifikate enthalten den OID 1.3.76.16.5 und die folgende Nutzungsbeschränkung:

- Certificate not usable to require SPID digital identity

Gemäß der Benachrichtigung Nr. 17 vom 24. Januar 2019 enthalten die auf Grundlage der **4-AutID-Identifizierung** unter Verwendung der digitalen Identitäten SPID ausgestellten Zertifikate den OID 1.3.76.16.5 und die folgende Nutzungsbeschränkung:

- Certificate issued through Sistema Pubblico di Identità Digitale (SPID) digital identity, not usable to require other SPID digital identity

Der Zertifikatsinhaber oder der Antragsteller kann zudem von der Certification Authority die Aufnahme von personalisierten Nutzungsbeschränkungen (max. 200 Zeichen) oder Wertgrenzen verlangen. Die Beantragung, andere spezifische Nutzungsbeschränkungen aufzunehmen, wird von der CA aufgrund der rechtlichen und technischen Aspekte sowie der Interoperabilität beurteilt und diesbezüglich bewertet.

Nutzungsbeschränkung für LongTerm- und OneShot-Zertifikate

Die LongTerm-Zertifikate können auf die ausschließliche Nutzung in der im Vertrag konkret genannten Domain für die Signierung von elektronischen Dokumenten beschränkt sein, die dem Zertifikatsinhaber von der CA oder dem Antragsteller zur Verfügung gestellt wurden. In diesen Fällen können die elektronischen Dokumente Beziehungen zwischen dem Antragsteller und dem Zertifikatsinhaber betreffen oder Dokumente Dritter sein.

Im **LongTerm-Zertifikat** wird also eine der folgenden Nutzungsbeschränkungen angegeben:

- Das Zertifikat kann nur in den Beziehungen zwischen dem Inhaber und dem Antragsteller genutzt werden. The certificate can be used only in the relationships between the holder and the requestor (max. 200 Zeichen).
- Zertifikat für die Signierung von Produkten und Dienstleistungen, die von [Name Zertifikatsinhaber] zur Verfügung gestellt werden. Certificate to subscribe product and services made available by [Name des Zertifikatsinhabers] (max. 200 Zeichen).

Das **One-Shot-Zertifikat** besitzt folgende Nutzungsbeschränkungen:

- Die Nutzung des Zertifikats ist auf die Signierung der zugrunde liegenden Dokumente beschränkt. The use of the certificate is technically limited to the signature of the underlying documents.

Unbeschadet der Haftung der CA gemäß CAD (Art. 30) ist der Nutzer (die Person, die das signierte Dokument erhält) für die Überprüfung der Einhaltung der in das Zertifikat aufgenommenen Nutzungsbeschränkungen und Wertgrenzen verantwortlich. Die CA haftet daher nicht für Schäden, die durch die Nutzung eines qualifizierten Zertifikats verursacht werden, welches die im Zertifikat gesetzten oder die durch Überschreitung der Wertgrenze bedingten Beschränkungen überschreitet.

4.6 Erneuerung des Zertifikats

4.6.1 Gründe für die Erneuerung

Die Erneuerung ermöglicht, ein neues Signaturzertifikat zu erhalten, das zur Signatur von Dokumenten und Transaktionen genutzt werden kann. Bei den automatischen Signaturzertifikaten, den LongTerm-, OneShot- und den an eine juristische Person ausgestellten Zertifikaten ist eine Erneuerung nicht vorgesehen, stattdessen ist eine neue Identifizierung und eine Neuausstellung durchzuführen.

4.6.2 Wer kann die Erneuerung beantragen

Der Zertifikatsinhaber kann die Erneuerung des Zertifikats vor seinem Ablauf nur beantragen, wenn dieses nicht widerrufen wurde und wenn alle bei der vorhergehenden Ausstellung gelieferten Informationen noch gültig sind. Nach dem Ablaufdatum ist eine Erneuerung nicht mehr möglich. Es muss ein neues Zertifikat beantragt werden.
Das Erneuerungsverfahren gilt ausschließlich für Zertifikate, die von InfoCert ausgestellt wurden.

4.6.3 Bearbeitung des Antrags auf Erneuerung des Zertifikats

Die Erneuerung erfolgt über einen von der CA bereitgestellten Dienst im Rahmen der Geschäfts- und Vertragsbeziehungen, die mit dem Zertifikatsinhaber und mit der RA, soweit vorhanden, definiert wurden.

4.7 Neuausstellung des Zertifikats

o. A.

4.8 Änderung des Zertifikats

o. A.

4.9 Widerruf und Suspendierung des Zertifikats

Der Widerruf oder die Suspendierung eines Zertifikats entzieht diesem die Gültigkeit vor dem

festgelegten Ablauf und macht nach dem Zeitpunkt der Veröffentlichung des Widerrufs gesetzte Signaturen ungültig. Die von der CA ausgestellten und widerrufenen oder suspendierten Zertifikate werden in eine von der CA signierte Sperrliste (CRL) eingetragen. Diese List wird im Zertifikatsregister mit einer vorab festgelegten Regelmäßigkeit veröffentlicht. Die CA kann aufgrund besonderer Umstände eine außerplanmäßige Ausgabe der CRL erzwingen. Der Widerruf und die Suspendierung sind ab der Veröffentlichung der Liste wirksam. Dieser Zeitpunkt wird durch das Datum bescheinigt, das auf der Registrierung des Vorfalls im Kontrolljournal der Certification Authority gesetzt ist.

4.9.1 Gründe für den Widerruf

Die Bedingungen, weshalb der Widerruf beantragt werden muss, sind folgende:

1. der private Schlüssel wurde kompromittiert oder es liegt einer der folgenden Fälle vor:
   - die sichere Signatureinheit, die den Schlüssel enthält, ist verloren gegangen;
   - die Geheimhaltung des Schlüssels oder seines Aktivierungscodes (PIN) ist nicht mehr gegeben oder das OTP-Gerät wurde kompromittiert bzw. ist verloren gegangen;
   - es ist ein Ereignis eingetreten, das die Stufe der Vertrauenswürdigkeit des Schlüssels beeinträchtigt hat;
2. der Zertifikatsinhaber kann die sich in seinem Besitz befindende sichere Signatureinheit nicht mehr nutzen, zum Beispiel wegen eines Defekts;
3. die im Zertifikat enthaltenen Daten des Zertifikatsinhabers haben sich geändert und sind nicht mehr richtig und/oder wahrheitsgemäß;
4. die Beziehung zwischen dem Zertifikatsinhaber und der CA oder zwischen dem Antragsteller und der CA endet;
5. es wird eine wesentliche Nicht-Einhaltung dieser Beschreibung der Zertifizierungspraxis festgestellt.

4.9.2 Wer kann den Widerruf beantragen?

Der Widerruf des Zertifikats kann beantragt werden:

- vom Zertifikatsinhaber;
- vom Antragsteller oder betroffenen Dritten;
- von Amts wegen von der CA;
- von der NCA bei einem Antrag auf Widerruf eines QSealC-PSD2-Zertifikats.

4.9.3 Verfahren für die Beantragung des Widerrufs

Nachstehend werden die Verfahren geschildert, mit denen die Berechtigten den Widerruf beantragen können.

Beantragung durch den Zertifikatsinhaber: Der Widerruf kann durch Unterzeichnung eines Formulars auf der Website InfoCert beantragt werden. Das vorgenannte Formular kann der RA übergeben oder per Einschreiben, zertifizierte E-Mail oder Fax mit beigefügter Fotokopie eines gültigen Ausweises direkt an die CA gesendet werden. Die CA oder die RA können außerdem weitere

Verfahrensweisen für die Übermittlung des Widerrufsantrags zur Verfügung stellen, sofern diese eine korrekte Identifizierung des Zertifikatsinhabers vorsehen. Die CA oder die RA teilen diese dem Zertifikatsinhaber ordnungsgemäß mit.

Die CA oder die RA prüfen die Authentizität des Antrags, wonach sie das Zertifikat widerrufen und den Zertifikatsinhaber und gegebenenfalls den Antragsteller darüber sofort unterrichten.

Sind in dem Zertifikat, für das der Widerruf beantragt wurde, Informationen über die Rolle des Zertifikatsinhabers enthalten, teilt die CA den erfolgten Widerruf dem eventuell betroffenen Dritten, mit dem spezifische Vereinbarungen bestehen, mit. Ist in dem Zertifikat, das Gegenstand des Widerrufs ist, die Organisation angegeben, teilt die CA dieser den erfolgten Widerruf mit. Zusätzliche Verfahren für den Widerrufsantrag durch den Zertifikatsinhaber können in den eventuellen Vereinbarungen zwischen dem Zertifikatsinhaber und der CA definiert werden

Für den Widerruf von LongTerm- und OneShot-Zertifikaten kann der Zertifikatsinhaber den Widerruf des Zertifikats beantragen, indem er sich hierfür bei den von der RA und/oder der CA zur Verfügung gestellten Systemen, auch über Anwendungsdienste, wie in der Vertragsdokumentation erläutert authentifiziert.

Beantragung durch den Antragsteller oder den betroffenen Dritten: Der Widerruf des Zertifikats des Zertifikatsinhabers kann mit den gleichen Verfahren beantragt werden, die für den Zertifikatsinhaber gelten. Es sind außerdem die Daten des Zertifikatsinhabers anzugeben, die zum Zeitpunkt der Zertifikatsausstellung der CA mitgeteilt wurden.

Die CA oder die RA prüfen die Authentizität des Antrags, damit die CA das Zertifikat widerrufen kann. Gleich danach benachrichtigen sie darüber den Zertifikatsinhaber mit dem bei der Beantragung des Zertifikats festgelegten Kommunikationsmittel. Zusätzliche Verfahren für den Widerrufsantrag durch den Zertifikatsinhaber können in den eventuellen Vereinbarungen zwischen dem Zertifikatsinhaber und der CA oder RA definiert werden.

Für den Widerruf von LongTerm- und OneShot-Zertifikaten kann der Antragsteller den Widerruf des Zertifikats des Zertifikatsinhabers beantragen, indem er sich hierfür bei den von der CA zur Verfügung gestellten Systemen, auch über Anwendungsdienste, wie in der Vertragsdokumentation erläutert authentifiziert.

Widerruf von Amts wegen durch die CA/RA: Falls notwendig, kann die CA das Zertifikat widerrufen. Sie teilt dies dem Zertifikatsinhaber vorab unter Angabe der Widerrufsgründe sowie des Datums und der Uhrzeit des Widerrufs mit.

Sind in dem Zertifikat, das Gegenstand des Widerrufs ist, Informationen über die Rolle des Zertifikatsinhabers enthalten, teilt die CA/RA den erfolgten Widerruf dem eventuell betroffenen Dritten, mit dem spezifische Vereinbarungen bestehen, mit. Ist in dem Zertifikat, das Gegenstand des Widerrufs ist, die Organisation angegeben, teilt die CA dieser den erfolgten Widerruf mit. Die CA/RA teilt den erfolgten Widerruf auch dem Antragsteller mit.

Beantragung durch die NCA: Im Fall eines Widerrufsantrags eines QSealC-PSD2-Zertifikats kann der Widerruf durch die NCA beantragt werden, die dem Zahlungsdienstleister (PSP) die im Zertifikat angeführte Autorisierungsnummer erteilt hat.

4.9.4 Übergangsfrist des Widerrufsantrags

Die Übergangsfrist der CRL ist der Zeitraum zwischen der Veröffentlichung der nächsten CRL durch die CA und dem Ablauf der aktuellen CRL. Damit keine der beteiligten Parteien ausfälle erleiden, ist dieser Zeitraum länger als jener der CA für die Erstellung und Veröffentlichung einer neuen CRL. Auf diese Weise bleibt die aktuelle CRL mindestens gültig, bis sie nicht von der neuen CRL ersetzt wird.

4.9.5 Maximal zulässige Bearbeitungsdauer des beantragten Widerrufs

Der Antrag wird innerhalb von einer Stunde bearbeitet, sofern nicht weitere Kontrollen bezüglich seiner Authentizität erforderlich sind. Bei ordnungsgemäßer Authentisierung des Antrags wird dieser sofort bearbeitet. Anderenfalls wird das Zertifikat in Erwartung der Durchführung weiterer Untersuchungen der Authentizität des eingegangenen Antrags ausgesetzt.

4.9.6 Anforderungen für die Überprüfung des Widerrufs

o. A.

4.9.7 Häufigkeit der Veröffentlichung der CRL

Die widerrufenen oder suspendierten Zertifikate werden in eine von der CA signierten Sperrliste (CRL) eingetragen und im öffentlichen Register veröffentlicht. Die CRL wird planungsgemäß jede Stunde veröffentlicht (ordentliche Ausgabe). Die CA kann aufgrund besonderer Umstände eine außerplanmäßige Ausgabe der CRL erzwingen (sofortige außerordentliche Ausgabe), zum Beispiel in dem Fall, in dem der Widerruf oder die Suspendierung eines Zertifikats wegen des Verdachts der Kompromittierung der Geheimhaltung des privater Schlüssels erfolgt (sofortiger Widerruf oder sofortige Suspendierung). Die CRL wird immer vollständig veröffentlicht. Der Zeitpunkt der Veröffentlichung der CRL wird unter Nutzung des Datums des Systems der Time Stamping Authority InfoCert als Bezugszeit bescheinigt. Diese Registrierung wird in das Überwachungsprotokoll eingetragen. Jedes Element der CRL-Liste enthält in der betreffenden Erweiterung das Datum und die Uhrzeit des Widerrufs oder der Suspendierung. Die CA behält sich vor, andere CRLs, Untergruppen der allgemeinen CRL, getrennt zu veröffentlichen, um die Netzbelastung zu reduzieren. Das Beziehen und Abfragen der CRL obliegt dem Nutzer. Die für das spezifische Zertifikat abzufragende CRL ist gemäß den geltenden Rechtsvorschriften im Zertifikat selbst angegeben.

4.9.8 Maximale Latenzzeit der CRL

Nachdem die Authentizität des Widerrufs- oder Suspendierungsantrags geprüft wurde, beträgt die Wartezeit zwischen der Übermittlung an die CA und seiner Veranlassung über die Veröffentlichung der CRL höchstens eine Stunde.

4.9.9 Online-Dienste zur Prüfung des Widerrufsstatus des Zertifikats

InfoCert stellt neben der Veröffentlichung der CRL in den LDAP- und HTTP-Verzeichnissen auch einen OCSP-Dienst für die Statusprüfung des Zertifikats bereit. Die URL des Dienstes ist im Zertifikat angeben. Der Dienst ist rund um die Uhr, 7 Tage die Woche verfügbar.

4.9.10 Anforderung von Online-Überprüfungsdiensten

S. Anhang A

4.9.11 Andere Formen des Widerrufs

o. A.

4.9.12 Spezifische Anforderungen für einen Schlüsselwechsel (Re-Keying) bei Kompromittierung

o. A.

4.9.13 Gründe für die Suspendierung

Die Suspendierung ist bei Eintritt der folgenden Bedingungen durchzuführen:

1. Es wurde ein Widerruf beantragt, ohne die Möglichkeit, rechtzeitig die Authentizität des Antrags festzustellen.
2. Der Zertifikatsinhaber, der Antragsteller oder der betroffene Dritte, die RA oder die CA haben Zweifel über die Gültigkeit des Zertifikats;
3. Es sind Zweifel über die Sicherheit der Signatureinheit oder das eventuell vorhandene OTP-Gerät aufgetreten.
4. Es ist eine vorübergehende Unterbrechung der Gültigkeit des Zertifikats notwendig.

In den genannten Fällen wird die Suspendierung des Zertifikats gegebenenfalls unter Angabe der Dauer beantragt. Nach Ablauf dieses Zeitraums oder nach Beantragung einer erneuten Aktivierung des Zertifikats folgt entweder ein endgültiger Widerruf oder die erneute Wiederaufnahme der Zertifikatsgültigkeit.

Bei einem Verdacht auf Identitätsdiebstahl kann die CA ohne Vorankündigung und aus Sicherheitsgründen eine Suspendierung vornehmen.

4.9.14 Wer kann die Suspendierung beantragen?

Die Suspendierung kann von dem Zertifikatsinhaber jederzeit und aus jedem Grund beantragt werden. Die Suspendierung des Zertifikats kann zudem auch von dem Antragsteller oder dem betroffenen Dritten aus den Gründen und mit den Verfahren gemäß dieser CPS beantragt werden. Schließlich kann das Zertifikat von Amts wegen von der CA ausgesetzt werden.

4.9.15 Verfahren für die Beantragung der Suspendierung

Die einfachste Weise, um die Suspendierung des Zertifikats zu beantragen, erfolgt über den entsprechenden Link der Website. Der Antragsteller wählt die Dauer der Suspendierung. Sollte er keine Angabe in diesem Sinne machen, bleibt das Zertifikat bis zur Fälligkeit suspendiert und wird dann widerrufen. Die Suspendierung endet um 24:00:00 Uhr des letzten Tags des beantragten Suspendierungszeitraums.

Einigen Kunden wird angesichts besonderer vertraglicher Abmachungen eine Reaktivierungsfunktion zur Verfügung gestellt. In diesem Fall kann das Zertifikat nur dann reaktiviert werden, wenn es nicht abgelaufen ist

4.9.15.1 Vom Zertifikatsinhaber beantragte Suspendierung

Der Zertifikatsinhaber hat die Suspendierung mit einem der folgenden Verfahren zu beantragen:

1. durch die auf der Website der CA bereitgestellte Suspendierungsfunktion unter Mitteilung der angeforderten Daten und Nutzung des Notfallcodes, der bei der Ausstellung des Zertifikats übergeben wurde, sofern bekannt.
2. durch Nutzung der Suspendierungsfunktion (soweit verfügbar) mit dem auf der Website verfügbaren OTP, die in der Vertragsdokumentation genannt ist, die bei der Registrierung soweit bekannt, wurde;
3. durch einen Anruf beim Callcenter der CA und Mitteilung der erforderlichen Informationen. Sollte kein Notfallcode vorhanden sein und nur in dem Fall, dass es sich um einen Suspendierungsantrag wegen Kompromittierung eines Schlüssels handelt, aktiviert das Callcenter nach Überprüfung der Telefonnummer des eingegangenen Anrufs eine sofortige Suspendierung des Zertifikats für eine Dauer von 10 (zehn) Kalendertagen in Erwartung des schriftlichen Antrags des Zertifikatsinhabers. Erhält die CA den unterzeichneten Antrag nicht innerhalb der genannten Frist, reaktiviert sie das Zertifikat;
4. über die Kontakte der Registration Authority, die die notwendigen Daten und Dokumente verlangt, alle erforderlichen Überprüfungen angesichts der Identität des Zertifikatsinhabers durchführt und schließlich bei der CA die Suspendierung beantragt;
5. durch Nutzung der Suspendierungsfunktion, die auf der Webinterface der RA für die CMS-Dienste verfügbar ist.

Sind in dem Zertifikat, für das die Suspendierung beantragt wurde, Informationen über die Rolle des Zertifikatsinhabers enthalten, teilt die CA die erfolgte Suspendierung dem eventuell betroffenen Dritten, mit dem spezifische Vereinbarungen bestehen, mit.

Ist in dem Zertifikat, das Gegenstand der Suspendierung ist, die Organisation angegeben, teilt die CA dieser die erfolgte Suspendierung mit.

Sofern es der Vertrag über das suspendierte Zertifikat vorsieht, unterrichtet die CA auch den Antragsteller über die erfolgte Suspendierung.

4.9.15.2 Vom Antragsteller oder dem betroffenen Dritten beantragte Suspendierung

Der Antragsteller oder der betroffene Dritte kann zudem die Suspendierung des Zertifikats des Zertifikatsinhabers beantragen, indem er das eigens dafür bestimmte Formular, das auf der Website der CA und bei den RAs zur Verfügung steht, unter Angabe der Gründe ausfüllt. Er hat dabei die eventuell vorhandene Dokumentation beizulegen und die der CA zum Zeitpunkt der Zertifikatsausstellung mitgeteilten Daten des Zertifikatsinhabers genau anzugeben.

Die CA überprüft die Authentizität des Antrags, setzt den Zertifikatsinhaber davon gemäß den bei der Zertifikatsbeantragung festgelegten Mitteilungsverfahren in Kenntnis und führt die

Suspendierung durch. Zusätzliche Verfahren für das Suspendierungsverlangen durch den Antragsteller oder des betroffenen Dritten können in den eventuell zwischen dem Letztgenannten und der CA abgeschlossenen Vereinbarungen definiert werden.

Für die Suspendierung von LonTerm- und OneShot-Zertifikaten kann der Antragsteller die Suspendierung des Zertifikats des Zertifikatsinhabers beantragen, indem er sich hierfür bei den von der CA zur Verfügung gestellten Systemen, auch über Anwendungsdienste, wie in der Vertragsdokumentation erläutert authentifiziert.

4.9.15.3 Suspendierung auf Initiative der CA

Die CA teilt, sofern es sich nicht um Dringlichkeitsfälle handelt, dem Zertifikatsinhaber vorab die Absicht der Suspendierung des Zertifikats unter Angabe des Suspendierungsgrunds und des Datums des Suspendierungsbeginns und -endes mit. Diese letztgenannten Informationen werden dem Zertifikatsinhaber auf jeden Fall so bald wie möglich mitgeteilt.
Sind in dem Zertifikat, für das die Suspendierung beantragt wurde, Informationen über die Rolle des Zertifikatsinhabers enthalten, teilt die CA die erfolgte Suspendierung dem eventuell betroffenen Dritten, mit dem spezifische Vereinbarungen bestehen, mit. Ist in dem Zertifikat, für das die Suspendierung beantragt wurde, die Organisation angegeben, teilt die CA dieser die erfolgte Suspendierung mit.

Sofern es der Vertrag über das suspendierte Zertifikat vorsieht, unterrichtet die CA auch den Antragsteller über die erfolgte Suspendierung.

4.9.16 Befristung der Suspendierung

Die Dauer der Suspendierung wird vom Antragsteller gewählt und kann den Gültigkeitszeitraum des Zertifikats nicht überschreiten. Nach Ablauf des beantragten Suspendierungszeitraums wird die Gültigkeit des Zertifikats durch Löschung des Zertifikats aus der Sperrliste (CRL) wieder in Kraft gesetzt. Die erneute Aktivierung erfolgt innerhalb von 24 Stunden nach dem Enddatum der Suspendierung. Fällt der Tag des Ablaufs der Suspendierung mit dem Tag des Ablaufs des Zertifikats zusammen, wird die Suspendierung in einen Widerruf mit Wirkung ab Beginn der Suspendierung umgewandelt.

Sofern es der Vertrag vorsieht, kann die Reaktivierung des Zertifikats vor dem Ablaufdatum der Suspendierung beantragt werden.

Erfolgte die Suspendierung über ein CMS, kann die Reaktivierungsfunktion verwendet werden, die auf der Webinterface für die CMS-Dienste verfügbar ist.

4.10 Dienste betreffend den Zertifikatsstatus

4.10.1 Funktionsmerkmale

Die Informationen über den Status der Zertifikate sind in der CRL und über den OCSP-Dienst zur Verfügung. Die Seriennummer eines widerrufenen Zertifikats bleibt auch nach Ablauf der Gültigkeit des Zertifikats und zumindest bis zum Ablauf des CA-Zertifikats in der CRL.
Die vom OCSP-Dienst für die Zertifikate gelieferten Informationen werden in Echtzeit aktualisiert.

4.10.2 Verfügbarkeit des Dienstes

Der OCSP-Dienst und die CRLs sind 24 Stunden an 7 Tagen der Woche verfügbar.

4.10.3 Optionale Merkmale

o. A.

4.11 Kündigung der CA-Dienste

Die Beziehung des Zertifikatsinhabers und/oder des Antragstellers mit der Certification Authority endet mit Ablauf des Zertifikats oder seines Widerrufs, sofern vertraglich nicht besondere Fälle bestimmt wurden.

4.12 Hinterlegung des Schlüssels bei Dritten und dessen Wiederherstellung

o. A.

5 SICHERHEITSMASSNAHMEN UND KONTROLLEN

Der Vertrauensdiensteanbieter InfoCert besitzt ein Sicherheitssystem des IT-Systems für den Dienst der digitalen Zertifizierung. Das implementierte Sicherheitssystem gliedert sich in drei Ebenen:

- eine physikalische Ebene, auf der die Sicherheit der Umgebungen sichergestellt werden soll, in denen am TSP den Dienst verwaltet,
- eine Verfahrensebene mit typischen organisatorischen Aspekten,
- eine Logikebene über die Bereitstellung von technischen Hardware- und Softwaremaßnahmen für die Probleme und Risiken im Zusammenhang mit der Art des Dienstes und mit der verwendeten Infrastruktur.

Dieses Sicherheitssystem wurde entwickelt, um die Risiken zu vermeiden, die aus Funktionsstörungen der Systeme, des Netzes und der Anwendungen sowie aus unberechtigtem Lesen oder Änderung der Daten entstehen.

Ein Auszug der InfoCert-Sicherheitsrichtlinie kann bei der zertifizierten E-Mail-Adresse infocert@legalmail.itangefordert werden.

5.1 Physische Sicherheit

Die ergriffenen Maßnahmen liefern angemessene Sicherheit in Bezug auf:

- die Merkmale des Gebäudes und der Konstruktion;
- die aktiven und passiven Eindringschutzsysteme;
- die Kontrolle der physischen Zugänge;
- die Stromversorgung und die Klimaanlage;
- den Brandschutz;
- den Schutz gegen Wassereinbruch;
- die Verfahrensweisen für die Archivierung von magnetischen Datenträgern;
- die Archivierungsorte von magnetischen Datenträgern.

5.1.1 Position und Konstruktion der Struktur

Das Rechenzentrum von InfoCert befindet sich in Padua. Der Standort der Disaster Recovery ist Modena. Er ist mit dem oben genannten Rechenzentrum über eine eigene redundante Anbindung auf zwei verschiedenen MPLS-Netzwerken mit einer Geschwindigkeit von je 40 Gbit/s (upgrade-fähig auf 100 Gbit/s), verbunden.

An beiden Standorten sind geschützte Räume mit den höchsten physischen und logischen Sicherheitsstufen eingerichtet, in denen IT-Geräte aufgestellt sind, die den Kern der Dienste der digitalen Zertifizierung, Zeitstempelung, Fernsignatur und automatischen Signatur darstellen.

Für die Business-Continuity-Dienste mit nahezu bei Null liegenden RTO/RPO-Werten sind einige Komponenten der CA-Dienste im Hinblick auf CRL-Veröffentlichung und OCSP in die AWS-Cloud

jeweils in der Region Europa Frankfurt und in der Region Europa Irland ausgelagert. Um darüber hinaus die Business-Continuity für die CA „InfoCert Qualified Electronic Signature CA 4“ zu garantieren, wird eine verschlüsselte Kopie der Daten auf der AWS-Cloud in der Region Europa Frankfurt ausgeführt.

AWS verfügt über Konformitätszertifizierungen nach den Standards ISO/IEC 27001:2013, 27017:2015, 27018:2019 und ISO/IEC 9001:2015.

Abbildung 2 – Standort Rechenzentrum von InfoCert und der Disaster Recovery

5.1.2 Physischer Zugang

Der Zugang zum Rechenzentrum ist durch die InfoCert-Sicherheitsverfahren geregelt. Im Bunkerbereich im Rechenzentrum befinden sich die Systeme der CA befinden und für den ein weiterer Sicherheitsfaktor verlangt wird.

5.1.3 Elektro- und Klimatisierungsanlage

Der Standort in Padua, an dem sich das Rechenzentrum von InfoCert befindet, ist zwar nicht zertifiziert, besitzt aber die Eigenschaften eines Tier-3-Rechenzentrums.

Die technischen Räume sind mit einem Stromversorgungssystem ausgestattet, um Störungen und vor allem Ausfällen vorzubeugen. Die Systemversorgung verfügt über die modernsten Technologien, um die Zuverlässigkeit zu erhöhen und die Redundanz der kritischsten Funktionen für die Erbringung der Dienstleistungen sicherzustellen.

Die Infrastruktur für die Versorgung umfasst:

- unterbrechungsfreie Stromversorgung, ausgestattet mit Wechselstrom -Akkumulatoren (USV);
- verfügbare Wechselspannung (220-380V AC);

- Schaltschränke mit redundanter Versorgung mit geschützten Leitungen, die für die entsprechende Aufnahme dimensioniert sind;
- Notstromaggregate;
- automatische Umschalt- und Synchronisierungseinrichtung zwischen Stromaggregaten, Netz und Akkumulatoren (STS).

Jeder im Rechenzentrum eingebaute Technikschrank nutzt zwei Stromleitungen, die im Fall einer Unterbrechung die Hochverfügbarkeit (HA) einer der beiden verfügbaren Linien sichert.

Der Technikschrank wird fernüberwacht. Es werden regelmäßige Kontrollen über den Status der Stromleitung (ein/aus) und der abgenommene Strom durchgeführt (keine Leitung darf 50 % der Last überschreiten)

Im Technikbereich herrscht normalerweise eine Temperatur von 20 ° bis 27 ° mit einem Feuchtigkeitsgehalt von 30 % bis 60 %. Die Anlagen sind mit Kondensatorbatterien mit versiegeltem System zum Sammeln und Entladen des Kondenswassers ausgestattet, das von einer Leckagesonde kontrolliert wird. Das gesamte Temperaturregelungssystem ist für Stromausfälle mit Notstromaggregaten gekoppelt. Jeder Schrank ist gekühlt, mit einer vorgesehenen Höchstleistung von 10 KW und höchstens 15 KW bei zwei nebeneinander stehenden Schränken.

5.1.4 Wasserschutz und Sicherheitsvorkehrungen

Das Gebiet des Gebäudes stellt keine Umweltrisiken aufgrund der Nähe von „gefährlichen“ Strukturen dar. Bei der Planung des Werks wurden sachgemäße Vorkehrungen getroffen, um die potenziell gefährlichen Räume zu isolieren, wie jene, in denen sich das Stromaggregat und die Heizanlage befinden.
Der Bereich, in dem sich die Geräte befinden, liegt im Erdgeschoss, das jedoch über dem Straßenniveau liegt.

5.1.5 Brandprävention und -schutz

Das Rechenzentrum besitzt eine Brandmeldeanlage, die von einer adressierbaren analogen NOTIFIER-Zentrale mit optischen Sensoren in den Räumen und in der Zwischendecke sowie mit Luftsensoren unter dem Fußboden und in den Luftkanälen verwaltet wird.
Die Brandmeldeanlage ist mit automatischen und umweltfreundlichen Gaslöschanlagen NAFS125 und PF23 und in einigen Räumen mit Aerosol-Löschanlagen verbunden.
Bei gleichzeitiger Aktivierung von zwei Meldern in demselben Bereich wird im betroffenen Bereich der Austritt des Löschmittels aktiviert.
Für jeden Brandabschnitt ist eine eigene Löschanlage vorgesehen.
Außerdem sind gemäß Gesetz und den geltenden Rechtsvorschriften tragbare Feuerlöscher vorhanden.
Die mit den Geräteräumen verbundenen Primärluftkanälen sind an den Übergängen der Brandabschnitte mit Brandschutzklappen ausgestattet, die von der automatischen Rauchmeldeanlage gesteuert werden.

5.1.6 Speichermedien

Die Speicherplattform umfasst im NAS-Bereich NetApp-Systeme(FAS 8060). Was den SAN-Bereich anbelangt, wurde dagegen eine auf Infinidat-Technologien mit 2 InfiniBox-Enclosures der

Generation F4000 und F6000 basierte Infrastruktur implementiert; für den CA-Bereich basiert die Infrastruktur auf der Pure-Storage-Technologie.

5.1.7 Abfallentsorgung

InfoCert ist nach ISO 14001 für das nachhaltige Umweltmanagement seiner Produktionszyklen, einschließlich der Abfalltrennung und der nachhaltigen Abfallentsorgung zertifiziert. Hinsichtlich des Dateninhalts von Elektronikabfällen werden alle Medien vor der Beseitigung gemäß den geregelten Verfahren bzw. unter Beteiligung eines zertifizierten Entsorgungsunternehmens bereinigt.

5.1.8 Offsite-Backup

Dieses erfolgt am Disaster-Recovery-Standort mithilfe eines EMC Data Domain 4200, auf dem die primäre Data Domain des Standorts Padua die Back-up-Daten repliziert.

5.2 Verfahrenskontrollen

5.2.1 Schlüsselrollen

Die Schlüsselrollen werden von Figuren besetzt, die die erforderliche Erfahrung, Professionalität und die technischen wie rechtlichen Kompetenzen besitzen, die mit jährlichen Beurteilungen ständig überprüft werden.
Die Liste der Namen und das Organigramm der Figuren in Schlüsselrollen wurde bei der ersten Akkreditierung bei der AgID hinterlegt und wird im Laufe der natürlichen Entwicklung der Unternehmensorganisation ständig aktualisiert.

5.3 Kontrolle des Personals

5.3.1 Verlangte Qualifikationen, Erfahrungen und Genehmigungen

Nach Abschluss des Personaljahresplanung ermittelt der Leiter der Funktion/Organisationsstruktur die Eigenschaften und Fähigkeiten des einzustellenden Personals (*Job Profile*). Danach wird in Absprache mit dem Leiter der Auswahlverfahren das Such- und Auswahlverfahren eingeleitet.

5.3.2 Überprüfung der Vorerfahrungen

Die ausgesuchten Bewerber nehmen an einem Auswahlverfahren teil und nehmen an einem ersten Informationsgespräch mit dem Leiter des Auswahlverfahrens teil, bei dem auch die Gründe für die Bewerbung hinterfragt werden. Diesem Gespräch folgt ein fachbezogenes Gespräch mit dem Leiter der Funktion/Organisationsstruktur, bei dem die vom Bewerber angegebenen Fähigkeiten geprüft werden. Weitere Prüfungsmittel sind Übungen und Tests.

5.3.3 Schulungsanforderungen

Um sicherzustellen, dass niemand aus Eigeninitiative die globale Sicherheit des Systems schädigen

bzw. abändern kann oder nicht genehmigte Eingriffe durchführt, ist die operative Verwaltung des Systems verschiedenen Personen mit getrennten und genau definierten Aufgaben anvertraut. Das für die Planung und Erbringung des Zertifizierungsdienstes zuständige Personal ist bei InfoCert beschäftigtes Personal, das auf Grundlage dessen Erfahrung in der Planung, Durchführung und Leitung von IT-Diensten sowie der Zuverlässigkeit und Vertraulichkeit ausgewählt wurde. Regelmäßige Schulungsmaßnahmen tragen dazu bei, das Bewusstsein für die zugewiesenen Aufgaben zu entwickeln. Insbesondere erfolgen vor der Eingliederung des Personals in die operativen Tätigkeiten Schulungsmaßnahmen mit dem Zweck, alle für die Durchführung der zugeteilten Aufgaben erforderlichen (technischen, organisatorischen und verfahrensbezogenen) Kompetenzen zu vermitteln.

5.3.4 Aktualisierung des Schulungsangebots

Am Anfang eines jeden Jahres erfolgt immer die vorbereitende Analyse des Schulungsbedarfs zur Festlegung der im Laufe des Jahrs durchzuführenden Schulungsaktivitäten. Die Analyse ist wie folgt aufgebaut:

- Treffen mit der Leitung zur Erhebung der Daten über den Bedarf an notwendigen Schulungen zur Erreichung der Unternehmensziele;
- Befragung der Leiter für die Feststellung des spezifischen Schulungsbedarfs der jeweiligen Bereiche;
- Weiterleitung der erhobenen Daten an die Unternehmensleitung zum Abschluss und zur Bewilligung des Schulungsplans.

Im Februar wird der so definierte Schulungsplan mitgeteilt und veröffentlicht.

5.3.5 Häufigkeit des Arbeitsschichtenwechsels

Die Anwesenheit vor Ort wird über einen Dienstplan geregelt, der vom Leiter der Organisationseinheit monatlich und mit mindestens 10 Tage Vorlauf erstellt wird. Jede Schicht besteht aus 8 Arbeitsstunden.
Unbeschadet des Vorhandenseins der notwendigen fachlichen und beruflichen Voraussetzungen sorgt das Unternehmen dafür, dass sich eine höchstmögliche Zahl von Arbeitnehmern im Schichtdienst wechselt, wobei den Mitarbeitern, die dies wünschen, Vorrang eingeräumt wird.
Es sind keine Nachtschichten vorgesehen. Die Schichten mit Anwesenheit vor Ort erfolgen in einem Zeitfenster von 07:00 bis 21:00 Uhr von Montag bis Freitag und von 07:00 bis 12:00 Uhr am Samstag.

5.3.6 Sanktionen für nicht genehmigte Handlungen

Für das Verfahren zur Verhängung von Sanktionen wird auf den italienischen Nationalen Tarifvertrag für Arbeitnehmer im Bereich Metall, Maschinen- und Anlagenbau Privatindustrie („CCNL Metalmeccanici e installazione impianti industria privata") verwiesen.

5.3.7 Überprüfung von externen Mitarbeitern

Der Zugang von externen Mitarbeitern ist durch eine spezielle Unternehmensrichtlinie geregelt.

5.3.8 Vom Personal vorzulegende Dokumentation

Der Arbeitnehmer hat bei der Einstellung eine Kopie eines gültigen Ausweisdokuments, eine Kopie der gültigen Krankenversicherungskarte und ein Passfoto für den Zutrittsausweis für den Zugang zu den Räumlichkeiten zu liefern. Er hat danach die Zustimmung zur Verarbeitung der personenbezogenen Daten sowie die Geheimhaltungsvereinbarung auszufüllen und zu unterzeichnen, mit der er sich verpflichtet, keine vertraulichen Informationen und/oder vertraulichen Dokumente preiszugeben. Er hat schließlich den Ethik-Code und die Netiquette von InfoCert zur Kenntnis zu nehmen.

5.4 Verwaltung desÜberwachungsprotokolls

Die mit der Verwaltung der CA und der Gültigkeitsdauer des Zertifikats verbundenen Vorfälle werden gemäß dem Reglement und den technischen Vorschriften in dem Überwachungsprotokoll gesammelt [5].

5.4.1 Arten der gespeicherter Ereignisse

Es werden Ereignisse in Bezug auf Sicherheit, Inbetriebsetzung und Abschaltung, Systemabsturz und Hardwarefehler, Firewall- und Router-Aktivität sowie Zugriffsversuche auf das PKI-System aufgezeichnet.
Alle Daten und Unterlagen werden aufbewahrt, die in der Phase der Identifizierung und Annahme der Beantragung durch den Antragsteller verwendet wurden: Kopie des Personalausweises, Vertragsunterlagen, HR-Auszüge usw.
Es werden die Ereignisse aufgezeichnet, die mit der Registrierung und dem Lebenszyklus der Zertifikate zusammenhängen: Zertifikats- und Erneuerungsanträge, Zertifikatsregistrierung, Generierung, Verbreitung und eventueller Widerruf/eventuelle Suspendierung.
Alle Ereignisse hinsichtlich der Personalisierung der Signatureinheit werden aufgezeichnet.
Alle physischen Zugänge zu den Hochsicherheitsräumen, in denen sich die Maschinen der CA befinden, werden aufgezeichnet.
Alle logischen Zugriffe auf die Anwendungen der CA werden aufgezeichnet.
Jedes Ereignis wird unter Angabe des Systemdatums und der Systemuhrzeit des Ereignisses gespeichert.

5.4.2 Häufigkeit der Bearbeitung und Speicherung des Überwachungsprotokolls

Die Verarbeitung und Zusammenfassung der Daten sowie die Speicherung in dem InfoCert-Aufbewahrungssystem erfolgen monatlich.

5.4.3 Aufbewahrungszeitraum des Überwachungsprotokolls

Die CA bewahrt das Überwachungsprotokoll für 20 Jahre auf.

5.4.4 Schutz des Überwachungsprotokolls

Der Schutz des Überwachungsprotokolls ist durch das InfoCert-Aufbewahrungssystem für elektronische Dokumente sichergestellt, das bei AgID gemäß den geltenden Rechtsvorschriften akkreditiert ist.

5.4.5 Verfahren für das Back-up des Überwachungsprotokolls

Das elektronische Dokumentenaufbewahrungssystem implementiert eine Back-up-Richtlinie und ein Back-up-Verfahren gemäß dem Sicherheitshandbuch des oben genannten Systems.

5.4.6 Speichersystem des Überwachungsprotokoll

Protokollierung der Ereignisse erfolgt über automatische Ad-hoc-Verfahren, gemäß den Verfahrensweisen des InfoCert-Aufbewahrungssystems und ist in dem Sicherheitshandbuch des oben genannten Systems beschrieben.

5.4.7 Benachrichtigung im Fall einer festgestellten Schwachstelle

o. A.

5.4.8 Schwachstellenanalysen

InfoCert führt regelmäßig am System Schwachstellenanalysen (vulnerability assessment) und Penetrationstests (penetration test) durch. Auf der Grundlage der Ergebnisse ergreift InfoCert alle notwendigen Gegenmaßnahmen zur Absicherung der Anwendungen.

5.5 Protokollarchivierung

5.5.1 Art der archivierten Protokolle

Über die wichtigsten Vorfälle werden von einer Certification Authority Protokolle erstellt und archiviert. Die Certification Authority bewahrt die Protokolle für 20 Jahre in dem von InfoCert bereitgestellten Aufbewahrungssystem für Dokumente auf.

5.5.2 Schutz der Protokolle

Der Schutz ist durch das von InfoCert bereitgestellte und bei AgID akkreditierte Aufbewahrungssystem für Dokumente sichergestellt.

5.5.3 Verfahren für das Back-up der Protokolle

Das Aufbewahrungssystem implementiert eine Back-up-Richtlinie und ein Back-up-Verfahren gemäß dem Sicherheitshandbuch des oben genannten Systems.

5.5.4 Anforderungen für die Zeitstempelung der Protokolle

o. A.

5.5.5 Speichersystem für Archive

Die Protokollierung erfolgt über automatische Ad-hoc-Verfahren. Die Speicherung erfolgt gemäß den Verfahrensweisen des InfoCert-Aufbewahrungssystems und ist in dem Sicherheitshandbuch des oben genannten Systems beschrieben.

5.5.6 Verfahren für das Einholen und Überprüfen von Informationen in Archiven

Für die Kontrolle des Status des Zertifizierungssystems und der gesamten technischen Infrastruktur der CA wurden automatische Verfahren und Systeme eingerichtet.

5.6 Wechsel des privaten CA-Schlüssels

Die CA wechselt regelmäßig den privaten Zertifizierungsschlüssel, der für die Signatur von Zertifikaten verwendet wird. Somit kann der Zertifikatsinhaber das sich in seinem Besitz befindliche Zertifikat bis zur Erneuerung nutzen. Jeder Wechsel bedingt eine Änderung dieser Beschreibung und eine Mitteilung an die Aufsichtsbehörde (AgID).

5.7 Kompromittierung des privaten CA-Schlüssels und Disaster Recovery

5.7.1 Verfahren für das Incident Management

Die CA hat die Verfahren für das Incident Management im Rahmen des nach ISO 27000 zertifizierten ISMS beschrieben. Jeder eventuelle Zwischenfall wird sofort nach seiner Entdeckung genauen Prüfungen, der Feststellung der betreffenden Gegenmaßnahmen und der Protokollierung durch den Leiter des Dienstes unterzogen. Das Protokoll wird digital signiert. Eine Kopie wird zusammen mit der Erklärung der Maßnahmen zur Beseitigung der möglichen Ursachen des Störfalls, wenn diese unter die Kontrolle von InfoCert fallen, gemäß Artikel 19 der Verordnung auch an die AgID gesendet.

5.7.2 Beschädigung von Maschinen, Software oder Daten

Bei einem Defekt des sicheren Signaturmoduls HSM, das die Zertifizierungsschlüssel enthält, wird auf das angemessen gesicherte und aufbewahrte Reservepaar des Zertifizierungsschlüssels zurückgegriffen. Es besteht keine Notwendigkeit, das entsprechende CA-Zertifikat zu widerrufen.

Für die Softwares und die Daten werden gemäß den internen Prozessen regelmäßige Back-ups erstellt.

5.7.3 Verfahren bei Kompromittierung des privaten CA-Schlüssels

Die Kompromittierung des Zertifizierungsschlüssels gilt als ein besonders kritischer Vorfall, da sie die mit diesem Schlüssel signierte ausgestellte Zertifikate ungültig macht. Dem Schutz des Zertifizierungsschlüssels und aller Entwicklungs- und Wartungsaktivitäten des Systems, die sich auf den Schlüssel auswirken können, wird daher besondere Aufmerksamkeit geschenkt.
InfoCert hat das zu befolgende Verfahren im Fall von Kompromittierung des Schlüssels im Rahmen des nach ISO 27000 zertifizierten ISMS beschrieben und dies auch der AgID und der CAB mitgeteilt.

5.7.4 Erbringung der CA-Dienste in Katastrophensituationen

InfoCert hat die notwendigen Verfahren umgesetzt, um die Kontinuität des Dienstes auch in kritischen Situation oder Katastrophen sicherzustellen.

5.8 Einstellung des Dienstes der CA oder der RA

InfoCert teilt die Absicht der Einstellung der Zertifizierungstätigkeit der Aufsichtsbehörde (AgID) und der Zertifizierungsstelle (CAB) mindestens 6 Monate vorher unter Angabe des eventuellen Ersatz-Zertifizierungsanbieters, dem Verwahrer des Zertifikatsregisters und der betreffenden Dokumentation mit. InfoCert informiert alle Besitzer der von ihm ausgestellten Zertifikate über die Einstellung der Tätigkeit mit derselben Vorlaufzeit. Wenn kein Ersatz-Zertifizierungsanbieter genannt wird, ist in der Mitteilung deutlich zu erklären, dass alle zum Zeitpunkt der Einstellung der Tätigkeit der CA noch nicht abgelaufenen Zertifikate widerrufen werden.

6 TECHNISCHE SICHERHEITSKONTROLLEN

6.1 Installation und Erzeugung des Schlüsselpaars

Zur Durchführung ihrer Tätigkeit muss die Certification Authority das Schlüsselpaar für die Signatur der Zertifikate der Zertifikatsinhaber erzeugen.

Die Schlüssel werden nur von ausdrücklich dazu beauftragtem Personal erzeugt. Die Schlüsselerzeugung und die Signatur erfolgen gemäß den Vorgaben der geltenden Rechtsvorschriften in den betreffenden und zertifizierten Verschlüsselungsmodulen.

Der Schutz der privaten CA-Schlüssel erfolgt durch das kryptografische Erzeugungs- und Verwendungsmodul dieses Schlüssels. Der private Schlüssel kann nur bei gleichzeitiger Anwesenheit von zwei mit der Erzeugung beauftragten Personen generiert werden. Die Schlüsselerzeugung erfolgt in Gegenwart des Leiters des Dienstes.

Die privaten CA-Schlüssel werden nur für den Zweck ihrer Wiederherstellung nach einer Beschädigung der sicheren Signatureinheit kopiert. Diese Duplikation erfolgt mit einem kontrollierten Verfahren, bei dem der Schlüssel und der Kontext auf mehrere Einheiten gemäß den Sicherheitskriterien der HSM-Einheit verteilt werden.

Das zur Schlüsselerzeugung und Signatur eingesetzte kryptografische Modul besitzt Anforderungen, die Folgendes sicherstellen:

- die Übereinstimmung des Paars mit den Anforderungen der Erzeugungs- und Überprüfungsalgorithmen;
- eine angemessene Erzeugungswahrscheinlichkeit aller möglichen Paare;
- die Identifizierung der Person, die das Erzeugungsverfahren aktiviert;
- die Erzeugung der Signatur erfolgt mithilfe der Einheit, sodass kein Abfangen des Werts des verwendeten privaten Schlüssels möglich ist.

6.1.1 Erzeugung des Schlüsselpaars des Zertifikatsinhabers

Die asymmetrischen Schlüssel werden mithilfe einer sicheren Signaturerstellungseinheit (SSCD oder QSCD) auch in Form eines HSM unter Nutzung der von diesen Einheiten angebotenen Funktionen erzeugt.
Wurde die Einheit nicht von der CA zur Verfügung gestellt, muss der Antragsteller durch Vorlage der betreffenden Dokumentation versichern, dass die Einheit den geltenden Rechtsvorschriften entspricht. Im Fall eines HSM behält sich InfoCert das Recht vor, der Schlüsselgenerierung vorzusitzen.

6.1.2 Übergabe des privaten Schlüssels an den Antragsteller

Der private Schlüssel ist in der kryptografischen Einheit (SSCD oder QSCD) enthalten. Bei den LongTerm- und OneShot-Zertifikaten ist die kryptografische Einheit stets ein HSM. Der Zertifikatsinhaber erhält mit der Übergabe der kryptografischen Einheit den vollen Besitz an dem privaten Schlüssel, den er ausschließlich über die ihm allein bekannte PIN nutzen kann.

Bei Registrierungsverfahren in Anwesenheit des Zertifikatsinhabers wird die Einheit unmittelbar nach der Schlüsselerzeugung übergeben.
Bei Registrierungsverfahren in Abwesenheit des Zertifikatsinhabers wird die Einheit gemäß den im Vertrag geregelten Verfahrensweisen übergeben. Dabei ist immer dafür zu sorgen, dass die Einheit und die Informationen für ihre Nutzung auf verschiedenem Wege oder dem Zertifikatsinhaber in zwei zeitlich unterschiedlichen Momenten übergeben werden. In einigen Fällen können die Einheiten dem Zertifikatsinhaber bereits zur Verfügung stehen, da sie vorab gemäß sicheren Verfahren und nach seiner vorherigen Identifizierung übergeben werden.

6.1.3 Übergabe des öffentlichen Schlüssels an die CA

o. A.

6.1.4 Übergabe des öffentlichen Schlüssels an die Nutzer

Wenn der Antragsteller es verlangt, erfolgt, ausgenommen bei den LongTerm- und OneShot-Zertifikaten, auch eine Veröffentlichung im öffentlichen Register, mit Bereitstellung für den Abruf durch den Benutzer.

6.1.5 Algorithmus und Länge der Schlüssel

Das asymmetrische Schlüsselpaar wird in einer der oben genannten Hardware-Verschlüsselungseinheiten erzeugt. Dabei wird der asymmetrische RSA-Algorithmus mit einer Schlüssellänge von mindestens 4096 Bits verwendet.
Für die Zertifikatsinhaber-Schlüssel wird der asymmetrische RSA-Verschlüsselungsalgorithmus verwendet und die Schlüssellänge beträgt mindestens 2048 Bits.

6.1.6 Qualitätskontrolle und Erzeugung des öffentlichen Schlüssels

Die verwendeten Einheiten sind gemäß hohen Sicherheitsstandards zertifiziert (siehe § 6.2.1) und garantieren, dass der öffentliche Schlüssel korrekt und randomisiert ist. Die CA überprüft vor Ausstellung des Zertifikats, dass der öffentliche Schlüssel nicht bereits verwendet wurde.

6.1.7 Verwendungszweck des Schlüssels

Der Verwendungszweck des privaten Schlüssels wird von der Erweiterung KeyUsage gemäß dem X509-Standard bestimmt. Für die in dieser Beschreibung der Zertifizierungspraxis erläuterten Zertifikate ist nur eine „nicht abstreitbare“ (non-repudiation) Verwendung erlaubt

6.2 Schutz des privaten Schlüssels und ingenieurtechnische Kontrollen des kryptografischen Moduls

6.2.1 Kontrollen und Standard des kryptografischen Moduls

Die von InfoCert verwendeten kryptografischen Module für die Zertifizierungsschlüssel (CA) und für den OCSP-Responder sind nach FIPS 140 Level 3 und Common Criteria (CC) Information Technology

Security Evaluation Assurance Level (EAL) EAL 4 + Type 3 (EAL 4 Augmented by AVA_VLA.4 and AVA_MSU.3) für die Nutzung in Europa validiert.
Die von InfoCert verwendeten Smartcards sind nach Common Criteria (CC) Information Technology Security Evaluation Assurance Level EAL 4+ Type 3 (EAL 4 Augmented by AVA_VLA.4 and AVA_MSU.3) oder EAL5 Augmented by ALC_DVS.2 , AVA_VAN.5 validiert.
Die von InfoCert verwendeten kryptografischen Module für die Fernsignaturschlüssel und automatischen Signaturschlüssel des Zertifikatsinhabers sind nach FIPS 140 Level 3 und Common Criteria (CC) Information Technology Security Evaluation Assurance Level EAL 4 validiert.

6.2.2 Kontrolle des privaten CA-Schlüssels durch mehrere Personen

Der Zugriff auf die Einheiten, in denen die Zertifizierungsschlüssel eingebettet sind, erfolgt nur mit zwei gleichzeitig authentisierte Personen.

6.2.3 Hinterlegung des privaten CA-Schlüssels bei Dritten

o. A.

6.2.4 Back-up des privaten CA-Schlüssels

Das Schlüssel-Back-up liegt in einem Tresor, auf den nur das Personal Zugriff hat, wobei Letzteres keinen Zugriff auf die HSM-Einheiten hat. Eine eventuelle Wiederherstellung verlangt also die Anwesenheit sowohl der zum Personal gehörenden Person, die Zugriff auf die Einheiten hat, als auch der Person, die Zugriff auf den Tresor hat.

6.2.5 Archivierung des privaten CA-Schlüssels

o. A.

6.2.6 Übertragung des privaten Schlüssels von einem Modul oder auf ein kryptografisches Modul

o. A.

6.2.7 Speicherung des privaten Schlüssels auf einem kryptografischen Modul

Der Zertifizierungsschlüssel wird in einem geschützten Bereich der Verschlüsselungseinheit erzeugt und gespeichert, die der Zertifizierungsanbieter verwaltet und den Export verhindert. Zudem wird im Fall eines Aufbrechens des Schutzes das Betriebssystem der Einheit blockiert oder die Einheit unleserlich gemacht.

6.2.8 Methode der Aktivierung des privaten Schlüssels

Der private Zertifizierungsschlüssel wird von der Software der CA nach dem Vier-Augen-Prinzip aktiviert, d. h. zwei Personen mit spezifischen Rollen und in Anwesenheit des Leiters des Dienstes.
Der Zertifikatsinhaber oder der Antragsteller als gesetzlicher Vertreter der juristischen Person ist dafür verantwortlich, den eigenen privaten Schlüssel mit einem starken Passwort vor unzulässiger Verwendung zu schützen. Für die Aktivierung des privaten Schlüssels muss sich der Zertifikatsinhaber authentifizieren.

6.2.9 Deaktivierung des privaten Schlüssels

o. A.

6.2.10 Zerstörung des privaten CA-Schlüssels

Das für diese Aufgabe beauftragte Personal von InfoCert sorgt nach Ablauf oder bei Widerruf des privaten Schlüssels für seine Zerstörung gemäß den Sicherheitsverfahren der Sicherheitsrichtlinien und den Spezifikationen des Herstellers der Einheit.

6.2.11 Klassifizierung der kryptografischen Module

o. A.

6.3 Weitere Aspekte der Schlüsselverwaltung

o. A.

6.3.1 Archivierung des öffentlichen Schlüssels

o. A.

6.3.2 Gültigkeitszeitraum des Zertifikats und des Schlüsselpaars

Der Gültigkeitszeitraum des Zertifikats wird auf Grundlage der folgenden Faktoren bestimmt:

- Stand der Technik;
- aktueller Stand der Kryptologie;
- für das betreffende Zertifikat vorgesehene Nutzung.

Der Gültigkeitszeitraum des Zertifikats ist auf diesem gemäß den unter Abschnitt § 3.3.1genannten Modalitäten genannt.

Das CA-Zertifikat hat derzeit eine Dauer von 16 Jahren. An natürliche oder juristische Personen ausgestellte Zertifikate haben eine Gültigkeitsdauer von höchstens 39 Monaten.

6.4 Aktivierungsdaten des privaten Schlüssels

Es wird auf die Abschnitte 4.2 und 6.3verwiesen.

6.5 IT-Sicherheitskontrollen

6.5.1 Spezifische Sicherheitsanforderungen an die Rechner

Das Betriebssystem der Rechner, die bei den Zertifizierungsaktivitäten für die Schlüssel- und Zertifikatserzeugung sowie für die Verwaltung des Zertifikatsregisters verwendet werden, ist gehärtet (hardening), d. h. es ist so konfiguriert, dass die Auswirkung eventueller Schwachstellen reduziert wird, indem alle Funktionen eliminiert werden, die nicht dem Betrieb und der Verwaltung der CA dienen.

Der Zugriff der Systemadministratoren, die gemäß den geltenden Rechtsvorschriften für diesen Zweck ernannt wurden, erfolgt über eine Root-Anwendung auf Abfrage, die die Nutzung der Root-

Rechte nur nach individueller Authentifizierung erlaubt. Die Zugriffe werden getrackt und protokolliert und für 12 Monate gespeichert.

6.6 Funktionsweise der Kontrollsysteme

Für InfoCert hat die sichere Verarbeitung der Informationen strategische Bedeutung und es ist sich der Notwendigkeit bewusst, ein Managementsystem für die Informationssicherheit (ISMS) gemäß der Norm ISO/IEC 27001 zu entwickeln, zu unterhalten, zu kontrollieren und ständig zu verbessern. InfoCert ist seit März 2011 für die Tätigkeiten der Bereiche EA:33-35 nach ISO/IEC 27001:2005 zertifiziert. Im März 2015 wurde es für die neue Version der Norm ISO/IEC 27001:2013 zertifiziert.
In dem ISMS sind Verfahren und Kontrollen für folgende Themenbereiche vorgesehen:

- Asset-Management;
- Zugriffskontrolle;
- physische und Umweltsicherheit;
- Sicherheit der operativen Tätigkeiten;
- Kommunikationssicherheit;
- Erwerb, Entwicklung und Instandhaltung der Systeme;
- Incident Management;
- operative Kontinuität.

Alle Verfahren werden von den jeweiligen Verantwortlichen genehmigt und intern im System des Dokumentenmanagements von InfoCert ausgetauscht.

6.7 Netzwerksicherheitskontrollen

InfoCert hat für den Zertifizierungsdienst eine Netzsicherheitsinfrastruktur entwickelt, die auf den Einsatz von Firewall-Lösungen und des SSL-Protokolls beruht, um einen sicheren Kanal zwischen den Registrierungsstellen und dem Zertifizierungssystem sowie zwischen Letzterem und den Administratoren/Akteuren zu schaffen.

Die Systeme und Netzwerke von InfoCert sind durch Firewall-Lösungen kontrolliert mit dem Internet verbunden, sodass die Verbindung in Bereiche mit progressiv höherer Sicherheit unterteilt werden kann: Internet, DMZ (Demilitarized Zone) bzw. externe Netzwerke, interne Netzwerke. Der gesamte Verkehr zwischen den verschiedenen Bereichen ist einer Akzeptanz auf Basis von festgelegten Regeln unterworfen. Die über die Firewalls definierten Regeln werden auf Basis der Grundsätze „Default Deny“ (wenn es nicht ausdrücklich erlaubt ist, ist es standardmäßig verboten, d. h. die Regeln erlauben den Verkehr nur, wenn es zur korrekten Funktion der Anwendung unbedingt erforderlich ist) und „Defense-in-Depth“ (progressive Verteidigungsebenen, zuerst über nacheinander folgende Firewall-Barrieren auf Netzebene und dann das Härten auf Systemebene).

6.8 Zeitstempelsystem

InfoCert stellt einen qualifizierten Zeitstempeldienst zur Verfügung. Für die Zeitmarkierung wird auf die Beschreibung der Zertifizierungspraxis ICERT-INDI-TSA verwiesen, die auf der Website des Vertrauensdiensteanbieters InfoCert zu finden ist.

7 FORMAT DES ZERTIFIKATS, DER CRL UND DES OCSP

7.1 Format des Zertifikats

In dem Zertifikat sind die in dem Zertifikatsantrag angegebenen Informationen angeführt.
Das erzeugte Zertifikatsformat entspricht der eIDAS-Verordnung und der Entscheidung 121/2019 [9]. So wird die volle Lesbarkeit und Überprüfbarkeit im Kontext der Rechtsvorschriften und der europäischen Zertifizierungsanbieter gewährleistet.
InfoCert verwendet für die gesamte PKI-Struktur den Standard ITU X.509, Version 3.
In Anhang A die Struktur der Root-Zertifikate und der Zertifikate der Zertifikatsinhaber, unabhängig davon, ob diese natürliche oder juristische Personen sind.

7.1.1 Versionsnummer

Alle von InfoCert ausgestellten Zertifikate sind im Format X.509, Version 3.

7.1.2 Zertifikatserweiterungen

Die qualifizierten Zertifikate sind durch die Erweiterungen in den QCStatement clause 3.2.6 des IETF RFC 3739 gekennzeichnet. Ihre Nutzung ist durch die Norm ETSI 319 412-5 geregelt.
Für die des Zertifikats Erweiterungen siehe Anhang A.

7.1.3 OID des Signaturalgorithmus

Die Zertifikate sind mit folgendem Algorithmus signiert:
sha256WithRSAEncryption [iso(1) member-body(2) us(840) rsadsi(113549) pkcs(1) pkcs-1(1) 11].

7.1.4 Namensformen

Jedes Zertifikat enthält von der ausstellenden CA eine eindeutige Seriennummer.

7.1.5 Namensbindungen

Siehe hierzu Abschnitt 3.1.

7.1.6 OID des Zertifikats

Siehe hierzu Abschnitt 1.2.

7.2 CRL-Format

Zur Bildung der CRL-Sperrlisten verwendet InfoCert das Profil RFC5280 „Internet X.509 Public Key Infrastructure Certificate Revocation List (CRL)“ und ergänzt das Basisformat um die Erweiterungen

gemäß der RFC 5280-Definitonen: „Authority Key Identifier“, „CRL Number“, „Issuing Distribution Point“ und „expiredCertsOnCRL“.

7.2.1 Versionsnummer

Alle von InfoCert ausgestellten Zertifikate sind im Format X.509, Version 2.

7.2.2 CRL-Erweiterungen

Für die CRL-Erweiterungen siehe Anhang A.

7.3 OCSP-Format

Um ohne Abfrage der CRL den Widerrufsstatus des Zertifikats bestimmen zu können, stellt InfoCert OCSP-Dienste entsprechend dem RFC6960-Profil „X.509 Internet Public Key Infrastructure Online Certificate Status Protocol – OCSP“ bereit. Dieses Protokoll nennt genau die Daten, die von einer Anwendung ausgetauscht werden müssen, die den Zertifikatsstatus und den OCSP-Dienst überprüfen will.

7.3.1 Versionsnummer

Das von InfoCert verwendete OCSP-Protokoll entspricht der Version 1 des RFC6960.

7.3.2 OCSP-Erweiterungen

Für die OCSP-Erweiterungen siehe Anhang A.

8 KONFORMITÄTSKONTROLLEN UND -BEWERTUNGEN

Um die Qualifikation als qualifizierter und nicht qualifizierter Vertrauensdiensteanbieter zu erhalten, ist es gemäß der eIDAS-Verordnung notwendig, das von Artikel 21 der Verordnung vorgesehene Verfahren zu durchlaufen.
InfoCert hat bei der AgID den betreffenden Antrag zur Anerkennung als „qualifizierter Vertrauensdienst“ zusammen mit einem Bewertungsbericht über die Konformität mit der Verordnung (Conformity Assessment Report - CAR) eingereicht, der von einer von dem übergeordneten nationalen Organ (CAB) – in Italien ACCREDIA – autorisierten Bewertungsstelle abgefasst wurde.
InfoCert erbringt den Dienst als qualifizierter Vertrauensdiensteanbieter im Sinne der Verordnung (EU) Nr. 910/2014 vom 23.07.2014 auf der Grundlage einer Konformitätsbewertung, die die Conformity Assessment Body CSQA Certificazioni S.r.l. im Sinne der oben genannten Verordnung und der Norm ETSI EN 319 401 durchgeführt hat. Diese Bewertung erfolgte nach dem von ACCREDIA aufgrund der Normen ETSI EN 319_403 und UNI CEI EN ISO/IEC 17065:2012 definierten eIDAS-Bewertungsschema.

8.1 Häufigkeit oder Grund der Konformitätsbewertung

Die Konformitätsbewertung wird alle zwei Jahre wiederholt. Die CAB führt jedoch jedes Jahr eine Aufsichtsaudit durch.

8.2 Identität und Qualifikationen der Bewerter

Die Kontrolle wird von folgendem Unternehmen durchgeführt:

Firma	**CSQA Certification S.r.l.**
Sitz	Via S. Gaetano n. 74, 36016 Thiene (VI)
Telefon	+39 0445 313011
HR-Nummer	Steuernummer 02603680246 Handelsregister Vicenza Nr. 02603680246 / Verzeichnis der Wirtschafts- und Verwaltungsdaten (REA) Nr. 258305
USt-Nr.	02603680246
Website	http://www.csqa.it

8.3 Beziehungen zwischen InfoCert und der CAB

InfoCert und CSQA unterhalten weder finanzielle Beteiligungen noch geschäftliche Beziehungen.
Es bestehen keine Geschäftsbeziehungen oder Partnerschaften, die die objektive Bewertung der CSQA zugunsten oder gegen InfoCert beeinträchtigen könnten.

8.4 Bewertete Aspekte

Die CAB bewertet die Konformität in Bezug auf die Beschreibung der Zertifizierungspraxis, die Verordnung und die für die angewandten Verfahren geltenden Rechtsvorschriften, die Organisation der CA, die Organisation der Aufgaben, die Schulung des Personals, die Vertragsdokumentation.

8.5 Vorgehen im Fall von Nichtkonformität

Die CAB entscheidet im Falle von Nichtkonformität, ob sie den Bericht an die AgID sendet oder ob sie sich vorbehält, das Audit nach Behebung der Konformitätsmängel erneut durchzuführen.
InfoCert verpflichtet sich, sämtliche Nichtkonformität umgehend unter Durchführung aller notwendigen Verbesserungs- und Anpassungsmaßnahmen zu beseitigen.

9 WEITERE RECHTLICHE UND GESCHÄFTLICHE ASPEKTE

9.1 Gebühren

9.1.1 Gebühren für die Ausstellung und die Erneuerung der Zertifikate

Bei LongTerm- und OneShot-Zertifikaten werden die Kosten für die Ausstellung des Zertifikats i. d. R. vom Antragsteller und nicht vom Zertifikatsinhaber auf Grundlage der im Dienstleistungsvertrag zwischen dem Antragsteller und InfoCert angeführten Gebühren getragen. Der Vertrag mit dem Zertifikatsinhaber kann dennoch auch für die Regelung der Beziehungen zum Zertifikatsinhaber spezifische Gebühren vorsehen.

In den anderen Fällen sind die Gebühren auf den Websites https://www.firma.infocert.it/ und http://ecommerce.infocert.it oder bei den RA angegeben. Die CA kann mit den RA und/oder den Antragstellern Geschäftsvereinbarungen mit spezifischen Gebühren vereinbaren.

9.1.2 Gebühren für den Zugriff auf Zertifikate

Der Zugriff auf das öffentliche Register der veröffentlichten Zertifikate ist frei und kostenlos.

9.1.3 Gebühren für den Zugriff auf Informationen über den Suspendierungs- und Widerrufsstatus der Zertifikate

Der Zugriff auf die Sperrliste ist frei und kostenlos.

9.1.4 Gebühren für weitere Dienste

Die Gebühren sind auf den Websites https://www.firma.infocert.it/ und http://ecommerce.infocert.it oder bei den RA angegeben.

Die CA kann mit den RA und/oder den Antragstellern Geschäftsvereinbarungen mit spezifischen Gebühren vereinbaren.

9.1.5 Erstattungsrichtlinien

Wird der Dienst von einem Verbraucher erworben, kann der Zertifikatsinhaber den Vertrag innerhalb einer Frist von 14 Tagen ab dem Datum des Vertragsabschlusses kündigen und den gezahlten Preis zurückerhalten. Die Anweisungen für die Ausübung des Kündigungsrechts und des Erstattungsantrags stehen auf der Website https://help.infocert.it/ oder bei den RAs zur Verfügung.

9.2 Finanzielle Haftung

9.2.1 Versicherungsdeckung

Der Vertrauensdiensteanbieter InfoCert hat über die Risiken der Geschäftstätigkeit und über die von Dritten verursachten Schäden einen Versicherungsvertrag abgeschlossen, dessen Text von der AgID verhandelt und akzeptiert wurde und der folgende Versicherungssummen festlegt:

- 10.000.000 Euro pro Versicherungsfall;
- 10.000.000 Euro pro Jahr.

9.2.2 Sonstige Tätigkeiten

o. A.

9.2.3 Garantie oder Versicherungsdeckung für die Endnutzer des Zertifikats

Siehe hierzu Abschnitt 9.2.1.

9.3 Vertraulichkeit der Geschäftsinformationen

9.3.1 Anwendungsbereich der vertraulichen Informationen

Im Bereich der Tätigkeit, die Gegenstand dieser Beschreibung ist, ist keine Verwaltung vertraulicher Informationen vorgesehen.

9.3.2 Nicht unter den Anwendungsbereich der vertraulichen Informationen fallende Informationen

o. A.

9.3.3 Verantwortung für den Schutz der vertraulichen Informationen

o. A.

9.4 Datenschutz

Die von der CA bei der Ausübung ihrer typischen Tätigkeiten behandelten Informationen über den Zertifikatsinhaber und den Antragsteller, gelten vorbehaltlich einer ausdrücklichen Zustimmung als vertraulich und dürfen nicht veröffentlicht werden. Davon ausgenommen sind die Informationen, die ausdrücklich für die öffentliche Verwendung [öffentlicher Schlüssel, Zertifikat (sofern vom Zertifikatsinhaber verlangt), Widerrufs- und Suspendierungsdaten des Zertifikats] bestimmt sind. InfoCert verarbeitet die personenbezogenen Daten insbesondere gemäß den Bestimmungen des ital. Gesetzesvertretenden Dekrets Nr. 196 vom 30. Juni 2003, und der Verordnung (EU) Nr. 2016/679 des Europäischen Parlaments und des Rates vom 27. April 2016 zum Schutz natürlicher Personen bei der Verarbeitung personenbezogener Daten, zum freien Datenverkehr, die seit 25.

Mai 2018 voll verbindlich ist [4].

9.4.1 Datenschutzprogramm

InfoCert wendet Richtlinien an, mit denen es den Schutz personenbezogener Daten in sein nach ISO 27001 zertifiziertes Managementsystem für die Informationssicherheit als Ergänzung aufnimmt, wobei es mit diesem System das Verfahren der kontinuierlichen Optimierung teilt.

9.4.2 Als personenbezogene Daten verarbeitete Daten

Als personenbezogene Daten werden die Daten verarbeitet, die gemäß den geltenden Rechtsvorschriften unter die entsprechende Definition fallen [4]. Als personenbezogene Daten gelten also alle Informationen, die sich auf eine identifizierte oder identifizierbare natürliche Person beziehen, auch durch Verweis auf andere Informationen, wie zum Beispiel eine persönliche Identifikationsnummer.

9.4.3 Nicht als personenbezogene Daten geltende Informationen

Die Daten, die von der technischen Verwaltung der CA veröffentlicht werden, d. h. öffentliche Schlüssel, Zertifikate (sofern vom Zertifikatsinhaber verlangt), Widerrufs- und Suspendierungsdaten des Zertifikats, gelten nicht als personenbezogene Daten.

9.4.4 Verantwortlicher der Verarbeitung personenbezogener Daten

InfoCert S.p.A.
Betriebsstätte
Via Marco e Marcelliano 45
00147 Roma
richieste.privacy@legalmail.it

9.4.5 Datenschutzerklärung und Zustimmung zur Verarbeitung von personenbezogenen Daten

Die Datenschutzerklärung seht auf der Website www.infocert.itzur Verfügung. Spezifische Erklärungen finden sich möglicherweise auf der Website des Antragstellers, der die Zustimmung zur Verarbeitung im Auftrag von InfoCert einholt. Vor Durchführung jeder Verarbeitung personenbezogener Daten holt InfoCert gemäß Gesetz [4] die Zustimmung zur Verarbeitung ein.

9.4.6 Offenlegung der Daten aufgrund behördlicher Anfragen

Die Daten müssen auf Anfrage von Behörden offengelegt werden. Dies erfolgt gemäß den von der Behörde von Fall zu Fall vorgegebenen Verfahren.

9.4.7 Weitere Offenlegungsgründe

Nicht vorgesehen.

9.5 Geistiges Eigentum

InfoCert S.p.A. besitzt das Urheberrecht an diesem Dokument. Alle Rechte vorbehalten.

9.6 Vertretung und Garantien

InfoCert trägt die Verantwortung für die Einhaltung der Verfahren gemäß der eigenen Richtlinie über den Schutz der Informationen. Dies gilt auch, wenn einige Funktionen im Sinne von Art. 2.4.1. des Anhangs zur Durchführungsverordnung (EU) 2015/1502 der Kommission an eine andere Person delegiert werden.
In letzterem Fall erfolgt die Vertretung durch einen Auftrag, den InfoCert an die Registrierungsstelle (RA) erteilt und in dem die Verantwortlichkeiten und die Pflichten der Parteien definiert werden. Die Registrierungsstelle verpflichtet sich insbesondere, die Registrierungstätigkeit unter Einhaltung der geltenden Rechtsvorschriften und der in der Beschreibung der Zertifizierungspraxis aufgeführten Verfahren, mit besonderem Bezug auf die sichere Identifizierung der Personen durchzuführen, die den Antrag auf eine digitale Zertifizierung unterzeichnen. Sie hat InfoCert die Ergebnisse dieser Tätigkeiten zu übermitteln.
Der Inhaber ist für die Richtigkeit der in dem Registrierungs- und Zertifizierungsantrag mitgeteilten Daten verantwortlich. Wenn er bei der Identifizierung, auch durch Verwendung falscher Ausweisdokumente, seine wahre Identität verheimlicht oder sich als jemand anderer ausgegeben hat, oder wenn er in einer Art und Weise gehandelt hat, die das Identifizierungsverfahren und die betreffenden Angaben in dem Zertifikat beeinträchtigen, haftet er für alle Schäden, die dem Zertifizierungsanbieter und/oder Dritten aus der Unrichtigkeit der im Zertifikat enthaltenden Informationen entstehen, mit der Pflicht, den Zertifizierungsanbieter gegenüber eventuellen Schadenersatzansprüchen klaglos und schadlos zu halten.
Der Inhaber und der Antragsteller haften ebenso für Schäden, die dem Zertifizierungsanbieter und/oder Dritten in dem Fall entstehen, dass sie die Aktivierung der im Punkt 4.9. dieser Beschreibung geregelten Verfahren (Widerruf und Suspendierung des Zertifikats) verspäten.

9.7 Garantiebeschränkungen

Der Zertifizierungsanbieter leistet keine Garantie (i) für die ordnungsgemäße Funktionsweise und Sicherheit der vom Inhaber verwendeten Hardware oder Software; (ii) für die von den geltenden Rechtsvorschriften und den Angaben in dieser Beschreibung der Zertifizierungspraxis abweichende Verwendung des privaten Schlüssels, der sicheren Signatureinheit – soweit vorhanden – und/oder des Signaturzertifikats; (iii) für die regelmäßige und kontinuierliche Funktionstüchtigkeit der nationalen und/oder internationalen Strom- und Telefonleitungen; (iv) für die Gültigkeit und Bedeutung, auch im Sinne der Beweiserheblichkeit, des Signaturzertifikats oder den diesem zugrunde liegenden oder über die Schlüssel dieses Zertifikats erzeugten Nachrichten, Schriftstücken oder Dokumenten, unbeschadet der Wirksamkeit handschriftlicher Unterschriften, die gemäß Art. 25 der Verordnung (EU) Nr. 910/2014 als qualifizierte elektronische Signatur anerkannt sind; (v) für die Geheimhaltung und/oder Vollständigkeit der dem Signaturzertifikat zugrunde liegenden oder über die Schlüssel dieses Zertifikats erzeugten Nachrichten, Schriftstücke oder Dokumente (in dem Sinne, dass eventuelle Verletzungen des Zertifikats i. d. R. vom Verantwortlichen oder Empfänger über das betreffende Überprüfungsverfahren festgestellt werden können).

Der Zertifizierungsanbieter garantiert nur die Funktionsweise des Dienstes auf den in Abschnitt 9.17 der Beschreibung der Zertifizierungspraxis genannten Ebenen.

9.8 Haftungsbeschränkungen

Der Zertifizierungsanbieter übernimmt keine Überwachungspflichten in Bezug auf den Inhalt, die Typologie oder das elektronische Format der Dokumente und/oder der eventuellen Hashwerte, die von dem vom Antragsteller oder Inhaber angegebenen IT-Verfahren übermittelt werden und für die er keine Haftung in Bezug auf deren Gültigkeit und Rückverfolgbarkeit auf den tatsächlichen Willen des Inhabers übernimmt.
Der Zertifizierungsanbieter übernimmt mit Ausnahme von Fällen schuldhaften Handelns keine Haftung für unmittelbare und mittelbare Schäden, die die Inhaber und/oder Dritte aufgrund der Nutzung oder der Nichtnutzung der auf der Basis der Vorgaben in dieser Beschreibung und der Allgemeinen Bedingungen der Zertifizierungsdienste ausgestellten Signaturzertifikate erleiden.
InfoCert haftet nicht für unmittelbare und mittelbare Schäden, die ,auch alternativ, (i) durch den Verlust, (ii) durch unsachgemäße Aufbewahrung, (iii) durch unsachgemäße Verwendung der Identifizierungs- und Authentifizierungsmittel und/oder (iv) aus der Nichteinhaltung des Vorbenannten durch den Inhaber verursacht werden.
Der Zertifizierungsanbieter haftet zudem ab der Abschlussphase des Vertrages über die Zertifizierungsdienste und auch während seiner Durchführung nicht für eventuelle Schäden und/oder Verzögerungen aufgrund einer Störung oder eines Stillstands des IT-Systems und des Internets.
InfoCert werden, außer im Fall vorsätzlichen oder fahrlässigen Handelns, mit keinen Kosten oder Haftungen für unmittelbare oder mittelbare Schäden irgendeiner Art und irgendeinen Umfangs belastet, die dem Inhaber, dem Antragsteller und/oder Dritten aufgrund von Eingriffen oder Maßnahmen durch Dritte am Dienst oder an den Geräten entstehen, die InfoCert nicht autorisiert hat.

9.9 Entschädigungen

InfoCert haftet für die eventuellen Schäden, die natürlichen oder juristischen Personen vorsätzlich oder fahrlässig aufgrund einer Nichterfüllung der Pflichten nach der Verordnung (EU) Nr. 910/2014 des Europäischen Parlaments und des Rates vom 23. Juli 2014 und aufgrund des fehlenden Ergreifens aller angemessenen Maßnahmen zur Vermeidung dieses Schadens seitens InfoCert direkt verursacht werden.

In dem im vorstehenden Abschnitt genannten Fall haben der Antragsteller und der Inhaber einen Anspruch auf Ersatz der aufgrund des Verhaltens im Sinne des vorstehenden Abschnitts verursachten direkten Schäden in Höhe eines Betrages, der in keinem Fall den vorgesehenen Höchstwert für jedes Ereignis und für jedes Jahr laut Art. 3 Absatz 7 des der Entscheidung 185/2017 beigefügten Reglements überschreiten darf .

Die Erstattung kann nicht verlangt werden, wenn die fehlende Inanspruchnahme der unsachgemäßen Nutzung des Zertifizierungsdienstes zuzuschreiben ist oder vom Verwalter des Telekommunikationsnetzes zu vertreten ist oder durch ein unvorhersehbares Ereignis, höhere Gewalt oder durch Gründe, die InfoCert nicht zu vertreten hat, wie zum Beispiel Streiks, Aufruhre,

Erdbeben, Terroranschläge, Volksaufstände, organisierte Sabotagen, chemische und/oder bakteriologische Zwischenfälle, Krieg, Überschwemmungen, Maßnahmen der zuständigen Behörden oder Unzulänglichkeit der vom Antragsteller verwendeten Einrichtungen, Hardwares und/oder Softwares verursacht werden.

9.10 Vertragsende und Vertragsbeendigung

9.10.1 Vertragsende

Das Zertifikat wird bei Beendigung der Beziehung zwischen CA und dem Zertifikatsinhaber, zwischen CA und RA, zwischen CA und Antragsteller widerrufen. Der Zertifizierungsvertrag zwischen dem Zertifizierungsanbieter und dem Zertifikatsinhaber hat dieselbe Gültigkeitsdauer wie das Signaturzertifikat, die in dem Feld „Gültigkeit“ (*validity*) angegeben ist.
Der Inhaber kann vor dem Ablauf die Erneuerung des Zertifikats gemäß den in dieser Beschreibung der Zertifizierungspraxis genannten Verfahren beantragen. Die Erneuerung bewirkt die Verlängerung desZertifizierungsvertrages bis zum Ablauf oder Widerruf des erneuerten Zertifikats und die Zahlung der für diesen Dienst vereinbarten Vergütungen. Ein abgelaufenes oder widerrufenes Zertifikat kann nicht verlängert werden.

9.10.2 Vertragsbeendigung

Die Wirksamkeit des Vertrages hängt vom positiven Ergebnis der Identitätsprüfung des Inhabers ab. Der Zertifizierungsanbieter stellt das Zertifikat im Fall eines negativen Ergebnisses der Identitätsprüfung nicht aus bzw. ab dem Zeitpunkt seiner Ausstellung gilt es als unwirksam und der Vertrag ist von Rechts wegen aufgelöst.
Der Vertrag wird von Rechts wegen mit gleichzeitiger Unterbrechung des Dienstes und gleichzeitigem Widerruf des ausgestellten Zertifikats aufgelöst, falls der Inhaber und/oder der Antragsteller die in den Vertragsklauseln laut Art. 3 (Haftung des Inhabers und des Antragstellers), Art. 4.6 (Geistiges Eigentum), Art. 8 (Pflichten des Inhabers), Art. 11 (Vergütungen), Art. 12.3 (über die Pflicht zur Benachrichtigung über die Fälle und Gründe einer Suspendierung und eines Widerrufs des Zertifikats), sArt. 45 (Weitere Pflichten des Inhabers und des Antragstellers), sofern anwendbar, Art. 47 (Weitere Pflichten des Inhabers) sofern anwendbar, sowie die in dieser Beschreibung der Zertifizierungspraxis geregelten Vorgaben nicht erfüllt. Der Vertrag wird von Rechts wegen aufgelöst, wenn die betroffene Partei der anderen Partei per zertifizierte E-Mail (PEC) oder per Einschreiben mit Rückschein erklärt, sich dieser Klausel bedienen zu wollen.
Handelt es sich bei dem Inhaber um einen Verbraucher, ist für zivilrechtliche Streitigkeiten im Zusammenhang mit dem vom Verbraucher abgeschlossenen Vertrag unabdingbar das Gericht des Wohnsitzes oder des gewöhnlichen Aufenthaltsortes des Verbrauchers zuständig.
Der Verbraucher kann nach freiem Ermessen außergerichtliche Streitbeilegungsverfahren gemäß italienischem Verbraucherschutzkodex (Codice del Consumo) und anderen einschlägigen Rechtsvorschriften in Anspruch nehmen.
Darüber hinaus wird gemäß der Verordnung (EU) Nr. 524/2013 darauf hingewiesen, dass für die Beilegung von Streitigkeiten über Online-Verträge und angebotene Online-Dienste die Möglichkeit besteht, die von der Europäischen Kommission vorgesehene Online Dispute Resolution (ODR, Online-Streitbeilegung) in Anspruch zu nehmen, die auf diesem Link zu finden ist: . https://webgate.ec.europa.eu/odr/ .

Der Zertifizierungsanbieter kann den Vertrag für die Zertifizierungsdienste jederzeit mit einer Frist von 30 Tagen beenden und folglich das Zertifikat widerrufen.
In allen Fällen, in denen der Inhaber oder der Antragsteller die übernommenen Pflichten nicht erfüllt, kann der Zertifikatsanbieter die Erbringung des Dienstes, auch durch Suspendierung des Zertifikats, einstellen. InfoCert hat insbesondere bei Nichtzahlung der Vergütung des Dienstes das Recht, den Vertrag mit dem Antragsteller und dem Inhaber jederzeit fristlos und ohne jegliche Verpflichtung aufzulösen und folglich sämtliche ausgestellte Zertifikate zu widerrufen.
Die Vergütung ist bei Vertragsbeendigung durch den Inhaber oder bei Widerruf des Zertifikats dennoch geschuldet und, wurde sie bereits bezahlt, behält InfoCert sie auch als Gegenleistung für die Vertragsbeendigung ein.
In sämtlichen Fällen der Vertragsbeendigung, Beendigung der Gültigkeit des Vertrages und seiner Auflösung bleiben die von dem Vertrag bis zu diesem Moment erzeugten Wirkungen unberührt.
Der Inhaber nimmt zur Kenntnis, dass der Dienst im Fall einer Vertragsbeendigung, unabhängig vom Beendigungsgrund, nicht mehr genutzt werden kann.

9.10.3 Wirkungen der Vertragsbeendigung

Die Vertragsbeendigung bedingt den sofortigen Widerruf des Zertifikats.

9.11 Offizielle Kommunikationskanäle

Es wird auf die in Abschnitt 1.5.1genannten Kanäle verwiesen.

9.12 Überarbeitung der Beschreibung der Zertifizierungspraxis

Die CA behält sich vor, dieses Dokument aufgrund technischer Anforderungen oder aufgrund von Verfahrensänderungen, die sowohl infolge gesetzlicher Vorschriften oder Regelungen als auch zur Optimierung des Arbeitszyklus eingetreten sind, abzuändern. Jede neue Version der Beschreibung der Zertifizierungspraxis hebt die vorherigen Versionen auf und ersetzt sie. Diese bleiben dennoch für die während ihrer Gültigkeit ausgestellten Zertifikate und bis zu deren ersten Ablauf gültig.

Bei Änderungen, die keine erhebliche Auswirkung auf die Benutzer haben, wird die Release-Nummer des Dokuments erhöht, während sich bei Änderungen mit einer erheblichen Auswirkung auf die Benutzer (wie zum Beispiel Änderungen der operativen Verfahren) die Versionsnummer des Dokuments erhöht. Die Beschreibung wird auf jeden Fall umgehend veröffentlicht und gemäß den vorgesehenen Verfahrensweisen verfügbar gemacht. Jede technische oder verfahrensbezogene Änderung dieser Beschreibung des Zertifizierungsprozesses wird ohne jede Verzögerung den RA mitgeteilt.
Bei wesentlichen Änderungen muss sich die CA einer Prüfung durch eine akkreditierte CAB unterziehen, den Konformitätsbewertungsbericht (*CAR – Conformity Assessment Report*) und die Beschreibung der Zertifizierungspraxis der Aufsichtsbehörde (AgID) vorlegen und die Erlaubnis für die Veröffentlichung abwarten.

9.12.1 Überarbeitungsverlauf

Version/Release Nr.:	**4.4**
Datum Version/Release:	10.02.2021
Beschreibung der Änderungen:	§ 4.2.1 Aktualisierung hinsichtlich der Verpflichtung und Eindeutigkeit von E-Mail-Adresse und Mobiltelefonnummer $ 4.2.2 Elektronisches Übergabeverfahren des verschlüsselten Umschlags als vorgegebene Verfahrensweise § 4.9.13 Ergänzung der Möglichkeit einer Suspendierung aus Sicherheitsgründen nach Ermessen der CA
Gründe:	AgID-Antrag

Version/Release Nr.:	**4.3**
Datum Version/Release:	15.06.2020
Beschreibung der Änderungen:	§ 3.2.3 Aktualisierung der Liste der Identitätsprüfungsverfahren § 3.2.3.4 Identitätsprüfung nach dem Interoperabilitätsrahmen des eIDAS-Knotens § 3.2.3.5 Unterscheidung zwischen Video mit Assistenz und ohne Assistenz mit Überweisung als Verstärkung § 3.2.3.6 eDocID - Identitätsprüfung mittels elektronischer Ausweisdokumente § 4.5.3 Aktualisierung des Abschnitts zur Einführung der Nutzungsbeschränkungen für autID und eDocID- Identitätsprüfungen § 4.9.15 und 4.9.16 Klarstellungen bezüglich der Dauer der Suspendierung
Gründe:	Erweiterung der Identitätsprüfungsverfahren Klarstellungen und Tippfehler

Version/Release Nr.:	**4.2**
Datum Version/Release:	24.03.2020
Beschreibung der Änderungen:	§ 5.1.1 Technologische Aktualisierung und Verweise auf die in die AWS-Cloud ausgelagerten Dienste § 5.1.6 Technologische Aktualisierung hinsichtlich der Speichermedien § Anhang A – Einführung der neuen Root CA Electronic Signature Qualified Root „InfoCert Qualified Electronic Signature CA 4“
Gründe:	Neue Root CA

Version/Release Nr.:	**4.1**

Datum Version/Release:	10.10.2019
Beschreibung der Änderungen:	§ 3.1.5 Ergänzung der Möglichkeit, als eindeutige Identifikationsnummer die lt. Dokument eIDAS eID Profile von EiDAS Cooperation Network vorgesehenen Mittel zu verwenden
Gründe:	-

Version/Release Nr.:	**4.0** (nie veröffentlichte Version, Aktualisierungen in Version 4.1 aufgenommen)
Datum Version/Release:	14.06.2019
Beschreibung der Änderungen:	Formale Korrekturen, Aktualisierung der Definitionen, Akronyme und Bezüge $ 1.2 Aktualisierung der Dokumentenversion, Beschreibung des OID agIDcert § 1.3.5 Aktualisierung hinsichtlich minderjähriger Person $ 1.6.1 Einführung Definitionen von OneShot-, und LongTerm-Zertifikaten und Domain § 2.2.3 Aktualisierung der CRL Distribution Points § 3.1.1 Aktualisierung hinsichtlich der Entscheidung AgID 121/2019 § 3.1.5 Aktualisierung hinsichtlich der Entscheidung AgID 121/2019 § 3.2.6 Verständlichere Beschreibung § 4.3.1.5 Beschreibung der für Testzwecke ausgestellten Zertifikate § 4.5.3 Ergänzung der Nutzungsbeschränkung für die Ausstellung mit SPID und aktualisierte Beschreibung der Wertgrenze § 4.9.2 Verständlichere Beschreibung § 5.1.1 Klärung bezüglich des Standorts des Rechenzentrums § 5.3.7 Ausgearbeitete Beschreibung der physischen Zugänge § 5.4.1 Ergänzung der Protokollierung der physischen Zugänge und der logischen Zugriffe Zusammenlegung folgender Abschnitte der beiden Beschreibungen: • $ 2.2.2 Veröffentlichung von Zertifikaten • $ 3.1.3 Anonymität und Pseudonymität der Antragsteller • $ 3.2.3.4 Identitätsprüfung nach dem Verfahren 4 – AUTID • $ 4.1.1 Wer kann ein Zertifikat beantragen? • $ 4.3.2 Benachrichtigung der Antragsteller über die erfolgte Ausstellung des Zertifikats • $ 4.4.2 Veröffentlichung des Zertifikats durch die Certification Authority • $ 4.5.1 Verwendung des privaten Schlüssels und des Zertifikats durch den Zertifikatsinhaber • $ 4.6.1 Gründe für die Erneuerung • $ 4.9.3 Verfahren für die Beantragung des Widerrufs • $ 4.9.15 Verfahren für die Beantragung der Suspendierung • $ 6.1.1 Erzeugung des Schlüsselpaars des Zertifikatsinhabers

	• $ 6.1.2 Übergabe des privaten Schlüssels an den Antragsteller • $ 6.1.4 Übergabe des öffentlichen Schlüssels an die Nutzer • $ 6.2.7 Speicherung des privaten Schlüssels auf einem kryptografischen Modul • $ 9.1.1 Gebühren für die Ausstellung und die Erneuerung der Zertifikate • $ 9.4.5 Datenschutzerklärung und Zustimmung zur Verarbeitung von personenbezogenen Daten • § 9.10.2 Vertragsauflösung
Gründe:	Fusion von ICERT-INDI-MO, Version 3.5 vom 30.11.2018 und ICERT-INDI-MO-ENT, Version 3.5 vom 30.11.2018. Aktualisierung auf die Entscheidung AgID 121/2019. Klarstellungen.

Version/Release Nr.:	**3.5**
Datum Version/Release:	30.11.2018
Beschreibung der Änderungen:	§ 1.2 Aktualisierung des OID und Beschreibung § 1.3 Aktualisierung der Firmenbezeichnung der Gruppe § 3.2.6 Identifizierung der juristischen Person PSP in Sachen PSD2 § 4.2.1.2 Informationen zur juristischen Person in Sachen PSD2 § 4.9 Widerrufsantrag durch die NCA für PSD2 Korrektur von Tippfehlern und Bezügen
Gründe:	Ausstellung von QSealC-Zertifikaten gemäß der PSD2-Richtlinie Änderung der Firmenbezeichnung TecnoInvestimenti

Version/Release Nr.:	**3.4**
Datum Version/Release:	20.06.2018
Beschreibung der Änderungen:	§ 1.5.1 Änderung der Nummer des Callcenters § 9.2.1 Aktualisierung der Versicherungssummen
Gründe:	-

Version/Release Nr.:	**3.3**
Datum Version/Release:	04.09.2918
Beschreibung der Änderungen:	Kap. 1 Korrektur von „digitale Signatur“ in „qualifizierte elektronische Signatur”. Einige begriffliche Korrekturen für ein besseres Verständnis, Ergänzung um einige Definitionen von Begriffen, die im Dokument verwendet

	werden § 3.1.5 Teilweise Bearbeitung des Abschnitts zur besseren Verständlichkeit § 3.2.3 Bearbeitung der Tabelle und von Unterabschnitten zur besseren Deutlichkeit des Inhalts und zur Einfügung in den Kontext über europäische Märkte. Erweiterung der 4-AutID-Modalität auf elektronische Identifizierungsmittel der Mitgliedstaaten. Definition eines spezifischen Dokuments mit Angabe der Dokumententypen sowie der akzeptierten elektronischen Identifizierungsmittel § 4.2 Der Abschnitt wurde teilweise zur besseren Verständlichkeit und zur Einbettung in die europäischen Märkte bearbeitet § 4.2.2 Weitere Authentifizierungssysteme § 4.3.3.2 Möglichkeiten zur Ausstellung eines bereits aktiven Zertifikats § 4.5.3 Aufnahme einer weiteren Nutzungsbeschränkung § 4.9.15 und 4.9.16 Suspendierung und Reaktivierung über CMS § 9.4 Bezug auf DSGVO hinzugefügt § 9.6, § 9.7, § 9.8, § 9.9, § 9.10 Neuformulierung der Abschnitte für eine bessere Einbettung Nutzerzertifikat: Zertifikate juristische Person auf QSCD hinzugefügt, einige Fehler korrigiert
Gründe:	-

Version/Release Nr.:	**3.2**
Datum Version/Release:	02.05.2017
Beschreibung der Änderungen:	Um Informationen betreffend die CA „Infocert Qualifizierte Signatur 2“ ergänzt Um einige OIDs betreffend die CA „Infocert Qualifizierte Signatur 2“ ergänzt Stilistische und orthografische Korrekturen
Gründe:	

Version/Release Nr.:	**3.1**
Datum Version/Release:	27.01.2017

Beschreibung der Änderungen:	§3.2.3 alle SPID-Bezugnahmen als Authentifizierungsmittel für die Identitätsprüfung gelöscht §3.2.3.1 Identitätsprüfung durch den Arbeitgeber im Einzelnen dargelegt § 04.08.2012 Verfahrensweise der Reaktivierung der Suspendierung beschrieben
Gründe:	-

Version/Release Nr.:	**3.0**
Datum Version/Release:	12.12.2016
Beschreibung der Änderungen:	o. A.
Gründe:	neue Ausgabe des Dokuments

9.12.2 Überarbeitungsverfahren

Die Verfahren für die Überarbeitung der Beschreibung der Zertifizierungspraxis entsprechen den Formulierungsverfahren. Die Überarbeitungen werden in Absprache mit dem Leiter des Zertifizierungsdienstes, dem Leiter der Sicherheit, dem Leiter des Datenschutzes, der Rechtsabteilung und der Beratungsabteilung vorgenommen und vom Management gebilligt.

9.12.3 Zeitraum und Ablauf der Benachrichtigungen

Die Beschreibung der Zertifizierungspraxis wird veröffentlicht:

- in elektronischem Format auf der Website des Vertrauensdiensteanbieters (http://www.firma.infocert.it/doc/manuali.htm);
- in elektronischem Format in der von der AgID veröffentlichten Liste der Zertifizierungsanbieter;
- in Papierformat, das bei den Registration Authorities oder der Kontaktstelle für Endnutzer angefordert werden kann.

9.12.4 Fälle, in denen der OID geändert werden muss

o. A.

9.13 Streitbeilegung

Für die Einzelheiten zur Beilegung von Rechtsstreitigkeiten wird auf die Vertragsunterlagen verwiesen, die den Dienst regeln.

9.14 Gerichtsstand

Für die Verbraucher ist der Gerichtsstand das Gericht der Stadt, in der der Verbraucher seinen gewöhnlichen Aufenthalt hat. Für andere Personen, die keine Verbraucher sind, ist der Gerichtsstand Rom. In den Vereinbarungen zwischen CA und RA, zwischen CA und Antragsteller oder zwischen CA und Zertifikatsinhaber kann ein anderer Gerichtsstand vereinbart werden.

9.15 Geltendes Recht

Diese Beschreibung der Zertifizierungspraxis unterliegt dem italienischen Recht.

Es folgt eine nicht erschöpfende Liste der wichtigsten geltenden einschlägigen Rechtsbestimmungen:

[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 (auch *eIDAS-Verordnung*).
[2] Gesetzesvertretendes Dekret Nr. 82 vom 7. März 2005 (Amtsblatt Nr. 112 vom 16. Mai 2005) – Kodex der digitalen Verwaltung (auch *CAD*) i. d. g. F.
[3] *nicht verwendet*
[4] Gesetzesvertretendes Dekret Nr. 196 vom 30. Juni 2003 (Amtsblatt Nr. 174 vom 29. Juli 2003) – Datenschutzgesetz i.d.g.F. und Verordnung (EU) 2016/679 des Europäischen Parlaments und des Rates vom 27. April 2016 zum Schutz natürlicher Personen bei der Verarbeitung personenbezogener Daten, zum freien Datenverkehr (gilt ab 25. Mai 2018)
[5] *nicht verwendet*.
[6] *nicht verwendet*
[7] Richtlinie 2011/83/EU des Europäischen Parlaments und des Rates vom 25. Oktober 2011 über die Rechte der Verbraucher und die betreffenden einzelstaatlichen Rechtsvorschriften zur Umsetzung.
[8] Vorabprüfung – 24. September 2015 [4367555] Verarbeitung personenbezogener Daten im Bereich des „Ausstellungsverfahren mit Identitätsprüfung über Webcam“ für qualifizierte elektronische oder digitale Signaturen.
[9] Beschluss CNIPA Nr. 45 vom 21. Mai 2009 in der Fassung gemäß den späteren Entscheidungen (ab. 5. Juli 2019 durch [13] ersetzt).
[10] Entscheidung AgID Nr. 189/2017.
[11] Richtlinie 2015/2366/EU des Europäischen Parlaments und des Rates vom 25. November 2015, die sogenannte Payment Services Directive – PSD2.
[12] Delegierte Verordnung (EU) 2018/389 der Kommission vom 27. November 2017 zur Ergänzung der Richtlinie (EU) 2015/2366 des Europäischen Parlaments und des Rates durch technische Regulierungsstandards für eine starke Kundenauthentifizierung und für sichere offene Standards für die Kommunikation.
[13] Entscheidung AgID Nr. 121/2019 Version 1.1 (ersetzt den Beschluss CNIPA 45/2009).

Es gelten zudem alle Rundschreiben und Beschlüsse der Aufsichtsbehörde [9] sowie die

[9] Verfügbar auf der Website https://www.agid.gov.it/index.php/it/piattaforme/firma-elettronica-qualificata.

Durchführungsrechtsakte gemäß der eIDAS-Verordnung [1].

9.16 Verschiedene Bestimmungen

Für alle anderen, in dieser Beschreibung nicht enthaltenen Bestimmungen wird auf die Vertragsunterlagen verwiesen, die den Dienst regeln.

9.17 Sonstige Bestimmungen

Die Bereitstellungszeiten des Dienstes sind (vorbehaltlich anderer vertraglicher Vereinbarungen):

Dienst	Uhrzeit
Zugriff auf das öffentliche Zertifikatsarchiv (umfasst die Zertifikate CRL und OCSP).	Von 0:00 bis 24:00 7 Tage/Woche (Mindestverfügbarkeit 99 %)
Widerrufs- und Suspendierungsantrag der Zertifikate.	Von 0:00 bis 24:00 7 Tage/Woche (Mindestverfügbarkeit 99 %)
Andere Tätigkeiten: Registrierung, Erzeugung, Veröffentlichung, Erneuerung[10].	Von 09:00 bis 17:00 von Montag bis Freitag mit Ausnahme von Feiertagen Von 9:00 bis 13:00 Samstag
Antrag und/oder Überprüfung des Datumstempels	24 Stunden, 7 Tage/Woche (Mindestverfügbarkeit 99 %)

[10] Die Registrierung erfolgt an den Registrierungsstellen, die andere Öffnungszeiten haben können. InfoCert garantiert auf jeden Fall die Bereitstellung seines Dienstes während der oben genannten Uhrzeiten.

Anhang A

Electronic Signature Qualified Root „InfoCert Qualifizierte Signatur 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 Qualifizierte Signatur 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 Qualifizierte Signatur 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
:   }
```

Qualifiziertes Zertifikat natürliche Person mit Identifikatoren und semantischen Schlüsseln auf 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	

Qualifiziertes Zertifikat natürliche Person OHNE Identifikatoren und semantische Schlüssel auf QSCD, ausgestellt von der CA „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	

Qualifiziertes Zertifikat natürliche Person OHNE Identifikatoren und semantische Schlüssel auf QSCD, ausgestellt von der CA „InfoCert Qualifizierte Signatur 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 Qualifizierte Signatur 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	
Uniform Resource ID2:	

Field	Value
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 (qualifizierte elektronische Signatur) • 1.3.76.36.1.1.2 (automatische qualifizierte Signatur) • 1.3.76.36.1.1.22 (qualifizierte elektronische Fernsignatur) • 1.3.76.36.1.1.32 (qualifizierte CMS-Signatur)
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	

Qualifiziertes Zertifikat natürliche Person mit Identifikatoren und semantische Schlüssel

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	

Qualifiziertes Zertifikat natürliche Person OHNE Identifikatoren und semantische Schlüssel

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	

Qualifiziertes Zertifikat juristische Person mit Identifikatoren und semantische Schlüssel

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	

Qualifiziertes Zertifikat juristische Person OHNE Identifikatoren und semantische Schlüssel

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	

Qualifiziertes Zertifikat juristische Person mit Identifikatoren und semantische Schlüssel auf 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	

Qualifiziertes Zertifikat juristische Person mit Identifikatoren und semantische Schlüssel auf 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	

Erweiterungen QCStatement für QSealC PSD2

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 der CRLs und OCSPs

Erweiterung	Wert
Issuer Signature Algorithm	sha-256WithRSAEncryption [1 2 840 113549 1 1 11]
Issuer Distinguished Name	InfoCert
thisUpdate	Datum im UTC-Format
nextUpdate	Datum der nächsten CRL In Format
Revoked Certificates List	Liste der widerrufenen Zertifikate mit Seriennummer und Datum des Widerrufs/der Suspendierung
Issuer's Signature	Signatur der CA

Werte und Erweiterungen für CRL und OCSP

Die CRLs haben folgende Erweiterungen:

Extension	Value
Authority Key Identifier	Hashwert 160-bit SHA-1 des Issuer PublicKey
CRL number	Die eindeutige Nummer der CRL, die die CA zugeteilt hat
ExpiredCertsOnCRL	Das Datum im Format GeneralizedTime, ab dem die abgelaufenen Zertifikate in der CRL gehalten werden Der Wert ist auf das Datum der Ausstellung der CA eingestellt
Issuing Distribution Point	Identifiziert den Verteilungspunkt der CRLs und den Zweck: Er gibt an, ob die CRL nur für CA-Zertifikate oder vom Zertifikatsinhaber (end-entity) erzeugt wurde
Invalidity Date	Datum im UTC-Format, ab dem das Zertifikat als ungültig gilt

Die OCSP-Anfrage enthält folgende Felder:

Field	Value
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	Hashwert der Aussteller-DN
Issuer Key Hash	Hashwert des öffentlichen Schlüssels des Ausstellers.
Serial Number	Seriennummer des Zertifikats

Die OCSP-Antwort enthält folgende Felder:

Field	Value
Response Status	Status der OCSP-Antwort
Response Type	id-pkix-ocsp-basic [1 3 6 1 5 5 7 48 1 1]
Responder ID	Subject DN des Unterzeichnerzertifikats der OCSP-Antwort.
Produced at	Das Datum im Format GeneralizedTime der Antwortgenerierung 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	Hashwert des distinguishName des Ausstellers
Issuer Key Hash	Hashwert des öffentlichen Schlüssels des Ausstellers
Serial Number	Seriennummer des Zertifikats
thisUpdate	Das Überprüfungsdatum des Zertifikatsstatus im Format GeneralizedTime
nextUpdate	Datum, in dem der Status der Zertifikats aktualisiert werden könnte
Issuer Signature Algorithm	sha-256WithRSAEncryption [1 2 840 113549 1 1 11]
Issuer's Signature	[OCSP response Signature]
Issuer certificate	[OCSP response signing certificate]

Die OCSP-Anfrage kann folgende Erweiterungen enthalten:

Extension	Value
nonce	Eine willkürliche Nummer, die nur einmal verwendet werden kann. Sie verknüpft kryptografisch eine Anfrage mit ihrer Antwort, um Replay-Angriffe zu verhindern. Sie ist im Fall der Anfrage in einer requestExtension enthalten, während sie bei der Antwort in einer responseExtension enthalten sein kann.

S. Anhang B

Mittel und Verfahrensweisen für das Unterzeichnen und die Überprüfung der digitalen Signatur

InfoCert stellt ein Produkt („Dike“) bereit, das die Zertifikatsinhaber kostenlos von der Website www.firma.infocert.it herunterladen können. Es ermöglicht:

- allen Zertifikatsinhabern, die im Besitz eines von InfoCert ausgestellten Zertifikats sind, Dokumente digital zu unterzeichnen;
- die auf digital unterzeichneten Dokumenten gemäß den von den Umsetzungsrechtsakten der Verordnung definierten Formaten gesetzte Signatur zu überprüfen.

Die Nutzungsbereiche von Dike, die Hardware- und Software-Anforderungen sowie alle Anweisungen für die Installation des Produkts sind auf der oben genannten Website-Adresse angeführt. Die Anweisungen zur Nutzung des Produkts sind in diesem selbst enthalten und können über die Help-Funktion abgefragt werden. Das Produkt Dike kann jeden Dateityp unterzeichnen. Für die Anzeige der Datei muss an der Arbeitsstation des Benutzers eine passende Visualisierungssoftware installiert sein.

InfoCert kann gegen Zahlung und gemäß den von Mal zu Mal mit den RAs, den Antragstellern, den Zertifikatsinhabern oder den Nutzern abgeschlossenen Geschäftsvereinbarungen weitere Produkte oder Signaturdienste und/oder Signaturüberprüfungsdienste bereitstellen. Die elektronischen Dokumente, die mit InfoCert ausgestellten Zertifikaten signiert wurden, sind auch über andere Mittel überprüfbar, die die vorgesehenen Signaturformate interpretieren können. InfoCert haftet nicht für solche Tools.

Zum Beispiel können die unter Verwendung der gemäß dieser CPS ausgestellten Zertifikate signierten Dokumente im PAdES-Format mit Adobe Reader® überprüft werden.

Hinweis

Einige Formate ermöglichen die Einbindung von ausführbaren Codes (Makros oder Befehle) in das Dokument, ohne dass dadurch die binäre Struktur geändert wird, während Funktionen aktiviert werden, die die in dem Dokument repräsentierten Rechtsakte, Fakten oder Daten abgeändert werden können. Digital signierte Dateien, die solche Strukturen enthalten, erzeugen keine Rechtswirkungen im Sinne von Artikel 25 Absatz 2 der Verordnung [1], d. h. sie können nicht wie eine handschriftliche Unterschrift anerkannt werden. Es obliegt dem Inhaber, sich mithilfe der typischen Funktionen eines jeden Produkts darüber zu vergewissern, dass keine solchen ausführbaren Codes vorhanden sind.