PDS

Prohlášení o zpřístupnění infrastruktury veřejných klíčů

KÓD DOKUMENTU	**ICERT-INDI-PDS**
VERZE	**3.3**
DATUM	**24. 5. 2022**

INFOCERT
TINEXTA GROUP

1. OBSAH

2. Úvod

Toto Prohlášení o zpřístupnění infrastruktury veřejných klíčů (PKI Disclosure Statement, PDS) splňuje požadavek na zveřejnění stanovený evropskou normou ETSI EN 319 411-1 týkající se certifikační služby nabízené kvalifikovaným poskytovatelem služeb vytvářejících důvěru, společností InfoCert S.p.A., (dále jen „**InfoCert**“, „**QTSP**“ nebo „**CA**“, a jeho cílem je poskytnout žadatelům o službu technické informace nezbytné pro její používání.

Nařízení Evropského parlamentu a Rady (EU) č. 910/2014 ze dne 23. července 2014 o elektronické identifikaci a službách vytvářejících důvěru pro elektronické transakce na vnitřním trhu a o zrušení směrnice 1999/93/ES se dále označuje jako „**nařízení eIDAS** (electronic identification authentication and trust service)“.

Tento dokument je přílohou všeobecných podmínek pro poskytování služeb a tvoří nedílnou součást smluvní dokumentace společnosti InfoCert.

Zveřejněním tohoto dokumentu PDS se nenahrazuje zveřejnění „Prohlášení o certifikační praxi“ (Certification Practice Statement, CPS), které poskytuje podrobnější informace a je k dispozici na internetových stránkách společnosti InfoCert na následujícím odkazu:
https://www.firma.infocert.it/documentazione/.

3. Kontakty

InfoCert S.p.A. - DIČ 07945211006
Kvalifikovaný poskytovatel služeb vytvářejících důvěru
Piazza Sallustio, 9
00187 - Řím, Itálie

Obchodní kanceláře
Piazza Luigi da Porto 3

35131 Padova, Itálie

Telefon: +39 06 836691 - Fax: +39 06 23328861
Call centrum pro elektronický podpis: viz odkaz https://help.infocert.it/contatti/
Web: http://www.firma.infocert.it/
e-mail: firma.digitale@legalmail.it
O **odvolání** certifikátu pro elektronický podpis lze požádat pomocí příslušného formuláře zveřejněného na internetových stránkách společnosti InfoCert a zasláním certifikátu ověřeným e-mailem (PEC), doporučeným dopisem nebo faxem, k němuž je přiložena fotokopie platného dokladu totožnosti. O odvolání lze rovněž zažádat na příslušném registračním úřadě v souladu s postupem uvedeným ve všeobecných podmínkách pro poskytování služeb. Společnost InfoCert si vyhrazuje právo provést další kontroly totožnosti žadatele.

O **pozastavení** platnosti certifikátu pro elektronický podpis lze požádat přímo online na webových stránkách společnosti InfoCert s použitím tajného kódu přiděleného během postupu registrace.

4. Typy certifikátů, ověřování a používání

Společnost InfoCert vydává kvalifikované certifikáty odpovídající evropské normě **ETSI EN 319 411** a dalším souvisejícím normám, které jsou nabízeny veřejnosti (soukromým podnikům, veřejným orgánům, odborníkům, jednotlivcům apod.) za podmínek zveřejněných na internetových stránkách QTSP nebo jiných registračních orgánů (RA).

Algoritmus používaný k podepisování certifikátů lze zvolit z následujících podkladů:

- 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)].

Podpisy a certifikáty lze ověřit pomocí aplikace **GoSign**, kterou lze zdarma stáhnout z webových stránek společnosti InfoCert.

5. Omezení v oblasti spolehlivosti

Společnost InfoCert vydává:

- **kvalifikované certifikáty fyzickým osobám** pro zaručený nebo kvalifikovaný elektronický podpis;
- **kvalifikované certifikáty právnickým osobám pro elektronickou pečeť**, včetně certifikátů pro soulad se směrnicí o platebních službách PSD2

Společnost InfoCert dále poskytuje služby vzdáleného elektronického podpisu na kvalifikovaných zařízeních pro vytváření elektronických podpisů (QSCD z anglického Qualified Signature Creation Device), generuje a spravuje klíče a certifikáty pro podepisující osobu.

Podrobnosti a prohlášení o zásadách jsou uvedeny v Prohlášeních o certifikační praxi, která jsou k dispozici na adrese *https://www.firma.infocert.it/documentazione*.

Doba platnosti každého certifikátu je uvedena v samotném certifikátu a může se pohybovat od minimálně jedné hodiny do maximálně tří let a tří měsíců.

Je zakázáno používat certifikát mimo limity a nastavení uvedené v dokumentu CPS a ve smlouvách a v každém případě porušovat limity použití a hodnoty (*použití klíče*, *rozšířené použití klíče*, *upozornění pro uživatele*) uvedené v certifikátu.

Záznamy o událostech spojených s vydáním certifikátů jsou uchovávány v kompatibilním Systému ukládání dat informačních dokumentů společnosti InfoCert, a to po dobu nejméně 20 (dvaceti) let od data ukončení platnosti certifikátu, maximálně však 23 (dvacet tři) let od data vydání.

6. Povinnosti subjektu

K povinnostem **subjektu** patří dodržování ustanovení obsažená v prohlášení CPS a Všeobecných podmínkách pro poskytování služeb, a dále zejména následující:

- prostudovat zadávací dokumentaci a veškerou další informativní dokumentaci a řádně jim porozumět;
- dodržovat identifikační postupy přijaté certifikačním orgánem, jak je popsáno v dokumentu CPS;
- poskytnout veškeré informace nezbytné pro účely identifikace a v případě potřeby k nim přiložit příslušnou dokumentaci;
- používat přidělený pár klíčů pouze pro účely a způsoby, které povoluje dokument CPS;
- podpisem žádosti o registraci a certifikaci přijmout smluvní podmínky upravující poskytování služby, jak jsou uvedeny v analogových nebo elektronických formulářích připravených certifikačním orgánem;
- po dobu platnosti certifikátu, až do data vypršení platnosti, neprodleně informovat certifikační nebo registrační orgán o následujících okolnostech:
    - došlo ke ztrátě, odcizení nebo poškození podpisového zařízení subjektu;
    - subjekt ztratil výhradní kontrolu nad svým soukromým klíčem, například v důsledku zneužití aktivačních údajů (např. kódu PIN) podpisového zařízení;
    - některé údaje v certifikátu subjektu jsou nepřesné nebo již neplatné;
- zabezpečit utajení pověření nezbytných pro používání podpisových zařízení nebo služeb, nesdělovat je ani je neprozrazovat třetím stranám a mít nad nimi výhradní kontrolu;

- okamžitě a s konečnou platností přestat používat klíč, který byl kompromitován, s výjimkou použití pro účely dešifrování téhož klíče;
- zajistit, aby subjekt dále nepoužíval soukromý klíč v případě, že je žadatel informován o tom, že byl zrušen certifikát subjektu nebo že došlo ke kompromitaci certifikačního orgánu.

Odpovědnost za pořízení a využívání internetového připojení a všech potřebných nástrojů (hardwaru a softwaru) nese žadatel.

7. Povinnosti Žadatele, pokud je odlišný od Subjektu

Žadatel, pokud je odlišný od Subjektu, je povinen dodržovat ustanovení dokumentu CPS a Všeobecných podmínek pro poskytování služeb, zejména je povinen:

- prostudovat zadávací dokumentaci a veškerou další informativní dokumentaci a řádně jim porozumět;
- dodržovat identifikační postupy přijaté QTSP;
- poskytnout veškeré informace nezbytné pro účely identifikace a v případě potřeby k nim přiložit příslušnou dokumentaci;
- podpisem žádosti o registraci a certifikaci přijmout smluvní podmínky upravující poskytování služby, jak jsou uvedeny v analogových nebo elektronických formulářích připravených certifikačním orgánem;
- identifikovat a informovat poskytovatele služeb TSP o postupu informačních technologií, jež bude použit k zaslání předkládaných dokumentů k postupu dálkového podpisu a k aktivaci podpisových klíčů Subjektem;
- hradit náklady na službu vzdáleného podpisu a prostřednictvím konkrétních listin a postupů uvést Subjekty, kterým musí být certifikáty vydány;
- uvést preferovaný typ autentizačního systému, který se má použít k aktivaci postupu vzdáleného podpisu;

- v případě rozhodnutí o zrušení nebo pozastavení platnosti certifikátu Subjektu podepsat příslušný formulář poskytnutý QTSP pro účely žádosti o zrušení nebo pozastavení platnosti;
- informovat Subjekt o povinnostech vyplývajících z certifikátu, uvádět správné a pravdivé informace o totožnosti Subjektu a dodržovat postupy a pokyny QTSP a/nebo registračního orgánu;
- v případě, že je Subjekt právnickou osobou, poskytnout QTSP následující informace:
    - Příjmení a jméno Žadatele;
    - DIČ nebo obdobný kód či číslo identifikující Žadatele (v Itálii „codice fiscale“);
    - údaje o dokladu totožnosti předloženém za účelem identifikace Žadatele, a to typ, číslo, vydávající orgán a datum vydání;
    - e-mailová adresa pro komunikaci zasílanou QTSP Žadateli;
    - název Subjektu jako právnické osoby;
    - kód DIČ nebo NTR (DIČ nebo registrační číslo společnosti pro italské subjekty);
- jsou-li klíče generovány zařízením patřícím Subjektu, je Žadatel povinen zaslat zvláštní žádost ve formátu PKCS #10 podepsanou samotným Žadatelem. V případě, že podpisové zařízení neposkytuje QTSP, je Žadatel povinen zajistit, aby zařízení bylo v souladu s platnými předpisy, předložit příslušnou dokumentaci a nadále se podrobovat pravidelným auditům prováděným QTSP.

8. Stav platnosti certifikátů

Všechny strany, které se odvolávají na informace obsažené v certifikátech, jsou povinny zkontrolovat, zda platnost certifikátů nebyla pozastavena nebo zrušena.

Informace o stavu certifikátů jsou dostupné nahlédnutím do seznamu zrušených certifikátů (CRL), který zveřejňuje certifikační orgán na adrese URL uvedené na certifikátu, nebo prostřednictvím služby OCSP (Online Certificate Status protocol). Kontrolu platnosti certifikátů lze provádět pomocí produktu

Dike GoSign, který lze zdarma stáhnout z webových stránek společnosti InfoCert.

9. Omezená záruka a vyloučení/omezení odpovědnosti

Kvalifikované certifikáty jsou poskytovány v souladu s tímto dokumentem a s všeobecnými podmínkami pro poskytování služeb. Veškeré nezbytné technické údaje jsou uvedeny v dokumentu CPS.

Společnost InfoCert přebírá odpovědnost za škody, které mohou být způsobeny přímo fyzické nebo právnické osobě, a to úmyslně nebo z nedbalosti, v důsledku nesplnění povinností stanovených v nařízení Evropského parlamentu a Rady (EU) č. 910/2014 ze dne 23. července 2014 a v důsledku nepřijetí všech vhodných opatření ze strany společnosti InfoCert k zamezení těchto škod.

V situaci popsané v předchozím odstavci bude Žadatel nebo Subjekt oprávněn požadovat částku z titulu náhrady škody, která mu vznikla v přímém důsledku výše uvedeného úmyslného nebo nedbalostního jednání, která nesmí v žádném případě přesáhnout maximální částky stanovené na jednu škodu a v jednom roce podle čl. 3 odst. 7 Nařízení, které je přílohou usnesení AgID č. 185/2017.

Náhradu nelze požadovat v případě, že ztráta nemohla vzniknout v důsledku nesprávného používání certifikační služby nebo činnosti provozovatele telekomunikační sítě nebo situace vyplývající z nahodilé události, vyšší moci nebo z příčin, které nelze jakkoli spojovat se společností InfoCert.

10. Příslušné dohody, zásady a prohlášení o certifikační praxi

Dohody a podmínky platné pro službu QTSP a prohlášení o certifikační praxi jsou zveřejněny na internetových stránkách společnosti InfoCert na následujícím odkazu https://firma.infocert.it/documentazione.

11. Zásady ochrany osobních údajů

Není-li výslovně dohodnuto jinak, informace týkající se Subjektu a Žadatele, které certifikační orgán získá v rámci své typické činnosti, se považují za důvěrné a nelze je zveřejnit, s výjimkou případů, kdy jsou výslovně určeny ke zveřejnění: *veřejný klíč, certifikát (pokud o něj Subjekt požádá), data zrušení a pozastavení platnosti certifikátu*.

Položky osobních údajů zpracovává společnost InfoCert zejména v souladu s italským legislativním nařízením č. 196 ze dne 30. června 2003 a s nařízením Evropského parlamentu a Rady (EU) 2016/679 ze dne 27. dubna 2016 o ochraně fyzických osob v souvislosti se zpracováním osobních údajů a o volném pohybu těchto údajů, které je závazné v plném rozsahu od 25. května 2018.

12. Zásady vracení peněz

V případě rozhodnutí odstoupit od smlouvy je Subjekt povinen informovat QTSP před uplynutím lhůty pro odstoupení od smlouvy, a to výslovným prohlášením zaslaným ověřeným e-mailem (PEC) na adresu *richieste.rimborso@legalmail.it* nebo doporučeným dopisem s doručenkou na adresu InfoCert S.p.A. - Direzione Generale e Amministrativa - Via Marco e Marcelliano, 45 00147 Řím. Za tímto účelem může Subjekt z praktických důvodů použít standardní formulář pro odstoupení od smlouvy, který je k dispozici na internetových stránkách společnosti InfoCert na tomto odkazu: *https://www.InfoCert.it/pdf/Modulo-di-recesso-tipo.pdf*.

Zatímco případné náklady na vrácení podpisového zařízení nese Subjekt a/nebo Žadatel, QTSP řádně vrátí již poukázané platby. Příslušná náhrada bude vyplacena na běžný účet použitý pro původní transakci, pokud Subjekt výslovně neuvedl jiné bankovní údaje pro platbu; v každém případě bude platba náhrady nařízena a poukázána bez jakýchkoli nákladů pro Subjekt.

13. Rozhodné právo, kterým se řídí stížnosti a řešení sporů

Poskytování certifikačních služeb a služeb spojených s vydáváním časových razítek se řídí platnými právními předpisy Itálie. Ve věcech, které nejsou výslovně upraveny v tomto dokumentu, se odkazuje na italský občanský zákoník a další platné právní předpisy.
Veškeré spory vyplývající z této smlouvy nebo související s jejím výkladem a plněním podléhají výlučné pravomoci příslušných soudů v Římě, pokud není v podmínkách samotné smlouvy uvedeno jinak.

Pokud je klientem spotřebitel, veškeré spory týkající se smlouvy uzavřené spotřebitelem budou předloženy k rozhodnutí soudci, který je povinen rozhodovat v obvodu, v němž má spotřebitel bydliště nebo sídlo.

14. Archivy, licence a ochranné známky, audity

Certifikační orgán nekontroluje používání zapsaných ochranných známek, může však odmítnout vygenerovat certifikát nebo může požádat o zrušení stávajícího certifikátu, pokud se účastní sporu.

Ověření shody s nařízením (EU) č. 910/2014 ze dne 23. 7. 2014 v normách ETSI EN 319 401, ETSI EN 319 411-1, ETSI EN 319 411-2 provedla společnost CSQA Certificazioni S.r.l, a to metodou hodnocení eIDAS definovanou společností ACCREDIA podle norem ETSI EN 319 403 a ISO/IEC 17065:2012.

Zprávu o shodě předložila společnost InfoCert Agentuře pro digitální Itálii (Agenzia per l'Italia Digitale, AgID), která potvrdila zařazení společnosti InfoCert na důvěryhodný seznam kvalifikovaných poskytovatelů služeb vytvářejících důvěru, jak vyžaduje nařízení (EU) č. 910/2014 ze dne 23. 7. 2014.

Důvěryhodný seznam certifikačních orgánů v Itálii naleznete na webových stránkách AGID na adrese *https://eidas.agid.gov.it/TL/TSL-IT.xml*