VÁLTOZÁSOK A TLS TERÜLETÉN

eSIGN DAY 2026.

VARGA VIKTOR

MICROSEC

ELŐADÁS TÉMÁJA

- TLS ÉLETTARTAM VÁLTOZÁSOK
- SŰRŰBB ROOT TANÚSÍTVÁNY CSERE, SZEPARÁCIÓ
- KLIENS AUTENTIKÁCIÓ KIVEZETÉSE TLS-BŐL
- PQC - POST-QUANTUM CRYPTOGRAPHY
- MTC - MERKEL TREE CERTIFICATES
- ACME
- PINNING KÉNYSZERŰ VÁLTOZÁSOK
- QWAC VÁLTOZÁSOK

TLS ÉLETTARTAM

Tanúsítvány kiadva aznap vagy utána	Tanúsítvány kiadva előtte	Maximum érvényesség	Ellenőrzött adatok max. élettartama	Domain ellenőrzés elfogadhatóságának max. élettartama
	2026.03.15	398 nap	825 nap	398 nap
2026.03.15	**2027.03.15**	**200 nap**	**398 nap**	**200 nap**
2027.03.15	2029.03.15	100 nap	398 nap	100 nap
2029.03.15		47 nap	398 nap	10 nap

ROOT ÉLETTARTAM

Program neve	Root élettartam	Köztes kiadó élettartam	Megjegyzés
CAB Forum BRG	~ 8-25 év	nem meghatározott	-
Mozilla	nem meghatározott	nem meghatározott	15 évnél régebbi (SMIME esetén 18) Root kikerül
Google	**nem meghatározott, de 5 évente cserélni kell**	**csak ajánlás: 3 év, évenkénti új CA kiadásával**	**15 évnél régebbi Root kikerül**
Apple	CAB Forum BRG-re hivatkozik		-

KLIENS AUTHENTIKÁCIÓ KIVEZETÉSE

A Google programja alapján halad a kivezetés:

- **2026 június 15.**
kevert root már nem tud bekerülni
- **2027 március 15. után**
TSL tanúsítvány csak ServerAuth-ot tartalmazhat a tanúsítványokban.

PQC – Post-Quantum Cryptography

- **Szabványi háttér rendben:**
  - FIPS 203 (ML-KEM / kulcstokozás)
  - FIPS 204 (ML-DSA / aláírás)

- **Megoldások:**
  - **TLS 1.3 Hibrid**
    ML-KEM (kicsi a kulcsméret) és EC együtt
  - **MTC - Merkel Tree Certificates**
  - **Microsoft PQC TLS Pilot Program**

MTC – Merkel Tree Certificates

- **Jelenleg nem előírás a draft-ietf-plants-merkle-tree-certs definálja**
- **A PQC méret probléma miatt találták ki**
  - EC - aláírás 64 byte – üzenet 1,5 kB
  - PQC – aláírás ~2500 byte – üzenet 10-15 kB
- **Beolvasztja magába a CT log funkciót, az megszűnik**
- **Google kommunikáció szerint 2026 végétől, illetve 2027-től várható ezeknek a Merkle Tree Certificate rendszereknek a kísérleti (staging), majd korlátozott éles bevezetése**
- **Vélemény: túl sok hiányzik még ehhez**

MTC – MŰKÖDÉSE 1.

A TSP tulajdonképpen létrehoz egy CT loghoz nagyon hasonló publikus Merkel Tree log szervert.

A tanúsítvány kiadási folyamata:

- **A TSP kiad X tanúsítványt, ezeket loggolja a saját publikus MT logjába.**
- **A TSP ezt követően aláírja a log head-jét (signed tree head - STH) PQC aláírással**
- **A TSP közzé teszi az STH-t és a consistency proof-ot**

(Ez utóbbi igazolja, hogy az előző Merkel-Tree folytatása a mostani.)

- **A tanúsítvány mellé a TSP visszaadja az ügyfélnek az STH-t is.**

MTC – MŰKÖDÉSE 2.

A kommunikációs folyamat: A szerver a TLS kézfogás során Merkle Proof csomagot küld.

Tartalma:

- **Az aláíratlan tanúsítvány**

Nem tartalmazza a TSP PQC aláírását.

- **Inclusion Proof**

Hash-lista (a Merkle-fa "ágak"), ami igazolja, hogy a szerver tanúsítványa része annak a nagy, aláírt fának, amit a TSP közzétett. Kompakt, 20-30 hash (100-200 byte).

- **Signed Tree Head (STH)**

MTC – MŰKÖDÉSE 3.

A webszerver (vagy egyéb szerver) feladatai megváltoznak, aktívvá válik.

- Régi feladat: Kezeli a tanúsítványt és a szerver PQC kulcsát.
- Folyamatosan szinkronizálnia kell a TSP-nél az STH-t és le kell töltenie a frisset, mert a böngésző felé ezt kell bemutatnia.)
- Le kell tudni generálnia az Inclusion Proof-okat a saját tanúsítványára vonatkozóan.
- Opcionális: PQC-kezelés képességgel kell rendelkezzen a szerver, mert a a kulcscsere (key exchange) fázisban a Microsoft által tesztelt hibrid (X25519+ML-KEM) módszerhez ez szükséges.

MICROSOFT PQC – TLS PILOT PROGRAM

Most indul, szigorúan teszt, nem éles.

- **X.509 tanúsítványok**
  - **Root**
    ML-DSA-87, 1 éves
  - **Köztes**
    ML-DSA-44, ML-DSA-65, ML-DSA-87, 1 éves
  - **TLS végfelhasználói**
    ML-DSA-44, ML-DSA-65, ML-DSA-87, 90 nap

🌱 **Microsec rész vesz benne.**

microsec

MICROSOFT PQC – TLS PILOT PROGRAM

A tesztelés célja: *AZ X25519MLKEM768 hibrid kulcscsere tesztelése a Windows 11, a Windows Server 2025 termékekben és az Edge böngészőben.*

Tesztelés fő oka a hálózati kompatibilitási kockázat.

- **A ClientHello üzenet key_share része:**
  - **X25519 esetében 32 byte**
  - **X25519MLKEM768 esetében 1216 byte**

  (32 byte X25519 + 1184 byte ML-KEM-768)

A ClientHello csomag mérete könnyen meghaladhatja az MTU limitet, az üzenet darabolásra kerül.

ACME

ACME PROTOKOL

ACME

2027. március 15-től 100 napra csökken a TLS tanúsítványok maximális érvényességi ideje. ACME nélkül a tanúsítványkezelés kezelhetetlenné válik.

- **Microsec teljes körűen támogatja:**
  - **Új igénylés** - válassza az ACME kulcsgenerálást
  - **Megújítás** - válassza az ACME kulcsgenerálást
  - **Élő tanúsítvány esetén** - kérje átállítását

Az ügyfélmenüben elérhetővé válnak majd a szükséges ACME azonosítók.

TANÚSÍTVÁNY PINNING

mobil alkalmazásokban

- **Android és Apple ajánlás/előírás:**
  - **A tanúsítványba foglalt nyilvános kulcs lenyomatának rögzítése**

  Amíg a kulcs nem változik ez változatlanul jó.
  - **Backup (második) kulcs rögzítése**

  Egy másik kulcsrögzítése, biztonsági terv céllal.
  (Ez ITB miatt kötelező lenne, de sokszor hiányzik.)

https://e-szigno.hu/hirek/tanusitvanyrogzites-biztonsagos-megvalositasa

QWAC VÁLTOZÁSOK

A QCP-W-GEN policy kiemelkedik a többi közül, csak ETSI hat rá:

- **Böngészőben nem használható, root programokban nem szerepel**
- **Bizalmi listáról ellenőrizhető**
- **Maximum érvényessége a 411-1 aktuális változását követően: 5 év**
- **PSD2 célokra most is kitűnően megfelel**
- **IPR, FIDA célokra is elképzelhető, hogy jó lesz**

Szigno

KÉRDÉSEK & VÁLASZOK

MICROSEC

BIZALMAT ÉPÍTÜNK

VARGA VIKTOR
MICROSEC / CA SERVICE MANAGER
VARGA.VIKTOR@MICROSEC.HU