

PDS

PKI közzétételi nyilatkozat

DOKUMENTUMKÓD	ICERT-INDI-PDS (HU)
VÁLTOZAT	3.3
DÁTUM	2022.05.24.

1. TARTALOMJEGYZÉK

1. TARTALOMJEGYZÉK.....	2
2. BEVEZETŐ.....	3
3. KAPCSOLAT.....	3
4. A TANÚSÍTVÁNY TÍPUSAI, ÉRVÉNYESÍTÉSE ÉS HASZNÁLATA.....	4
5. A MEGBÍZHATÓSÁG KORLÁTAI	5
6. AZ ALANY KÖTELEZETTSÉGEI	6
7. AZ IGÉNYLŐ – HA AZ ALANYTÓL ELTÉRŐ – KÖTELEZETTSÉGEI	7
8. A TANÚSÍTVÁNYOK ÉRVÉNYESSÉGI ÁLLAPOTA.....	8
9. KORLÁTOZOTT GARANCIA ÉS A FELELŐSSÉG KIZÁRÁSA/KORLÁTOZÁSA.....	9
10. ALKALMAZANDÓ MEGÁLLAPODÁSOK, SZABÁLYOK ÉS HITELESÍTÉSI SZOLGÁLTATÁSI SZABÁLYZATOK	9
11. ADATVÉDELMI SZABÁLYZAT.....	10
12. VISSZATÉRÍTÉSI SZABÁLYOK	10
13. A PANASZOK ÉS JOGVITÁK RENDEZÉSÉRE IRÁNYADÓ JOG	11
14. ARCHÍVUMOK, LICENCEK ÉS VÉDJEGYEK, AUDIT.....	11

2. Bevezető

Ez a PKI-közzétételi nyilatkozat (PDS) megfelel az InfoCert SpA minősített bizalmi szolgáltató (a továbbiakban: **InfoCert**, **QTSP** vagy **CA**) által kínált hitelesítési szolgáltatásra vonatkozó ETSI EN 319 411-1 európai szabvány szerinti közzétételi kérelemnek, és célja, hogy a szolgáltatás igénylőinek rendelkezésére bocsássa a használatához szükséges technikai információkat.

Az Európai Parlament és a Tanács 2014. július 23-i 910/2014/EU számú rendelete „a belső piacon történő elektronikus tranzakciókhoz kapcsolódó elektronikus azonosításról és bizalmi szolgáltatásokról, valamint az 1999/93/EK irányelv hatályon kívül helyezéséről” megnevezése a továbbiakban „**eIDAS-rendelet**”.

A jelen dokumentum a szolgáltatás nyújtására vonatkozó feltételekhez tartozik, és az InfoCert szerződési dokumentációjának szerves részét képezi.

A PDS közzététele nem helyettesíti a hitelesítési szolgáltatási szabályzat (CPS) közzétételét, amely a részletesebb információkat tartalmazza, és az InfoCert webhelyén érhető el:

<https://www.firma.infocert.it/documentazione/>.

3. Kapcsolat

InfoCert S.p.A. – Adószám 07945211006
Minősített bizalmi szolgáltató
Piazza Sallustio, 9
00187 - Roma

Iroda
Piazza Luigi da Porto 3
35131 Padova

Telefon: +39 06836691 - Fax: +39-06 23328861

Digitális aláírás telefonos ügyfélszolgálat: lásd itt <https://help.infocert.it/contatti/>

Web: <http://www.firma.infocert.it/>

e-mail: firma.digitale@legalmail.it

A digitális aláírás tanúsítványának **visszavonása** az InfoCert webhelyén közzétett űrlap segítségével kérhető, tanúsított elektronikus levélben, ajánlott levélben vagy faxon, érvényes személyazonosító okmány fénymásolatának kíséretében. A visszavonást az illetékes regisztrációs irodánál is lehet kérni, a szolgáltatás nyújtására vonatkozó feltételeknek megfelelően. Az InfoCert fenntartja a jogot, hogy további ellenőrzéseket végezzen az Igénylő személyazonosságával kapcsolatban.

A digitális aláírás tanúsítványának **felfüggesztése** közvetlenül az InfoCert webhelyén igényelhető, a regisztráció során megadott titkos kód használatával.

4. A tanúsítvány típusai, érvényesítése és használata

Az InfoCert az Európai **ETSI EN 319 411** szabvány és más kapcsolódó szabványok szerint minősített tanúsítványokat bocsát ki, a tanúsítványokat a QTSP webhelyén vagy a regisztrációs hatóságok (RA) által közzétett feltételek mellett a nyilvánosság (magánvállalatok, közintézmények, szakemberek, magánszemélyek stb.) számára kínálja fel.

A tanúsítványok aláírásához használt algoritmus az alábbiak közül választható:

- 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)].

Az aláírások és tanúsítványok az InfoCert webhelyéről ingyenesen letölthető **GoSign** alkalmazás segítségével ellenőrizhetők.

5. A megbízhatóság korlátai

Az InfoCert kibocsát:

- **minősített tanúsítványokat természetes személyeknek**, fokozott biztonságú vagy minősített elektronikus aláíráshoz;
- **minősített tanúsítványokat jogi személyeknek elektronikus bélyegzőhöz**, PSD2 teljesítéshez is

Az InfoCert távoli elektronikus aláírási szolgáltatásokat is biztosít QSCD-n (minősített elektronikus aláírást létrehozó eszközön), valamint kulcsokat és tanúsítványokat állít elő és kezel az aláíró számára.

A részleteket és a szabályokat a <https://www.firma.infocert.it/documentazione> oldalon elérhető hitelesítési szolgáltatási szabályzatok tartalmazzák.

Minden egyes tanúsítvány érvényességi ideje a tanúsítványban szerepel, és legalább egy órától legfeljebb három évig és három hónapig terjedhet.

A tanúsítványt tilos a CPS-ben meghatározott korlátokon és körülményeken kívül, valamint bármiképpen a tanúsítványban megadott használati és érték-korlátok (*key usage, extended key usage, user notice*) megsértésével használni.

A tanúsítványok kibocsátásához kapcsolódó eseménynaplókat az InfoCert megfelelő adattároló rendszerében tárolják a tanúsítvány lejáratától számított legalább 20 (húsz) évig, de legfeljebb a kibocsátástól számított 23 (huszonhárom) évig.

6. Az Alany kötelezettségei

Az **Alany** köteles a CPS-ben és a szolgáltatás nyújtására vonatkozó feltételekben foglaltakat betartani, különösen pedig:

- vizsgálja át a szerződés dokumentációját és minden további tájékoztató dokumentációt;
- hajtsa végre a hitelesítő hatóság által alkalmazott azonosítási eljárásokat a CPS-ben leírtak szerint;
- adja meg az azonosításhoz szükséges összes információt, kívánságra a megfelelő dokumentációval együtt;
- a kulcspárt csak a CPS által engedélyezett célokra és módon használja;
- a regisztráció és tanúsítvány igénylésének aláírásával fogadja el a szolgáltatás nyújtására vonatkozó szerződéses feltételeket a CA által készített analóg vagy elektronikus formanyomtatványon;
- a tanúsítvány lejáratí határidejéig haladéktalanul értesítse a CA-t vagy az RA-t az alábbi esetekben:
 - az Alany aláírási eszköze elveszett, ellopták vagy megsérült;
 - az Alany elveszítette a magánkulcsa feletti kizárólagos ellenőrzést, például az aláírási eszköz aktiváló adatainak (például PIN) sérülése miatt;
 - a tanúsítványában szereplő egyes információk helytelenek vagy érvényüket veszítették;
- védje az aláírási eszközök vagy szolgáltatások használatához szükséges hitelesítő adatok titkosságát azáltal, hogy azokat nem közli harmadik féllel, illetve nem hozza nyilvánosságra, és azokat kizárólagos ellenőrzése alatt tartja;
- azonnal és véglegesen hagyja abba a sérült kulcs használatát, kivéve a dekódolás céljából való használatot;
- ügyeljen arra, hogy a magánkulcsot az Alany többé ne használja, amennyiben az Igénylő arról értesül, hogy az Alany tanúsítványát visszavonták, vagy a CA megsérült.

Az internetkapcsolat és az összes szükséges eszköz (hardver és szoftver) biztosításáért és használatáért az Igénylő a felelős.

7. Az Igénylő – ha az Alanytól eltérő – kötelezettségei

Az **Igénylő**, ha az Alanytól eltérő, köteles a CPS-ben és a szolgáltatás nyújtására vonatkozó feltételekben foglaltakat betartani, így különösen:

- vizsgálja át a szerződés dokumentációját és minden további tájékoztató dokumentációt;
- hajtsa végre a QTSP által elfogadott azonosítási eljárásokat;
- adja meg az azonosításhoz szükséges összes információt, kívánságra a megfelelő dokumentációval együtt;
- a regisztráció és tanúsítvány igénylésének aláírásával fogadja el a szolgáltatás nyújtására vonatkozó szerződéses feltételeket a CA által készített analóg vagy elektronikus formanyomtatványon;
- határozza meg és közölje a TSP-vel azt a számítógépes eljárást, amelynek segítségével a távoli aláírási eljáráshoz benyújtandó dokumentumokat eljuttatják és az Alany az aláírási kulcsokat aktiválja;
- fedezze a távoli aláírás-szolgáltatás költségeit, és egyedi iratok és eljárások útján tüntesse fel azokat az Alanyokat, akik számára a tanúsítványok kibocsátásra kerülnek;
- tüntesse fel a távoli aláírási eljárás aktiválásához választott hitelesítési rendszer típusát;
- ha az Alany tanúsítványát vissza kívánja vonni vagy fel kívánja függeszteni, írja alá a QTSP által rendelkezésére bocsátott visszavonási vagy felfüggesztési kérelmet;
- tájékoztassa az Alanyt a tanúsítvánnyal járó kötelezettségekről, szolgáltatasson az Alany személyazonosságára vonatkozó pontos és valós információkat, és hajtsa végre a QTSP és/vagy az RA eljárásait és útmutatásait;
- amennyiben az Alany jogi személy, adja meg a QTSP-nek a következő információkat:
 - Az Igénylő vezeték- és utónevét;
 - Az Igénylő TIN-kódját vagy ezzel egyenértékű azonosító kódját (olasz környezetben a 'codice fiscale');

- Az Igénylő által az azonosításhoz bemutatott azonosító okmány adatait, például a típust, a számot, a kibocsátó szervezet és a kibocsátás dátumát;
- e-mail címet, ahová a QTSP közleményeit küldheti az Igénylő számára;
- a jogi személy Alany nevét;
- HÉA-kódot, NTR-t (olasz vállalkozás esetén adószám vagy cégnyilvántartási szám) vagy LEI-kódot (jogalany-azonosító);
- ha a kulcsok generálása az Alany készülékén történt, az Igénylőnek megfelelő kérelmet kell benyújtania PKCS#10 formátumban, az Igénylő által aláírva. Abban az esetben, ha a aláírást létrehozó eszközt nem a QTSP bocsátotta rendelkezésre, akkor az Igénylő megfelelő dokumentáció benyújtásával és a QTSP rendszeres auditjának vállalásával biztosítsa, hogy az eszköz megfeleljen a hatályos jogszabályoknak.

8. A tanúsítványok érvényességi állapota

Mindazoknak, akik a tanúsítványokban szereplő információkra támaszkodnak, ellenőrizniük kell, hogy a tanúsítványok nincsenek-e felfüggesztve vagy visszavonva.

A tanúsítványok állapotára vonatkozó információk megtalálhatók a CA által kiadott Visszavont tanúsítványok listájában (CRL), a tanúsítványban megadott URL címen, vagy az OCSP szolgáltatáson keresztül. A tanúsítványok érvényessége az InfoCert webhelyéről ingyenesen letölthető Dike GoSign termék használatával ellenőrizhető.

9. Korlátozott garancia és a felelősség kizárása/korlátozása

A minősített tanúsítványokat a jelen dokumentum és a szolgáltatás nyújtására vonatkozó feltételek betartásával adják ki. Minden szükséges technikai részletet a CPS határoz meg.

Az InfoCert felelős a közvetlenül meghatározható, a 910/2014/EU számú, 2014. július 23-i európai parlamenti és tanácsi irányelvekben foglalt kötelezettségek nem teljesítése következtében természetes vagy jogi személynek szándékosan vagy gondatlanságból okozott kárért, vagy ha az InfoCert nem alkalmaz minden szükséges intézkedést a kár elkerülése érdekében.

Az előző bekezdésben leírt helyzetben az Igénylő vagy az Alany jogosult a fent említett szándékos vagy gondatlan magatartás közvetlen következményeként elszenvedett károk megtérítésének igénylésére, amely összeg azonban nem haladhatja meg a 185/2017. sz. AgID-határozathoz csatolt rendelet 3. cikkének 7. szakasza szerint egy káreseményre vonatkozó, illetve egy évre megengedett maximális összegeket.

Visszatérítés nem igényelhető, ha a szolgáltatás felhasználásának elmaradása a tanúsítási szolgáltatás helytelen használatából, a távközlési hálózat üzemeltetőjétől függő vagy váratlan esetből, vis maiorból vagy egyéb, az InfoCertnek nem felróható okokból ered.

10. Alkalmazandó megállapodások, szabályok és hitelesítési szolgáltatási szabályzatok

A QTSP és a CPS szolgáltatásra alkalmazandó szerződések és feltételek megtalálhatók az InfoCert webhelyén, a <https://firma.infocert.it/documentazione> címen.

11. Adatvédelmi szabályzat

Hacsak erre vonatkozóan nincs kifejezetten eltérő megállapodás, a CA tipikus tevékenységei során a CA birtokába jutó, az Alanyra és az Igénylőre vonatkozó információk bizalmasnak minősülnek, és nem hozhatók nyilvánosságra, kivéve, ha kifejezetten nyilvánosságra hozatalra szánták őket: *nyilvános kulcs, tanúsítvány (ha az Alany kéri), a tanúsítvány visszavonásának és felfüggesztésének dátuma.*

Az InfoCert az adatokat a 2003. június 30-i 196. számú (olasz) törvényerejű rendelet rendelkezéseinek és az Európai Parlament és Tanács 2016. április 27-i 2016/679/EU számú, a természetes személyeknek a személyes adatok kezelése tekintetében történő védelméről és az ilyen adatok szabad áramlásáról szóló rendeletének megfelelően dolgozza fel, amely 2018. május 25-től teljes mértékben kötelező.

12. Visszatérítési szabályok

Az Alany a szerződéstől való elállásra vonatkozó döntéséről köteles az elállási időszak lejárta előtt a QTSP-t tanúsított e-mailben a következő címre küldött kifejezett nyilatkozat útján tájékoztatni: *richieste.rimborso@legalmail.it* vagy az InfoCert S.p.A. főigazgatóságának és adminisztratív igazgatóságának címzett, Via Marco e Marcelliano 45, 00147 Roma címre küldött ajánlott levél útján. Ennek érdekében az Alany az InfoCert webhelyén az alábbi linken elérhető szabványos elállási űrlapot is használhatja: <https://www.InfoCert.it/pdf/Modulo-di-recesso-tipo.pdf>.

Fenntartva azt, hogy az aláírási eszköz visszajuttatásának költségei az Alanyt és/vagy az Igénylőt terhelik, a QTSP a már teljesített kifizetéseket visszatéríti. Az említett visszatérítést az eredeti ügyletnél használt folyószámla javára teljesíti, kivéve, ha az Alany kifejezetten eltérő banki adatokat adott meg; azonban az Alany egyik esetben sem visel a visszatérítés miatt költséget.

13. A panaszok és jogviták rendezésére irányadó jog

A tanúsítási és időbélyegzési szolgáltatás nyújtását az Olaszországban hatályos törvények szabályozzák. Mindarra, amiről ez a dokumentum kifejezetten nem rendelkezik, az olasz Polgári törvénykönyv és az egyéb vonatkozó törvények az irányadók.

A jelen megállapodás értelmezéséből és végrehajtásából eredő, azzal kapcsolatos minden jogvita a római bíróság kizárólagos hatáskörébe tartozik, hacsak az általános szerződési feltételek másként nem rendelkeznek.

Abban az esetben, ha az ügyfél fogyasztó, akkor a fogyasztó által kötött szerződéssel kapcsolatos polgári viták szigorúan a fogyasztó lakóhelye vagy tartózkodási helye szerinti bíróság területi illetékességébe tartoznak.

14. Archívumok, licencek és védjegyek, audit

A CA nem végez ellenőrzéseket a bejegyzett védjegyek használatára vonatkozóan, de jogvita esetén elutasíthatja egy tanúsítvány generálását, illetve kérheti annak visszavonását.

Az ETSI EN 319 401, ETSI EN 319 411-1, ETSI EN 319 411-2 szabványokat kielégítő, 2014.07.23-i 910/2014/EU sz. rendeletnek való megfelelés ellenőrzését a CSQA Certificazioni S.r.l végezte, az ACCREDIA által meghatározott eIDAS értékelési rendszer szerint, amely a következő szabványokon alapul: ETSI EN 319 403 és ISO/IEC 17065: 2012.

Az InfoCert benyújtotta a megfelelőségi jelentést az Agenzia per l'Italia Digitale (Hatóság a Digitális Olaszországért) – AgID részére, amely megerősítette, hogy a 2014.07.23-i 910/2014/EU rendeletnek megfelelően az InfoCert, mint minősített bizalmi szolgáltató, szerepel a bizalmi listán.

Az olaszországi hitelesítésszolgáltatók megbízható listája az AGID webhelyén található a következő címen: <https://eidas.agid.gov.it/TL/TSL-IT.xml>