PDS

PKI Disclosure Statement

DOKUMENTEN-CODE	ICERT-INDI-PDS
VERSION	3.3
DATUM	24.05.2022

INFOCERT
TINEXTA GROUP

INHALTSVERZEICHNIS

1. EINLEITUNG 3
2. KONTAKTE 3
3. ARTEN VON ZERTIFIKATEN, VALIDIERUNG UND VERWENDUNG 4
4. VERTRAUENSGRENZEN 5
5. PFLICHTEN DES ZERTIFIKATSINHABERS 5
6. PFLICHTEN DES ANTRAGSTELLERS, WENN DIESER NICHT DER ZERTIFIKATSINHABER IST 7
7. GÜLTIGKEITSSTATUS DER ZERTIFIKATE 8
8. BESCHRÄNKTE GARANTIE UND HAFTUNGSFREIHEIT/-BESCHRÄNKUNG 8
9. ANWENDBARE VERTRÄGE, POLITIKEN UND BESCHREIBUNGEN DER ZERTIFIZIERUNGSPRAXIS 9
10. DATENSCHUTZERKLÄRUNG 9
11. ERSTATTUNGSRICHTLINIEN 10
12. ANWENDBARES RECHT FÜR REKLAMATIONEN UND BEILEGUNG VON STREITIGKEITEN 10
13. ARCHIVE, LIZENZEN UND MARKEN, AUDIT 11

1. Einleitung

Dieses PKI-Disclosure-Statement (PDS) erfüllt die von der europäischen ETSI-Norm EN 319 411-1 vorgesehene Offenlegungspflicht in Bezug auf den Qualified Trust Service Provider InfoCert SpA., (in der Folge „**InfoCert“ oder „QTSP“**) angebotenen Zertifizierungsdienst und hat den Zweck, dem Antragsteller des Dienstes die für seine Nutzung notwendigen technischen Informationen bereitzustellen.

Die 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“ wird als „**eIDAS-Verordnung**“ bezeichnet.

Dieses Dokument ergänzt die allgemeinen Geschäftsbedingungen und ist ein fester Bestandteil der Vertragsdokumentation von InfoCert.

Die Veröffentlichung dieses PDS ist kein Ersatz für die Veröffentlichung des Certification Practice Statement (CPS), in dem die Informationen noch detaillierter sind, und das auf der Website von InfoCert unter der folgenden Adresse verfügbar ist: https://www.firma.infocert.it/documentazione/.

2. Kontakte

InfoCert S.p.A. – USt-IdNr. 07945211006
Qualified Trust Service Provider
Piazza Sallustio 9
00187 - Rom

Dienststellen
Piazza Luigi da Porto 3
35131 Padova

Telefon: +39 06836691 - Fax: +39 06 23328861
Call Center für digitale Signatur: siehe Link https://help.infocert.it/contatti/
Web: http://www.firma.infocert.it/

E-Mail: firma.digitale@legalmail.it

Der **Widerspruch** kann durch Einsendung des hierfür vorgesehenen, auf der Website von InfoCert veröffentlichten Formulars zusammen mit einer Fotokopie eines gültigen Ausweisdokuments per zertifizierter E-Mail (PEC), Einschreiben oder Fax beantragt werden. Gemäß den Bestimmungen der allgemeinen Geschäftsbedingungen kann der Widerspruch auch bei der zuständigen Registrierungsstelle beantragt werden. InfoCert behält sich vor, weitere Kontrollen der Identität des Antragstellers vorzunehmen.

Die **Suspendierung** kann direkt online auf der Website von InfoCert beantragt werden, hierzu wird der bei Registrierung zugewiesene Geheimcode benötigt.

3. Arten von Zertifikaten, Validierung und Verwendung

InfoCert stellt qualifizierte Zertifikate gemäß dem europäischen Standard **ETSI EN 319 411** und anderen einschlägigen Standards aus, die Zertifikate werden zu den auf der Website des qualifizierten Vertrauensdiensteanbieters (QTSP) oder der Registrierungsstellen (RA) veröffentlichten Bedingungen öffentlich (privaten Unternehmen, öffentlichen Einrichtungen, Freiberuflern, Privatpersonen, usw.) angeboten.

Für die Signatur von Zertifikaten kann wahlweise einer der folgenden Algorithmen verwendet werden:

• sha256WithRSAEncryption [iso(1) member-body(2) us(840) rsadsi(113549) pkcs(1) pkcs-1(1) sha256WithRSAEncryption(11)]

• ecdsa-with-SHA256 [iso(1) member-body(2) us(840) ansi-x962(10045) signatures(4) ecdsa-with-SHA2(3) ecdsa-with-SHA256(2)]

• ecdsa-with-SHA384 [iso(1) member-body(2) us(840) ansi-x962(10045) signatures(4) ecdsa-with-SHA2(3) ecdsa-with-SHA384(3)]

• ecdsa-with-SHA512 [iso(1) member-body(2) us(840) ansi-x962(10045) signatures(4) ecdsa-with-SHA2(3) ecdsa-with-SHA512(4)].

Signaturen und Zertifikate können mit dem Produkt **GoSign** überprüft werden, das von der Website von InfoCert kostenlos heruntergeladen werden kann.

4. Vertrauensgrenzen

InfoCert stellt aus:

- **qualifizierte Zertifikate einer natürlichen Person** für die fortgeschrittene oder qualifizierte elektronische Signatur;
- **qualifizierte Zertifikate einer juristischen Person für elektronisches Siegel**, auch zur Erfüllung von PSD2-Pflichten

Außerdem erbringt InfoCert Fernsignaturdienste auf QSCD (Qualified Electronic Signature Creation Device), generiert und verwaltet Schlüssel und Zertifikate für den Unterzeichner.

Die Details und die Policies sind in der Beschreibung der Zertifizierungspraxis enthalten, die auf der Website https://www.firma.infocert.it/documentazione zur Verfügung stehen.

Die Gültigkeitsdauer jedes Zertifikats ist im Zertifikat selbst enthalten und kann zwischen mindestens einer Stunde bis zu maximal drei Jahren und drei Monaten variieren.

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

Die Ereignisprotokolle in Verbindung mit der Ausstellung der Zertifikate werden mindestens 20 (zwanzig) Jahre lang in dem an die in Italien geltenden Rechtsvorschriften gebundenen System InfoCert-Aufbewahrungssystem aufbewahrt.

Ereignisprotokolle, die mit der Ausstellung von Zertifikaten verbunden sind, werden im konformen Datenspeichersystem für Informatikdokumente von InfoCert für mindestens 20 (zwanzig) Jahre ab dem Datum des Ablaufs des Zertifikats bis zu einem Maximum von 23 (dreiundzwanzig) Jahren ab dem Ausstellungsdatum aufbewahrt.

5. Pflichten des Zertifikatsinhabers

Der **Zertifikatsinhaber** muss die im CPS und in den allgemeinen Geschäftsbedingungen enthaltenen Klauseln beachten und insbesondere:

- die Vertragsdokumentation und die eventuell weiteren Informationsunterlagen zur Kenntnis nehmen;
- die von der Certification Authority angewandten und im CPS erläuterten Identifizierungsverfahren befolgen;
- alle für die Identifizierung notwendigen Angaben bereitstellen, die auf Verlangen mit der geeigneten Dokumentation ausgestattet sein müssen;
- sein Schlüsselpaar nur für die Zwecke und in der Art und Weise verwenden, wie laut CPS zulässig ist;
- den Registrierungs- und Zertifizierungsantrag unter Annahme der allgemeinen Geschäftsbedingungen, die die Bereitstellung des Dienstes regeln, auf den von der CA erstellten analogen oder elektronischen Formularen unterzeichnen.
- bis zum Ablaufdatum des Zertifikats in folgenden Fällen sofort die CA oder die RA benachrichtigen:
  - bei Verlust, Diebstahl oder Beschädigung seiner Signatureinheit; ○ wenn er die alleinige Kontrolle über seinen privaten Schlüssel verloren hat, beispielsweise aufgrund Kompromittierung der Aktivierungsdaten (zum Beispiel PIN) seiner Signatureinheit; ○ wenn einige in seinem Zertifikat enthaltenen Informationen falsch oder nicht mehr gültig sind;
- die Geheimhaltung der für die Nutzung der Einheiten oder der Signaturdienste notwendigen Zugangsdaten wahren, diese keinen Dritten mitteilen oder bekanntgeben und sie unter seiner ausschließlichen Kontrolle behalten;
- die Verwendung dieses kompromittierten Schlüssels sofort und endgültig einstellen, außer zum Entschlüsseln des Schlüssels selbst;
- sicherstellen, dass der private Schlüssel nicht vom Zertifikatsinhaber verwendet wird, wenn der Antragsteller informiert wird, dass das Zertifikat des Zertifikatsinhabers widerrufen oder die CA kompromittiert wurde.

Die Bereitstellung und die Nutzung einer Internetverbindung und aller notwendigen Instrumente (Hard- und Software) obliegen dem Antragsteller.

6. Pflichten des Antragstellers, wenn dieser nicht der Zertifikatsinhaber ist

Wenn er nicht der Zertifikatsinhaber ist, muss der **Antragsteller** die im CPS und in den allgemeinen Geschäftsbedingungen enthaltenen Klauseln beachten und insbesondere:

- die Vertragsdokumentation und die eventuell weiteren Informationsunterlagen zur Kenntnis nehmen;
- die vom QTSP angewandten Identifizierungsverfahren 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 unterzeichnen;
- das zur Übermittlung der Dokumente, die dem Fernsignaturverfahren und der Aktivierung der Signaturschlüssel durch den Zertifikatsinhaber unterzogen werden sollen, verwendete IT-Verfahren ermitteln und dem Vertrauensdiensteanbieter mitteilen;
- die Kosten des Fernsignaturdienstes tragen und über spezifische Vorgänge und Verfahren die Zertifikatsinhaber angeben, denen die Zertifikate ausgestellt werden sollen;
- die Art des gewählten Authentifizierungssystems angeben, um das Fernsignaturverfahren zu aktivieren;
- das dafür vorgesehene und von der QTSP bereitgestellte Formular für die Beantragung eines Widerrufs oder einer Suspendierung unterzeichnen, wenn er beabsichtigt den Widerruf oder die Suspendierung des Zertifikats des Zertifikatsinhabers zu beantragen;

- den Zertifikatsinhaber über die aus dem Zertifikat entstehenden Pflichten informieren, die korrekten und wahrheitsgemäße Angaben über die Identität des Zertifikatsinhabers bereitstellen und die Verfahren und Anweisungen des QTSP und/oder der RA befolgen;
- dem QTSP die folgenden Informationen bereitstellen, wenn es sich beim Zertifikatsinhaber um eine juristische Person handelt: ○ 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 für die Zusendung der Mitteilungen vom QTSP an den Antragsteller; ○ Name der juristischen Person, die Zertifikatsinhaber ist;
    - ○ VAT Code, NTR (USt-IdNr. oder Handelsregisternummer für italienische Zertifikatsinhaber) oder LEI code (Kennung der juristischen Person);
- wenn die Schlüssel in einer Einheit des Zertifikatsinhabers generiert werden, muss der Antragsteller den entsprechenden, von ihm selbst unterzeichneten Antrag im Format PKCS#10 zusenden. Wurde die Signatureinheit nicht vom QTSP zur Verfügung gestellt, muss der Antragsteller versichern, dass die Einheit den geltenden Rechtsvorschriften entspricht, indem er die entsprechende Dokumentation vorlegt und den regelmäßigen Audits durch den QTSP unterzogen wird.

7. Gültigkeitsstatus der Zertifikate

Alle, die sich auf die in den Zertifikaten enthaltenen Informationen verlassen, müssen sich davon überzeugen, dass die Zertifikate nicht eingestellt oder widerrufen sind.

Die Informationen über den Status der Zertifikate stehen durch Konsultation der von der CA unter der im Zertifikat angegebenen URL veröffentlichten Sperrliste der widerrufenen Zertifikate (CRL) oder über den OCSP-Dienst zur Verfügung. Die Gültigkeit der Zertifikate

kann mithilfe des Produkts Dike GoSign überprüft werden, das von der Website von InfoCert kostenlos heruntergeladen werden kann.

8. Beschränkte Garantie und Haftungsfreiheit/-beschränkung

Die qualifizierten Zertifikate werden gemäß diesem Dokument und den allgemeinen Geschäftsbedingungen bereitgestellt. Alle erforderlichen technischen Details sind im CPS festgelegt.

InfoCert haftet für eventuelle Schäden, die natürlichen oder juristischen Personen vorsätzlich oder fahrlässig aufgrund einer Nichterfüllung der Pflichten nach Verordnung (EU) Nr. 910/2014 des Europäischen Parlaments und des Rates vom 23. Juli 2014 und aufgrund der Nichtanwendung aller angemessenen Maßnahmen zur Vermeidung des 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 AgID (Agentur für die Digitalisierung Italiens) Nr. 185/2017 beigefügten Reglements überschreiten darf.

Die Erstattung kann nicht verlangt werden, wenn die Nichtnutzung auf den unsachgemäßen Gebrauch des Zertifizierungsdienstes oder den Betreiber des Telekommunikationsnetzes bzw. ein unvorhersehbares Ereignis, höhere Gewalt oder nicht von InfoCert zu vertretende Ursachen zurückzuführen ist.

9. Anwendbare Verträge, Politiken und Beschreibungen der Zertifizierungspraxis

Die auf den Dienst des QTSP und die CPS anwendbaren Vereinbarungen und Bedingungen sind auf der Website von InfoCert unter der Adresse https://firma.infocert.it/documentazione veröffentlicht.

10. Datenschutzerklärung

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.

11. Erstattungsrichtlinien

Der Zertifikatsinhaber ist verpflichtet, den QTSP mit einer ausdrücklichen Willenserklärung, die vor Ablauf der Kündigungsfrist per zertifizierter Mail (PEC) an die Adresse: *richieste.rimborso@legalmail.it* oder per Einschreiben mit Rückschein an InfoCert S.p.A., Direzione Generale e Amministrativa, Via Marco e Marcelliano 45, 00147 Roma geschickt werden muss, über seinen Beschluss der Vertragskündigung zu informieren. Zu diesem Zweck kann er der Bequemlichkeit halber das auf der Website bereitgestellte Kündigungsformular verwenden, das unter folgendem Link zur Verfügung steht: *https://www.InfoCert.it/pdf/Modulo-di-recesso-tipo.pdf*.

Unbeschadet der Kosten für die Rückgabe der eventuellen Signatureinheit zu Lasten des Zertifikatsinhabers und/oder des Antragstellers nimmt der QTSP die Erstattung der bereits geleisteten Zahlungen vor. Besagte Erstattungen erfolgen zugunsten des für die anfängliche Transaktion verwendeten Girokontos, es sei denn, der Zertifikatsinhaber hat ausdrücklich eine andere Bankverbindung angegeben; auf jeden Fall trägt der Zertifikatsinhaber keinerlei Kosten infolge dieser Erstattung.

12. Anwendbares Recht für Reklamationen und Beilegung von Streitigkeiten

Die Erbringung des Zertifizierungs- und Zeitstempeldienstes wird von den in Italien geltenden Gesetzen geregelt. Für alles, was nicht ausdrücklich im vorliegenden Dokument vorgesehen ist, wird auf das italienische Zivilgesetzbuch und auf die anderen anwendbaren Gesetze verwiesen.
Alle Streitigkeiten infolge oder im Zusammenhang mit der Auslegung und Ausführung dieses Vertrags werden der ausschließlichen Gerichtsbarkeit der zuständigen Gerichte

von Rom zugewiesen, sofern in den allgemeinen Geschäftsbedingungen nichts anderes angegeben ist.

Handelt es sich beim Kunden um einen Verbraucher, ist für eventuelle Streitigkeiten in Bezug auf den mit dem Verbraucher abgeschlossenen Vertrag unabdingbar die territoriale Gerichtsbarkeit des Wohnsitzes oder des gewöhnlichen Aufenthaltsortes des Verbrauchers zuständig.

13. Archive, Lizenzen und Marken, Audit

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

Die Überprüfung der Konformität mit der Verordnung (EU) Nr. 910/2014 vom 23.07.2014, gemäß ETSI-Normen ETSI EN 319 401, ETSI EN 319 411-1 und ETSI EN 319 411-2 erfolgte durch CSQA Certificazioni S.r.l nach dem von ACCREDIA aufgrund der Normen ETSI EN 319 403 und ISO/IEC 17065:2012 definierten eIDASBewertungsschema.

InfoCert hat den Konformitätsbericht bei der Agentur für die Digitalisierung Italiens – AgID eingereicht, die bestätigt hat, dass InfoCert als qualifizierter Vertrauensdiensteanbieter gemäß Verordnung (EU) Nr. 910/2014 vom 23.07.2014 in der Trusted List aufgeführt ist.

Die italienische Liste der vertrauenswürdigen CA (Trusted List) kann auf der Website https://eidas.agid.gov.it/TL/TSL-IT.xml abgerufen werden.