PDS

PKI Disclosure Statement

CODICE DOCUMENTO	ICERT-INDI-PDS
VERSIONE	3.2
DATA	21.09.2021

InfoCert
TINEXTA GROUP

SOMMARIO

1. INTRODUZIONE 3
2. CONTATTI 3
3. TIPOLOGIE DI CERTIFICATO, VALIDAZIONE E UTILIZZO 4
4. LIMITI DI AFFIDAMENTO 5
5. OBBLIGHI DEL TITOLARE 5
6. OBBLIGHI DEL RICHIEDENTE SE DIVERSO DEL TITOLARE 6
7. STATUS DI VALIDITÀ DEI CERTIFICATI 8
8. GARANZIA LIMITATA ED ASSENZA/LIMITAZIONE DI RESPONSABILITÀ 8
9. ACCORDI APPLICABILI, POLITICHE E MANUALI OPERATIVI 9
10. PRIVACY POLICY 9
11. POLITICHE DI RIMBORSO 9
12. LEGGE APPLICABILE AI RECLAMI ED ALLA RISOLUZIONE DELLE CONTROVERSIE 10
13. ARCHIVI, LICENZE E MARCHI, AUDIT 10

1. Introduzione

Il presente PKI-Disclosure-Statement (PDS) adempie alla richiesta di pubblicazione prevista dalla norma europea ETSI EN 319 411-1, relativa al servizio di certificazione offerto dal Qualified Trust Service Provider InfoCert SpA., (da qui in avanti "**InfoCert" o "QTSP"**) e ha lo scopo di indicare al richiedente del servizio le informazioni tecniche necessarie al suo utilizzo.

Il Regolamento (UE) n. 910/2014 del Parlamento Europeo e del Consiglio del 23 luglio 2014 "in materia di identificazione elettronica e servizi fiduciari per le transazioni elettroniche nel mercato interno e che abroga la direttiva 1999/93/CE è indicato come "**Regolamento eIDAS**".

Il presente documento si aggiunge alle Condizioni Generali di Contratto come parte integrante della documentazione contrattuale di InfoCert.

La pubblicazione del presente PDS non sostituisce la pubblicazione del Certification Practice Statement (CPS), in cui le informazioni sono ulteriormente dettagliate, disponibile sul sito web di InfoCert all'indirizzo:
https://www.firma.infocert.it/documentazione/.

2. Contatti

InfoCert S.p.A. – Partita IVA 07945211006
Qualified Trust Service Provider
Piazza Sallustio, 9
00187 - Roma

Uffici operativi
Piazza Luigi da Porto 3
35131 Padova

Telefono: +39 06836691 - Fax: +39 06 23328861
Call Center Firma Digitale: consultare il link https://help.infocert.it/contatti/
Web: http://www.firma.infocert.it/
e-mail: firma.digitale@legalmail.it

È possibile richiedere la **revoca** utilizzando l'apposito modulo pubblicato sul sito web InfoCert e inviandolo via PEC, posta raccomandata o fax corredata da fotocopia di un documento di identità valido. È anche possibile richiedere la revoca presso l'ufficio di registrazione di competenza, secondo quanto previsto dalle condizioni generali di contratto. InfoCert si riserva di fare ulteriori verifiche sull'identità del richiedente.

È possibile richiedere la **sospensione** direttamente online sul sito web InfoCert, utilizzando il codice segreto assegnato durante la registrazione.

3. Tipologie di certificato, validazione e utilizzo

InfoCert rilascia certificati qualificati secondo lo standard europeo **ETSI EN 319 411** e altri standard correlati, i certificati sono offerti al pubblico (aziende private, enti pubblici, professionisti, privati, ecc.), alle condizioni pubblicate sul sito web del QTSP o delle Registration Authorities (RA).

L'algoritmo utilizzato per la firma dei certificati può essere scelto tra i seguenti:

• 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)].

Firme e certificati sono verificabili attraverso il prodotto **Dike GoSign**, gratuitamente scaricabile dal sito InfoCert.

4. Limiti di affidamento

InfoCert emette:

- **certificati qualificati a persona fisica** per firma elettronica avanzata o qualificata;
- **certificati qualificati a persona giuridica per sigillo**, anche per adempimenti PSD2

InfoCert, inoltre, eroga servizi di firma remota su QSCD (Qualified Electronic Signature Creation Device), generando e gestendo chiavi e certificati per il firmatario.

I dettagli e le policy sono riportati nei manuali operativi disponibili su https://www.firma.infocert.it/documentazione.

Il termine di validità di ogni certificato è contenuto nel certificato stesso e può variare da un minimo di un'ora ad un massimo di tre anni e tre mesi.

È vietato l'utilizzo del certificato fuori dai limiti e dai contesti specificati nel CPS e nei contratti, e comunque in violazione dei limiti d'uso e di valore (*key usage*, *extended key usage*, *user notice*) indicati nel certificato.

I log degli eventi connessi all'emissione dei certificati sono conservati per almeno 20 (venti) anni nel sistema InfoCert di conservazione vincolato dalla normativa vigente in Italia.

5. Obblighi del Titolare

Il **Titolare** deve rispettare le clausole contenute nel CPS e nelle condizioni generali di contratto, in particolare:

- prendere visione della documentazione contrattuale e dell'eventuale ulteriore documentazione informativa;
- seguire le procedure di identificazione adottate dalla Certification Authority come descritte nel CPS;
- fornire tutte le informazioni necessarie alla identificazione, corredate, ove richiesto, da idonea documentazione;
- utilizzare la sua coppia di chiavi solo per gli scopi e nei modi consentiti dal CPS;

- sottoscrivere la richiesta di registrazione e certificazione accettando le condizioni generali di contratto, che disciplinano l'erogazione del servizio, sulla modulistica analogica o elettronica predisposta dalla CA.
- fino alla data di scadenza del certificato, informare tempestivamente la CA o la RA nei seguenti casi:
    - il suo dispositivo di firma è andato perduto, rubato o danneggiato;
    - ha perso il controllo esclusivo della propria chiave privata, ad esempio a causa della compromissione dei dati di attivazione (ad esempio PIN) del proprio dispositivo di firma;
    - alcune informazioni contenute nel suo certificato sono inesatte o non più valide;
- tutelare la segretezza delle credenziali necessarie per utilizzare i dispositivi o i servizi di firma, non comunicandole o divulgandole a terzi e mantenendole sotto il suo controllo esclusivo;
- Interrompere immediatamente e definitivamente l'uso di questa chiave che sia stata compromessa, ad eccezione che per la decifrazione della chiave stessa;
- Assicurarsi che la chiave privata non sia più utilizzata dal soggetto qualora il richiedente venga informato che il certificato del soggetto è stato revocato, o che la CA è stata compromessa.

La fornitura e l'utilizzo di una connessione a Internet e di tutti gli strumenti necessari (hardware e software) sono responsabilità del richiedente.

6. Obblighi del Richiedente se diverso del Titolare

Il **Richiedente**, se diverso dal Titolare, deve rispettare le clausole contenute nel CPS e nelle condizioni generali di contratto, in particolare:

- prendere visione della documentazione contrattuale e dell'eventuale ulteriore documentazione informativa;
- seguire le procedure di identificazione adottate dal QTSP;
- fornire tutte le informazioni necessarie alla identificazione, corredate, ove richiesto, da idonea documentazione;
- sottoscrivere la richiesta di registrazione e certificazione accettando le condizioni contrattuali che disciplinano l'erogazione del servizio, sulla modulistica analogica o elettronica predisposta dalla CA;

- Individuare e comunicare al TSP la procedura informatica a mezzo della quale saranno inviati i documenti da sottoporre alla procedura di firma remota e all'attivazione delle chiavi di firma da parte del Titolare;
- Sostenere i costi del servizio di firma remota e di indicare, attraverso specifici atti e procedure, i soggetti Titolari a cui i certificati dovranno essere rilasciati;
- indicare la tipologia di sistema di autenticazione prescelta al fine di attivare la procedura di firma remota;
- se intende chiedere la revoca o sospensione del certificato del Titolare, sottoscrivere l'apposito modulo di richiesta di revoca o sospensione messo a disposizione dal QTSP;
- informare il Titolare sugli obblighi derivanti dal certificato, fornire le informazioni corrette e veritiere sull'identità del Titolare e seguire i processi e le indicazioni del QTSP e/o della RA;
- nel caso il Titolare sia una persona giuridica, fornire al QTSP le seguenti informazioni:
    - Cognome e nome del Richiedente;
    - Codice TIN o analogo codice identificativo del Richiedente (codice fiscale per il contesto italiano);
    - Estremi del documento di riconoscimento presentato per l'identificazione del Richiedente, quali tipo, numero, ente emittente e data di rilascio dello stesso;
    - e-mail per l'invio delle comunicazioni dal QTSP al Richiedente;
    - Nome del Titolare persona giuridica;
    - VAT code ovvero NTR (partita IVA o numero di Registro Imprese per i Soggetti italiani);
- quando le chiavi sono generate in un dispositivo del Soggetto, il Richiedente deve inviare apposita richiesta in formato PKCS#10 firmata dal Richiedente stesso. Nel caso in cui il dispositivo di firma non sia messo a diposizione dal QTSP, il Richiedente deve assicurare che il dispositivo rispetti la normativa vigente, presentando apposita documentazione ed essendo soggetto a audit periodici da parte del QTSP.

7. Status di validità dei certificati

Tutti coloro che si affidano alle informazioni contenute nei certificati devono verificare che i certificati non siano sospesi o revocati.

Le informazioni sullo stato dei certificati sono disponibili consultando l'elenco dei certificati revocati (CRL) pubblicato dalla CA all'url indicato all'interno del certificato oppure tramite il servizio OCSP. La verifica della validità dei certificati può essere eseguita utilizzando il prodotto Dike GoSign, gratuitamente scaricabile dal sito InfoCert.

8. Garanzia limitata ed assenza/limitazione di responsabilità

I certificati qualificati sono forniti nel rispetto del presente documento e delle condizioni generali di contratto. Tutti i dettagli tecnici necessari sono determinati nel CPS.

InfoCert è responsabile degli eventuali danni direttamente determinati, con dolo o per negligenza, a qualsiasi persona fisica o giuridica, in seguito a un mancato adempimento degli obblighi di cui al Regolamento (UE) N. 910/2014 del Parlamento Europeo e del Consiglio del 23 luglio 2014 e dal mancato utilizzo, da parte di InfoCert, di tutte le misure idonee ad evitare il danno stesso.

Nel caso di cui al paragrafo precedente, il Richiedente o il Titolare avranno diritto di ottenere, a titolo di risarcimento dei danni direttamente subiti in conseguenza del comportamento di cui al paragrafo precedente, un importo che non potrà in ogni caso essere superiore ai valori massimi previsti, per ciascun sinistro e per anno, dall'art. 3, c. 7, del Regolamento allegato alla Determinazione AgID 185/2017

Il rimborso non potrà essere richiesto qualora la mancata fruizione sia imputabile all'utilizzo improprio del servizio di certificazione o al gestore della rete di telecomunicazioni ovvero derivante da caso fortuito, forza maggiore o cause comunque non imputabili ad InfoCert.

9. Accordi applicabili, politiche e manuali operativi

Gli accordi, le condizioni applicabili al servizio del QTSP e i CPS sono pubblicati sul sito web di InfoCert all'indirizzo https://firma.infocert.it/documentazione.

10. Privacy policy

Le informazioni relative al Soggetto e al Richiedente di cui la CA viene in possesso nell'esercizio delle sue tipiche attività, sono da considerarsi, salvo espresso consenso, riservate e non pubblicabili, con l'eccezione di quelle esplicitamente destinate ad uso pubblico: *chiave pubblica, certificato (se richiesto dal Soggetto), date di revoca e di sospensione del certificato*.

In particolare, i dati personali vengono trattati da InfoCert in conformità a quanto indicato nel Decreto Legislativo 30 giugno 2003, n. 196 e nel Regolamento Europeo 2016/679 del Parlamento Europeo e del Consiglio del 27 aprile 2016 relativo alla protezione delle persone fisiche con riguardo al trattamento dei dati personali, nonché alla libera circolazione di tali dati, pienamente vincolante dal 25 maggio 2018.

11. Politiche di Rimborso

Il Titolare è tenuto ad informare il QTSP della sua decisione di recedere dal contratto tramite una dichiarazione esplicita inviata, prima della scadenza del periodo di recesso, a mezzo PEC all'indirizzo: *richieste.rimborso@legalmail.it* oppure a mezzo lettera raccomandata a.r. indirizzata ad InfoCert S.p.A., Direzione Generale e Amministrativa, Via Marco e Marcelliano, 45 00147 Roma. A tal fine, può utilizzare, per sua comodità, il modulo tipo di recesso reperibile sul sito, mediante accesso al seguente link: *https://www.InfoCert.it/pdf/Modulo-di-recesso-tipo.pdf*.

Fermi restando i costi di restituzione dell'eventuale dispositivo di firma a carico del Titolare e/o del Richiedente, il QTSP procederà al rimborso dei pagamenti già effettuati. Detti rimborsi saranno effettuati in favore del conto corrente usato per la transazione iniziale, salvo che il Titolare non abbia espressamente indicato delle coordinate bancarie diverse; in ogni caso, il Titolare non sosterrà alcun costo quale conseguenza di tale rimborso.

12. Legge applicabile ai reclami ed alla risoluzione delle controversie

La fornitura del servizio certificazione e validazione temporale è regolata dalle leggi vigenti in Italia. Per quanto non espressamente previsto nel presente documento, si fa riferimento al Codice civile italiano ed alle altre leggi applicabili.
Tutte le controversie derivanti da, o in connessione con, l'interpretazione e l'esecuzione del presente accordo, sono sottoposte alla giurisdizione esclusiva dei tribunali competenti di Roma, quando non diversamente specificato nelle condizioni generali di contratto.

Nel caso in cui il cliente sia un consumatore, eventuali controversie relative all'accordo concluso dal consumatore sono sottoposte all'inderogabile giurisdizione territoriale del giudice del luogo di residenza o di domicilio dello stesso consumatore.

13. Archivi, licenze e marchi, audit

La CA non fa verifiche sull'utilizzo di marchi registrati, ma può rifiutarsi di generare o può richiedere di revocare un certificato coinvolto in una disputa.

La verifica di conformità al Regolamento (EU) No 910/2014 del 23/07/2014, conforme agli standard ETSI EN 319 401, ETSI EN 319 411-1, ETSI EN 319 411-2, è stata eseguita da CSQA Certificazioni S.r.l, secondo lo schema di valutazione eIDAS definito da ACCREDIA secondo gli standard ETSI EN 319 403 e ISO/IEC 17065: 2012.

InfoCert ha presentato il rapporto di conformità all'Agenzia per l'Italia Digitale – AgID che ha confermato la presenza di InfoCert come Prestatore di servizi fiduciari qualificato come da regolamento (EU) No 910/2014 of 23/07/2014 nella trusted list.

La lista delle CA affidabili (Trusted List) Italiana è raggiungibile dal sito https://eidas.agid.gov.it/TL/TSL-IT.xml