Igazságügyi Minisztérium

Tanúsítványprofil
a Céginformációs és az Elektronikus Cégeljárásban Közreműködő Szolgálat által elektronikusan nyújtott szolgáltatásokban elfogadott tanúsítványokhoz

Verzió:	1.0.
Jóváhagyta:	dr. Dávid-Damó Ágnes
Hatálybalépés dátuma:	2019. november 29.

Tartalom

1 Bevezetés

Jelen dokumentum az Igazságügyi Minisztérium Céginformációs és az Elektronikus Cégeljárásban Közreműködő Szolgálat által elektronikusan nyújtott szolgáltatásokban elfogadott, természetes személyek számára kibocsátott végfelhasználói tanúsítványok szerkezetét írja le.

A tanúsítványok szerkezetét leíró nemzetközi specifikációk, például az X.509, sokféle tanúsítványról – köztük szerverek, eszközök számára kibocsátott tanúsítványokról is – szólnak, és nagyon kevés megszorítást tesznek a tanúsítvány szerkezetére.

A tanúsítványok használatának elengedhetetlen feltétele, hogy a tanúsítványt befogadó érintett fél elvárhasson bizonyos adatszerkezetet a tanúsítványoktól, és elvárhasson bizonyos kitöltési szabályokat és ellenőrzési lépéseket az őket kibocsátó hitelesítés szolgáltatóktól. Ennek megfelelően, az egyes alkalmazásokban további, az X.509 specifikáción túlmenő megszorításokat szokás tenni a tanúsítványok tekintetében.

Jelen dokumentum ezen megszorításokat tanúsítványprofil formájában tartalmazza.

A jelen tanúsítványprofilt támogató hitelesítés szolgáltatók írásban nyilatkoznak, hogy az általuk kibocsátott tanúsítványok megfelelnek jelen tanúsítványprofilnak.

2 Megfelelés

A jelen dokumentumban meghatározott tanúsítványprofilok megfelelnek a következő specifikációknak:

1. ITU X.509 – Information technology – Open Systems Interconnection – The Directory: Publickey and attribute certificate frameworks.
2. ISO/IEC 9594-8 – Information technology – Open Systems Interconnection – The Directory: Publickey and attribute certificate frameworks
3. RFC 5280 Internet X.509 Public Key Infrastructure Certificate and Certificate Revocation List (CRL) Profile
4. RFC 4043 Internet X.509 Public Key Infrastructure Permanent Identifier
5. RFC 5480 Elliptic Curve Cryptography Subject Public Key Information
6. ETSI TS 119 312 Electronic Signatures and Infrastructures (ESI); Cryptographic Suites
7. ETSI EN 319 412-1 Electronic Signatures and Infrastructures (ESI); Certificate Profiles; Part 1: Overview and common data structures
8. ETSI EN 319 412-2 Electronic Signatures and Infrastructures (ESI); Certificate Profiles; Part 2: Certificate profile for certificates issued to natural persons
9. ETSI EN 329 412-5 Electronic Signatures and Infrastructures (ESI); Certificate Profiles; Part 5: QCStatements

3 Tanúsítványprofil

E fejezetben a tanúsítványok szerkezetére vonatkozó megszorítások kerülnek ismertetésre, kerülve a 2. fejezetben hivatkozott dokumentumokban (így például az X.509 specifikációban) szereplő előírások ismétlését, ahol csak lehet.
Ahol külön nem jelöljük, ott – jelen dokumentum kontextusában – kötelező előírásról beszélünk. Ahol külön nem jelöljük, ott a feltüntetett mező kitöltése kötelező.

3.1 A tanúsítványban szereplő alapmezők

Az X.509 tanúsítványok alapmezőire az itt leírt további kitöltési szabályok érvényesek.

3.1.1 Verzió (version)

A jelen dokumentum szerinti tanúsítványok az X.509 specifikáció szerinti „v3” tanúsítványoknak felel meg.

3.1.2 Sorozatszám (serial number)

A sorozatszám a tanúsítványt kibocsátó hitelesítő egység által generált egyedi azonosító.
A sorozatszám az adott hitelesítő egységen belül legyen egyedi.
A sorozatszámnak tartalmaznia kell legalább 8 byte-nyi véletlenszámot.

> *Megjegyzés: A sorozatszám nem feltétlenül kis szám, nem feltétlenül ember által könnyen begépelhető érték, nem feltétlenül szigorúan monoton növekvő érték, és nem feltétlenül egyesével növekszik. Egyes alkalmazások adatok lenyomatát szerepeltetik e mezőben, amely akár 16-20 karakter hosszú is lehet.*

3.1.3 Algoritmus azonosító (algorithm identifier)

Azon algoritmuskészlet, amelynek segítségével a tanúsítványt kibocsátó hitelesítés szolgáltató aláírja a tanúsítványt. Elfogadott algoritmuskészletek:

- SHA-256 RSA
- SHA-384 RSA
- SHA-512 RSA
- SHA-256 ECDSA
- SHA-384 ECDSA
- SHA-512 ECDSA

> *Megjegyzés: az SHA-1-es lenyomatképző algoritmus nem elfogadott.*

3.1.4 Aláírás (signature)

A hitelesítés szolgáltató aláírása a tanúsítványon, az előző pontban szereplő algoritmuskészlet szerint.

3.1.5 Kibocsátó (issuer)

A tanúsítvány kibocsátójának egyedi megnevezése. A tanúsítvány kibocsátójának megnevezése tekintetében jelen dokumentum nem tesz megkötéseket.

3.1.6 Érvényesség kezdete (notBefore) és vége (notAfter)

A tanúsítvány érvényességének kezdő és végdátuma.

1. RSA algoritmus esetén a notAfter értékének a kibocsátó CA lejáratán belül kell esnie, és nem lehet későbbi, mint 2022. december 31 23:59:59 (ETSI AlgoPaper - ETSI TS 119 312 Electronic Signatures and Infrastructures (ESI); Cryptographic Suites).
2. ECC algoritmus esetén a notAfter értékének a kibocsátó CA lejáratán belül kell esnie, és legfeljebb 10 évvel haladhatja meg a notBefore értéket.
   Megjegyzés: A tanúsítvány érvényességének kezdete nem feltétlenül egyezik meg a tanúsítvány kibocsátásának időpontjával. A tanúsítvány a notAfter érték előtt is érvénytelenné válhat, amennyiben a hitelesítés szolgáltató felfüggeszti vagy visszavonja.

3.1.7 Alany (subject)

A tanúsítvány alanyának megnevezése. Részletes szabályait a 3.3. fejezet tartalmazza.

3.1.8 Az alany nyilvános kulcsára vonatkozó információk (subject public key info)

Azon algoritmus azonosítója, amely a tanúsítvány alanya a tanúsítványban szereplő nyilvános kulcsot használja. Itt kizárólag az RSA vagy ECC algoritmus azonosítója szerepelhet.

Az RSA kulcshosszra vonatkozó megkötések:

- A nyilvános kulcs hossza legalább 2048 bit.
- RSA kulcshoz kiadott tanúsítvány érvényességének lejárata nem lehet később, mint 2022.12.31 23:59:59 (ETSI AlgoPaper - ETSI TS 119 312 Electronic Signatures and Infrastructures (ESI); Cryptographic Suites)

Az ECC kulcshosszra vonatkozó megkötések:

- A nyilvános kulcs hossza legalább 256 bit.
- görbe: prime256v1 (P-256)

3.2 A tanúsítványban szereplő kiterjesztések

Az alábbiakban a tanúsítványokban kötelezően szereplő X.509 kiterjesztéseket soroljuk fel. A tanúsítványok további kiterjesztéseket is tartalmazhatnak, a következő megkötésekkel:

- a további kiterjesztések nem kaphatnak „kritikus” megjelölést,
- a további kiterjesztések nem változtathatják meg alapvetően a tanúsítvány jelentését.

Megjegyzés: A vonatkozó szabványok értelmében amennyiben egy alkalmazás nem tud feldolgozni egy „kritikus” jelzéssel ellátott kiterjesztést, kötelezően el kell utasítania a tanúsítványt.

3.2.1 Hitelesítési rendek (certificate policies)

OID: 2.5.29.32 kötelező, nem kritikus

Az adott végfelhasználói tanúsítványra vonatkozó hitelesítési rendek hivatkozása. E mezőben szerepelhetnek:

- hitelesítési rendek OID-jei,
- a vonatkozó szolgáltatási szabályzat elérhetősége,
- tetszőleges szöveges felhasználói figyelmeztetés.

Legalább egy hitelesítési rend OID feltüntetése kötelező. A hitelesítési rendnek nyilvánosan elérhetőnek kell lennie.
Olyan hitelesítési rendet kell feltüntetni, amely megköveteli az alany személyes találkozás során történt azonosítását és a magánkulcs minősített aláíró eszközön történő előállítását és átadását.

3.2.2 A kibocsátó kulcsának azonosítója (authority key identifier)

OID: 2.5.29.35 kötelező nem kritikus
A kulcs egyedi azonosítója a vonatkozó nemzetközi specifikációk szerint.
keyIdentifier: kötelező, nem kritikus
authorityCertIssuer: opcionális
authorityCertSerialNumber: opcionális

3.2.3 Az alany kulcsának azonosítója (subject key identifier)

OID: 2.5.29.14 kötelező, nem kritikus
A kulcs egyedi azonosítója a vonatkozó nemzetközi specifikációk szerint.
keyIdentifier: kötelező, nem kritikus

3.2.4 Az alany alternatív nevei (subject alternative names)

OID: 2.5.29.17 kötelező, nem kritikus

A mezőre az alábbi szabályok vonatkoznak:

- ha a tanúsítvány e-mail címet tartalmaz, e mező kitöltése kötelező, és az RFC822name elemének tartalmaznia kell az e-mail címet;
- e mező tartalmazhatja az alany alternatív, a 3.3. fejezetben szereplőtől eltérő, megnevezését, de a hitelesítés szolgáltatónak az itt szereplő minden egyes értéket is ellenőriznie kell;
- e mező további értékeket is tartalmazhat;
- ha a tanúsítvány nem tartalmaz e-mail címet, e mezőt nem kötelező kitölteni;
- az RFC 4043 szerint a permanent Identifier megadása kötelező.

3.2.5 Alapvető megkötések (basic constraints)

Végfelhasználói tanúsítványban nem szerepelhet.

3.2.6 Kulcshasználat (key usage)

OID: 2.5.29.15 kötelező, KRITIKUS

A kulcshasználat mező meghatározza, hogy a tanúsítvány milyen célra használható. Értéke:

- minősített aláírás létrehozására alkalmas tanúsítványokban: kizárólag nonRepudiation.
- fokozott biztonságú (de nem minősített) aláírás létrehozására alkalmas tanúsítványokban: a nonRepudiation kötelező, a digitalSignature opcionális.
- titkosító tanúsítványokban:
  - RSA esetén: keyEncipherment
  - ECC esetén: keyAgreement
- kliens autentikációs tanúsítványokban:
  - RSA esetén digitalSignature
  - ECC esetén: digitalSignature és keyAgreement

3.2.7 Kiterjesztett kulcshasználat (Extended Key Usage)

OID: 2.5.29.37 kötelező, nem kritikus

A kulcs engedélyezett használatának további meghatározása. Értéke:

- minősített aláírás létrehozására alkalmas tanúsítványokban: üres.
- fokozott biztonságú (de nem minősített) aláírás létrehozására alkalmas tanúsítványokban: secureEmail.
- titkosító tanúsítványokban: secureEmail.
- kliens authentikációs tanúsítványokban: clientAuthentication, és itt további értékek is megengedettek.

3.2.8 CRL elosztási pontok (CRL distribution points)

OID: 2.5.29.31 kötelező, nem kritikus

Az adott tanúsítványra vonatkozó CRL elérhetősége. Mindenképpen tartalmaznia kell legalább egy HTTP-hivatkozást.

3.2.9 Szolgáltatói információ elérhetősége (authority information access)

OID: 1.3.6.1.5.5.7.1.1 kötelező, nem kritikus

További információk, amelyeket a szolgáltató a tanúsítvánnyal kapcsolatban a tanúsítványt ellenőrző érintett fél rendelkezésére bocsát.

Az alábbi elemeket kötelezően tartalmaznia kell:

- A tanúsítványra vonatkozó online tanúsítvány-állapot szolgáltatás (OCSP) elérhetőségét.
- A tanúsítványt kibocsátó hitelesítő egység tanúsítványának elérhetőségét (HTTP).

3.2.10 Minősített tanúsítvánnyal kapcsolatos állítások (qualified certificate statements)

OID: 1.3.6.1.5.5.7.1.3 kötelező, nem kritikus

Minden minősített tanúsítványban szerepelnek a következő állítások:

- A tanúsítvány minősített tanúsítvány (0.4.0.1862.1.1). Kötelező.
- A tanúsítványhoz kapcsolódó tranzakciós limit, más néven ügyleti érték (0.4.0.1862.1.2). Opcionális.

- Azon időtartam hossza (10 év), amíg a tanúsítványt kibocsátó hitelesítés szolgáltató a tanúsítványhoz kapcsolódó adatokat a tanúsítvány lejárta után megőrzi (0.4.0.1862.1.3). Kötelező.
- A tanúsítványhoz kapcsolódó aláírás-létrehozó adat biztonságos aláírás-létrehozó eszközön helyezkedik el (0.4.0.1862.1.4). Kötelező.
- A végfelhasználói tanúsítványra vonatkozó szolgáltatási szabályzat rövidített, kivonatolt változatát tartalmazó dokumentum elérhetősége (0.4.0.1862.1.5). Kötelező.
- Annak jelzése, hogy a tanúsítvány aláírás célra került kibocsátásra (0.4.0.1862.1.6.1). Kötelező.

3.3 A tanúsítvány alanyának megnevezése

Az e fejezet szerinti előírások vonatkoznak a tanúsítvány alanyának megnevezésére (DN, distinguished name). A tanúsítvány alanyának megnevezése további elemeket is tartalmazhat, de ezek nem befolyásolhatják alapvetően a megnevezés értelmét.

3.3.1 Név (common name)

OID: 2.5.4.3 kötelező

Az alany neve, a személyazonosító okmányában (személyi igazolvány, útlevél vagy új típusú jogosítvány) szereplő írásmód szerint, magyar írásmóddal, ékezethelyesen.

A tanúsítványban nem szerepelhet álnév.

3.3.2 Vezetéknév (surname)

OID: 2.5.4.4 kötelező

E mezőbe az alany vezetékneve kerül.

3.3.3 Keresztnév (given name)

OID: 2.5.4.42 kötelező

E mezőbe az alany keresztneve kerül.

3.3.4 Azonosító (serial number) – Permanent Identifier

OID: 2.5.4.5 kötelező

Az alany globálisan egyedi azonosítója valamely nyilvántartás szerint. A tanúsítványt kibocsátó szolgáltatónak biztosítania kell, hogy az adott permanent identifier értéket kizárólag ugyanezen alany tanúsítványaiban szerepelteti. A tanúsítvány megújításakor vagy cseréjekor a hitelesítés szolgáltató alapértelmezetten[1] ugyanazon permanent identifier értéket tünteti fel az új tanúsítványban. Az azonosítót az RFC 4043 – Permanent Indentifier szabványnak megfelelően kell feltüntetni a tanúsítványban, azaz a Subject/serialNumber mezőben, illetve a SAN mezőben együttesen.

[1] Ezzel szemben a szolgáltató új permanent identifier értéket tüntethet fel a tanúsítványban, ha ezt az alany kifejezetten kéri.

Amennyiben a tanúsítványt befogadó érintett fél két tanúsítványban azonos permament identifier értéket talál, akkor alappal feltételezheti, hogy a két tanúsítvány alanya azonos. Ugyanakkor, ha a tanúsítványt befogadó érintett fél két tanúsítványban eltérő permanent identifier értéket talál, abból nem következik, hogy a két tanúsítvány alanya különböző.

A mező formátuma – a szabványok adta lehetőségeken belül – tetszőleges lehet.

Megjegyzések:

1. *Ezen azonosító használata jelentősen csökkenti a befogadó érintett félre háruló adminisztratív terheket, mert ha már ismeri az alany kilétét, nem kell ismét meggyőződnie az alany kilétéről a tanúsítvány cseréjét követően.*
2. *Ezen azonosító nem azonos az X.509 serial number alapmezővel. E mező az alany azonosítóját tartalmazza, míg az X.509 alapmezőben a tanúsítvány azonosítója szerepel.*

3.3.5 Organization Identifier

OID: 2.5.4.97 opcionális

Az Organization mezőben szereplő szervezet azonosítója, kitöltése opcionális.

3.3.6 Szervezet (organization)

OID: 2.5.4.10 szervezethez kapcsolódó tanúsítványban kötelező

Amennyiben a tanúsítvány egy szervezethez kapcsolódik, akkor e mezőbe kerül a szervezet teljes vagy rövid neve az alapító okirat vagy valamely közhiteles adatbázis (pl. cégnyilvántartás) szerint, ékezetesen. Amennyiben a szervezet neve nem fér el e mezőben, a név rövidíthető, feltéve, hogy a rövidítés nem befolyásolja a név értelmét.

3.3.7 Szervezeti egység (organization unit)

OID: 2.5.4.7 opcionális

A szervezeten belüli szervezeti egység megnevezése, a szervezet állítása vagy nyilatkozata szerint. E mezőből több is szerepelhet a megnevezésben.

3.3.8 Helység (locality)

OID: 2.5.4.7 opcionális, szervezeti tanúsítvány esetén kötelező

A szervezet székhelye szerinti helység neve.

3.3.9 Ország (country)

OID: 2.5.4.6 kötelező

Az alany állandó lakcíme, illetve a szervezet székhelye szerinti ország ISO 3166-1 szerinti kétbetűs kódja.

3.3.10 Titulus (title)

OID: 2.5.4.12 opcionális

Az alany szerepe, hivatása vagy a szervezeten belüli beosztása.

3.3.11 Email (email)

OID: 1.2.840.113549.1.9.1 opcionális

Az alany e-mail címe. Az alany e-mail címét alapvetően az alternatív nevei között, az RFC822name mezőben kell elhelyezni. Az alany megnevezésében szereplő e-mail cím elemre csak a régi alkalmazásokkal való kompatibilitás miatt lehet szükség. Amennyiben kitöltésre kerül, meg kell, hogy egyezzen az alternatív nevek között szereplő RFC822name értékkel.