Rövidülő tanúsítvány-élettartamok és az ACME protokoll szerepe a Web PKI-ban

Rozgonyi Attila

PKI és információbiztonsági szakértő, Microsec zrt.

MELASZ e-Sign Day 2025

Agenda

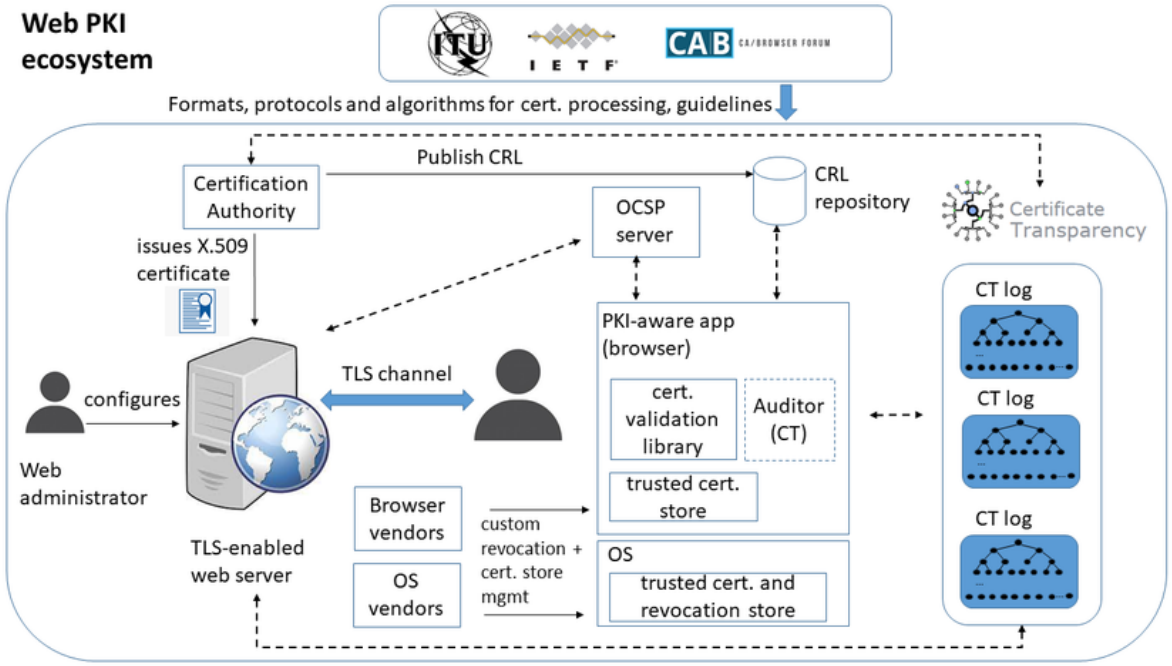
1. Bevezetés (Web PKI, tanúsítványok)
2. Élettartam-trendek
3. A rövid lejáratú tanúsítványok kihívásai
4. ACME
5. Mire számíthatunk a jövőben?

MICROSEC

1. Bevezetés

1.1 Web PKI

- HTTPS kommunikáció mára szinte alapértelmezetté vált
  - TLS protokoll – a szerver X.509 tanúsítvánnyal igazolja a hitelességét
  - Tanúsítványt CA (hitelesítésszolgáltató) állítja ki – mi alapján?
- PKI alapelv: a befogadó határozza meg az elvárásokat
  - Befogadó Web PKI esetén: böngészőprogramok (+ felhasználó)
  - Elvárások Web PKI esetén:
    - Böngésző tanúsítványtár szabályzatok,
    - CA/Browser Forum Baseline Requirements – egységes követelményrendszer
- CA/Browser Forum: böngészők és hitelesítésszolgáltatók közös fóruma



Forrás: Diana Gratiela BERBECARU, Antonio LIOY: An Evaluation of X.509 Certificate Revocation and Related Privacy Issues in the Web PKI Ecosystem

1.2 Tanúsítvány érvényessége

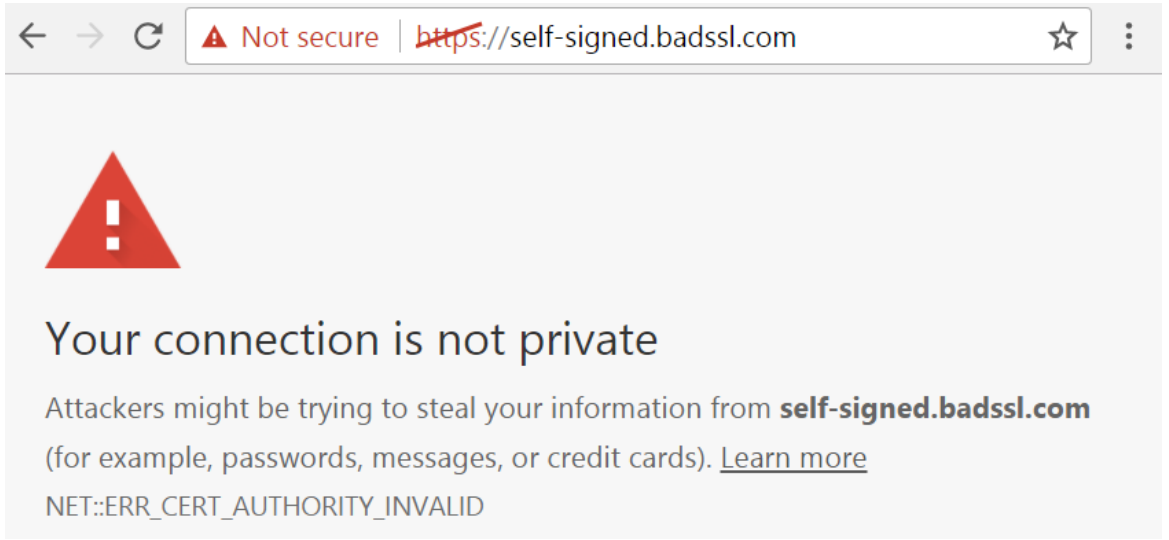
- Ha a tanúsítvány nem érvényes – riasztás
- Mikor érvényes?

  Ha megbízható hitelesítésszolgáltató adta ki
  - (Akiben a befogadó (böngésző) megbízik)

  \+ Nem járt le
  - Egy tanúsítvány csak a benne meghatározott ideig érvényes, azután érvénytelenné válik

  \+ Nem vonták vissza
  - Tanúsítvány soron kívül is érvénytelenné válhat (adatváltozás, kompromittálódás)
  - Web PKI esetén nehézkes (ld. később)

  → nagyobb hangsúly az élettartamon



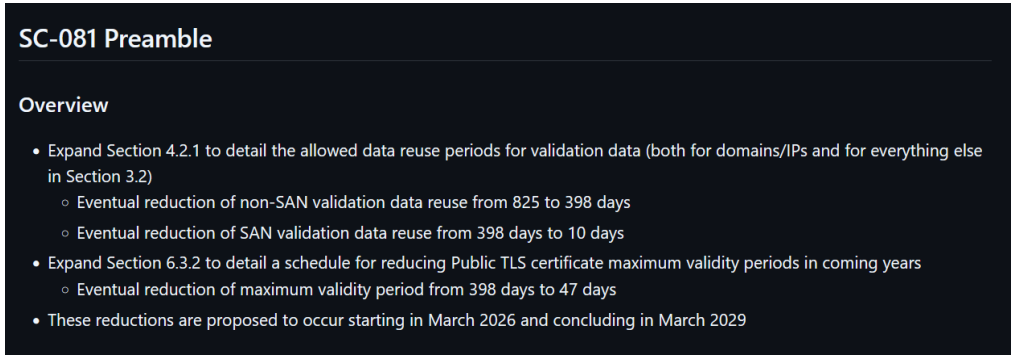
1.3 Tanúsítványok típusai

- A weboldal-hitelesítő tanúsítványoknak több szintje létezik, attól függően, hogy milyen információt igazol a birtokosról.
  - Domain validated (DV): Csak a domain feletti kontroll kerül ellenőrzésre
  - Organization validated (OV): Domain feletti kontroll + szervezeti adatok kerülnek ellenőrzésre
  - Extended Validated (EV): Domain feletti kontroll + szervezeti adatok kerülnek ellenőrzésre, de sokkal szigorúbb folyamat, több ellenőrzési feladattal

2. Élettartam-trendek

2.1 Változások

- CA/Browser Forum Baseline Requirements követelmények:
- Tanúsítványok maximális érvényessége:
  - Jelenlegi maximum: 398 nap
  - 2026.03.15-től: 200 nap
  - 2027.03.15-től: 100 nap
  - 2029.03.15-től: 47 nap
- Domain / IP cím ellenőrzés:
  - Jelenlegi újrahasználhatósági korlát: 398 nap
  - 2026.03.15-től: 200 nap
  - 2027.03.15-től: 100 nap
  - 2029.03.15-től: 10 nap
- OV és EV tanúsítványok információi:
  - Jelenlegi maximum: 825 nap
  - 2026.03.15-től: 398 nap



SC-081 Preamble

Overview

- Expand Section 4.2.1 to detail the allowed data reuse periods for validation data (both for domains/IPs and for everything else in Section 3.2)
  - Eventual reduction of non-SAN validation data reuse from 825 to 398 days
  - Eventual reduction of SAN validation data reuse from 398 days to 10 days
- Expand Section 6.3.2 to detail a schedule for reducing Public TLS certificate maximum validity periods in coming years
  - Eventual reduction of maximum validity period from 398 days to 47 days
- These reductions are proposed to occur starting in March 2026 and concluding in March 2029

2.2 Fő mozgatórugók

- Rövid lejáratú tanúsítvány koncepciója nem újkeletű – „one-shot aláíró tanúsítványok”, OCSP responder, V2X AT
- Web PKI indokok az Apple által előterjesztett módosításban:
  - Automatizált tanúsítványmenedzsment térnyerése
  - Gyakrabban rotált kulcsok – kisebb esély a kompromittálódásra
  - Gyakrabb ellenőrzés – kisebb esély elavult információkra
  - Visszavonási hiányosságok
    - Végfelhasználói tanúsítványokra bongészőknél nem kifejezett prioritás, sőt!
    - CRL: nagy, nem valós idejű
    - OCSP: adatvédelem, latency problémák
    - Jó megoldás: OCSP stapling – a webszerver gyűjti be a választ és átadja a kliensnek – de nem minden szerver támogatja

3. A rövid lejáratú tanúsítványok kihívásai

3.1 Rendszeradminisztráció

- Kritikus rendszerekben tanúsítványmenedzsment is kritikus – rendelkezésre állás stb.
- Manuális megújítás egy ideig korlátozottan kivitelezhető marad
  - Kockázatos – elfelejtett megújítás → szolgáltatáskiesés
  - DevOps / IT csapatok terhelése folyamatosan nő
  - Nagyszámú tanúsítványnál már most is nehéz
  - 2029-től a 10 naponta történő ismételt domainvalidáció gyakorlatilag lehetetlenné teszi
- Hosszú távú megoldás: automatizáció

MICROSEC

3.2 CA

- Több ellenőrzés nem teljesen automatizálható – megnövekedett adminisztrációs teher + ügyfélszolgálat, support terhelés
- Domainellenőrzés automatizálása még kritikusabb, mint a webszerver-üzemeltetés tekintetében → Követelmény is
- Multi-perspective issuance corroboration (MPIC) megjelenik - többletköltség
- Rövid élettertam = gyakrabb ellenőrzés, több tanúsítvány
  → hiba esetén korrekciós időablak csökken
- EE tanúsítvány egyre kevésbé hangsúlyos, viszont CA-kon egyre nagyobb nyomás
- CT logok száma még nagyobb mértékben nő
- A CA-k szerepe elsőre úgy tűnhet, hogy háttérbe szorul a gyakori megújítás miatt, de valójában ez még nagyobb elvárásokat támaszt rájuk nézve.

MICROSEC

4. ACME

4.1 Automatizációs kísérletek

- Koncepciót tekintve a DV igénylés viszonylag triviálisan automatizálható → Korábbian már voltak kísérletek szabványosításra,
- pl. SCEP (RFC 8894), de limitációk:
  - Csak RSA kulcsokkal használható
  - Kérelmező autentikációja esetén a tanúsítványalapú autentikáció a legerősebb, de sok deployment nem támogatja

  → shared secret

  → CSR (PKCS#10 tanúsítványkérelem) challengePassword mezőben szerepel külső titkosítással

  → Csak CA látja a CSR-t, de lehetnek olyan felek is, akiknek jogosan szüksége lenne rá (pl. RA)

4.2 ACME

- ACME = Automatic Certificate Management Environment
- Kommunikációs protokoll a hitelesítésszolgáltatók és a tanúsítványt használó webszerverek közötti interakció automatizálására
- RFC 8555 írja le
- JSON-formázott üzenetek, HTTPS
- Sokféle kliensoldali implementáció
- Teljes DV igénylési folyamat automatizálható, mind CA, mint webszerver oldalról
- JWS autentikáció, minden üzenet aláírt

5. Mire számíthatunk a jövőben?

MICROSEC

5.1 A jövő?

- Ami automatizálható, előbb-utóbb automatizálásra kerül
  - ACME egyre jobban előtérbe kerül – uniformabb és biztonságosabb, mint az SCEP
  - Előnyök: emberi hibák csökkennek, kulcsok kitettsége csökken
  - Hátrányok: egyelőre rengeteg rendszerben nem megoldható, ezeknél viszont rövid élettartam miatt manuálisan bonyolult
- Kulcsok ettől még kompromittálódhatnak – visszavonás hatékony megoldása még mindig fontos lenne EE szinten is
- Reverse proxyk – néhány előny, rengeteg kockázat + Belső CA-k: nagy feladat, nagy kockázat
- ACME-támogatott megoldásokra való átállás elkerülhetetlen – webszerver-üzemeltető, CA és appliance vendor szinten is
  - Nemcsak DV, de szervezeti tanúsítványok esetén is támogatott

Köszönöm a figyelmet!

Rozgonyi Attila

PKI és információbiztonsági szakértő, Microsec zrt.

mailto:rozgonyi.attila@microsec.hu