MELASZ

DR. SZŐKE SÁNDOR

Minősített weboldal-hitelesítő tanúsítványok: mit hoz az eIDAS 2.0?

Magyar Elektronikus Aláírás Napja

- *„45. cikk*
- **Weboldal hitelesítésére szolgáló minősített tanúsítványokra vonatkozó követelmények**
- (1) A weboldal hitelesítésére szolgáló minősített tanúsítványoknak meg kell felelniük a IV. mellékletben foglalt követelményeknek. Amennyiben a weboldal hitelesítésére szolgáló minősített tanúsítvány megfelel a (3) bekezdésben említett szabványoknak, vélelmezni kell a IV. mellékletben foglalt követelmények teljesülését.
- (2) Az (1) bekezdésben említett, weboldal hitelesítésére szolgáló minősített tanúsítványokat a webböngészőknek fel kell ismerniük. E célból a webböngészők biztosítják, hogy a valamely módszer alkalmazásával megadott személyazonosító adatok felhasználóbarát módon jelenjenek meg. A webböngészők biztosítják az (1) bekezdésben említett, weboldal hitelesítésére szolgáló minősített tanúsítványok támogatását és interoperabilitását. Ez alól kivételt képeznek a működésük első öt évében azok a webböngészési szolgáltatásokat nyújtó vállalkozások, amelyek a 2003/361/EK bizottsági ajánlás értelmében mikro- és kisvállalkozásnak minősülnek.
- (3) E rendelet hatálybalépésétől számított 12 hónapon belül a Bizottság végrehajtási jogi aktusok útján meghatározza az (1) bekezdésben említett, weboldal hitelesítésére szolgáló minősített tanúsítványokra vonatkozó műszaki előírásokat és összeállítja az ezekre vonatkozó szabványok hivatkozási számainak listáját. Ezeket a végrehajtási jogi aktusokat a 48. cikk (2) bekezdésében említett vizsgálóbizottsági eljárással összhangban kell elfogadni.”

MELASZ állásfoglalás

eIDAS előtti világ

- Az IT világ és az internet alapú rendszerek/szolgáltatások meghatározó szállítói USA nagyvállalatok
- Az interneten kiemelten fontos a biztonságos kommunikáció
- Liberális megközelítés – a piaci résztvevők majd megoldják a problémákat
- Önkéntes alapon létrejött nyílt szervezetek műszaki előírásai, szabványai (RFC, IETF ..)
- A PKI technológia térnyerése – SSL/TLS tanúsítványok összekapcsolják a kriptográfiai kulcsot a weboldalt üzemeltető személy azonosító adataival
  - Globális szoftver szállítók
  - Lokális jelenléttel és ismerettel rendelkező helyi hitelesítés szolgáltatók

- Kölcsönös egymásra utaltság, szabályozni kellett az együttműködést

Root Programok – megbízható gyökértanúsítvány tárak

- globális operációs rendszer és egyes alkalmazás szállítók létrehoztak saját Root Programokat és megbízható gyökértanúsítvány tárakat
- az adott alkalmazás csak a megbízható CA-k által kiadott tanúsítványokat fogadja el
- egyedi követelmények, amik egyoldalúan és könnyen változtathatók
- deklaráltan saját hatáskörben szabadon dönt a felvételi kérelmekről
- a nagyobb piaci súlyú CA-kat preferálják a feldolgozás ütemezése során
- a felvételi folyamat évekig is tarthat
- nagy piaci súlyú IT szállító gazdasági érdekei mentén képes diktálni a szakmai kérdésekben is – erőfölény kihasználása
- nem végeznek saját helyszíni vizsgálatot
- különféle megfelelőségértékelő sémák és szervezetek jöttek létre
- minden Root Programba külön kell bekerülni
- igény a harmonizációra

CA/BROWSER FORUM 2005

Cél a helyzet konszolidálása

CA/BROWSER FORUM

- Önkéntes szerveződés, kétfajta tag:
  - CA-k (tanúsítvány kibocsátók)
  - alkalmazás szállítók (tanúsítvány elfogadók)
- egységes(ebb) műszaki követelményrendszer kidolgozása a biztonság növelése és a költségek csökkentése érdekében
- fókusz területek:
  - a böngészők által a weboldal azonosítására használt SSL/TLS tanúsítványok
  - általános hálózati biztonság
  - kódaláíró tanúsítványok illetve az ezekhez kapcsolódó időbélyegzés (újra)
  - S/MIME tanúsítványok emailek aláírására (tervezett)
- Többféle TLS tanúsítvány alaptípus (DV, OV, IV)
- Plusz követelmények a nagyobb bizonyosságot nyújtó EV (Extended Validation) tanúsítványokra
- Nem foglalkoznak megfelelőségértékeléssel és nincs saját Root Programjuk
- A legelterjedtebb operációs rendszer és böngésző szállítók többsége CABF tag
- Az egyes Root Programokba kerüléshez nem feltétel a CABF tagság

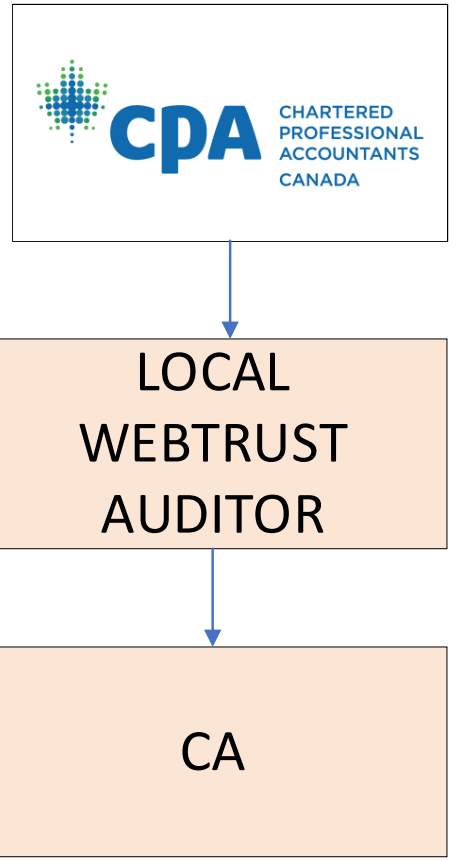
https://cabforum.org/

CA/BROWSER FORUM működése

- A nyílt folyamat keretében kidolgozott változtatási javaslatokat szavazással fogadják el
- külön szavaznak a CA-k és a böngészők
- a két csoport között előfordulnak eltérő vélemények az eltérő piaci helyzet/érdek miatt
- a CA-k függenek a böngészőktől, mert a Root Program tagságuk visszavonható
- ha a böngészők javaslatát elutasítják a CA-k, kiadhatják azt a saját Root Program követelményeként
    - tanúsítvány élettartam folyamatos és radikális csökkentése
- CABF követelmények gyorsan változnak, akár 2 naponta (*) is – nehéz követni
- Google egyre erősebb dominancia
- (2021-ben 257 milliárd USD árbevétel (Magyar GDP ~160 milliárd USD))

WEBTRUST SEAL PROGRAM

- USA és kanadai könyvvizsgáló kamarák dolgozták ki a vizsgálati módszert
- CABF követelményeknek való megfelelés
- Minden böngésző elfogadja
- A program világszerte elérhető, a vizsgálatot helyi auditorok végzik WebTrust licensz alapján
- CPA Canada adja ki a WebTrust sealt
- a sikeres audit nem jelent automatikus felvételt a Root Programokba
- A felvételi döntés továbbra is a böngészők kezében van

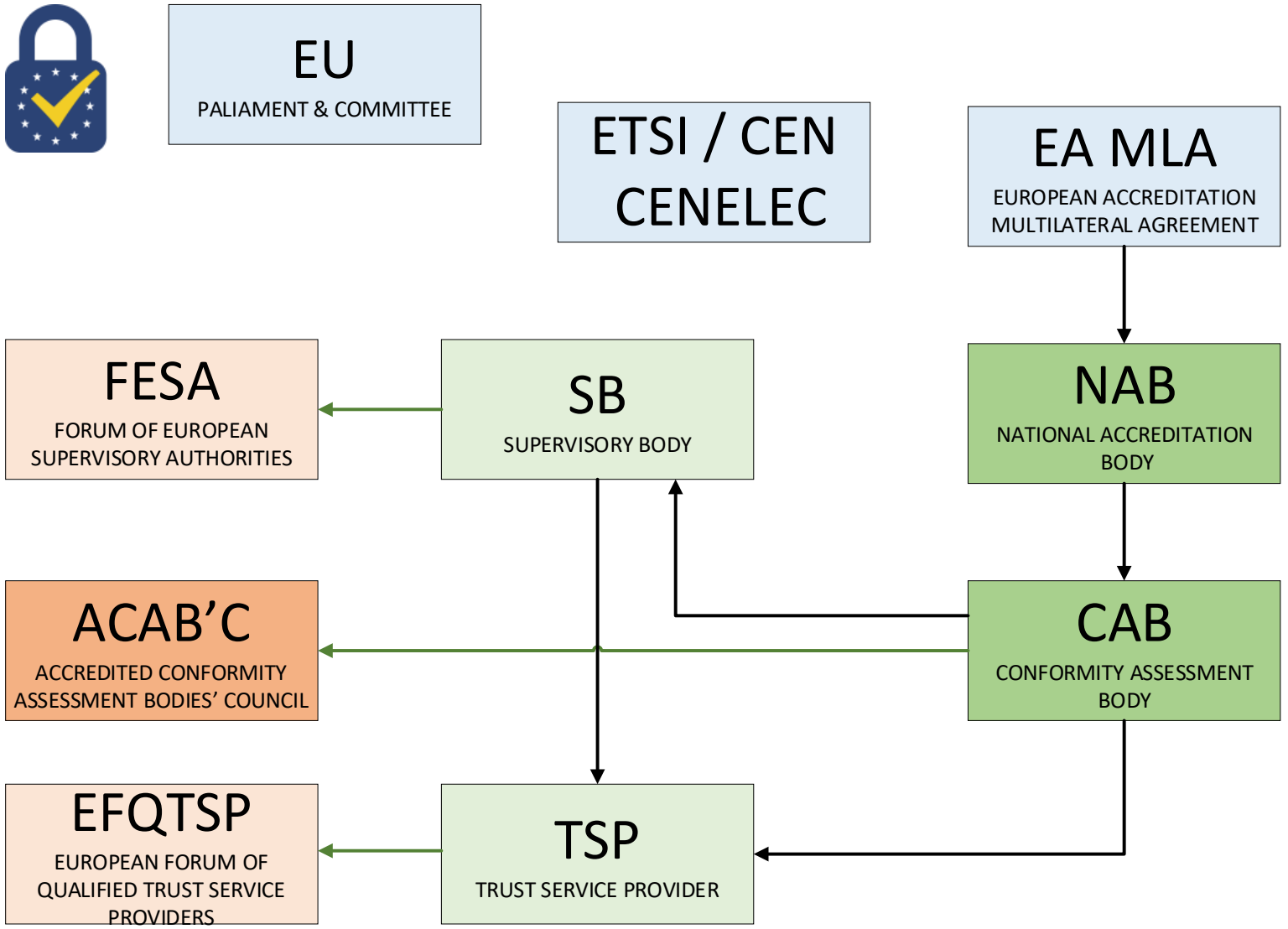


eIDAS Rendelet - 2014

- Jogi keretrendszer a bizalmi szolgáltatások számára
- Új elemként szabályozza a weboldal hitelesítő tanúsítványok kiadását is, ezzel eddig „önszabályozó” területre fogalmaz meg követelményeket
- Európai Bizottság Mandate 460 (ETSI, CEN, CENELEC)
- ETSI épít a CABF követelményekre, de óhatatlanul vannak kisebb eltérések
    - Organization Identifier (kötelező) használata
    - QCStatements kiterjesztések értelmezése
- A böngészők hozzáállása ellentmondásos, néha komoly ellentétek keletkeztek
    - PSD2 tanúsítványok
- ETSI követelményeken alapuló egységes EU megfelelőség értékelési rendszer létrehozása
- Bizalmi listák bevezetése a minősített szolgáltatásokra

EU / ETSI audit

- EU TSP-k számára „kötelező” az ETSI alapú audit
- A plusz WebTrust audit növelné a költségeket
- Sok kis EU CA van
- Root programok nem szeretik, de általában elfogadják
- A felvételről továbbra is a Root Program dönt
- Rendszeres egyeztetések a Root Programok és az EU szervezetei és az ETSI között
- ETSI követelmények többszöri finomhangolása
- Új követelmény az ACAB’C tagság



TLS tanúsítványok adattartalma

MELASZ

		DV	OV	IV	EV	DVCP	OVCP	IVCP	EVCP	QCP-w	QEVCP-w	QNCP-w
Subject Alternative Name Extension	dNSName	✓	✓	✓	✓							
	iPAddress	✓	✓	✓	☒							
Subject Distinguished Name Fields	commonName kivezetendő	✓	✓	✓	✓							
	organizationName	☒	✓	✓	✓					✓	✓	✓
	givenName	☒		✓	☒					✓	✓	✓
	surname	☒		✓	☒					✓	✓	✓
	pseudonym	☒			☒					✓	✓	✓
	streetAddress	☒	✓	✓	✓							
	localityName	☒	✓	✓	✓					✓	✓	✓
	stateOrProvinceName	☒	✓	✓	✓							
	postalCode	☒	✓	✓	✓							
	countryName	✓	✓	✓	✓					✓	✓	✓
	organizationalUnitName kivezetik 2022-09-01	☒	✓	✓	✓							
	businessCategory	☒			✓							
	jurisdictionLocalityName	☒			✓							
	jurisdictionStateOrProvinceName	☒			✓							
	jurisdictionCountryName	☒			✓							
	organizationIdentifier	☒			✓					✓	✓	✓
	cabfOrganizationIdentifier	☒			✓							
QCStatements	id-etsi-qcs 1 (eIDAS minősített)									✓	✓	✓
	id-etsi-qcs-QcType 3 (weboldal hit.)									✓	✓	✓

Böngésző felhasználói felület változása

- 2017-19 során a böngészők fokozatosan megváltoztatták a felhasználói felület jelzéseit.
- Biztonsági figyelmeztetést adnak tanúsítvánnyal nem védett oldalak használata esetén.
- A változás és az ingyenes DV tanúsítványok kibocsátása elősegítette a tanúsítvánnyal védett weboldalak elterjedését
- Korábban az EV (QWAC) tanúsítványokat zöld szín jelölte és alapból feltüntetésre került a tanúsítvány birtokos szervezet megnevezése
- A pozitív változással egyidejűleg a böngészők megszüntették a felhasználói felületen a tanúsítvány birtokos adatainak megjelenítését, így jelenleg megjelenésben nincs különbség a DV és EV tanúsítványok között
- A tanúsítványhasználat elmozdul az EV-ből az OV és DV irányba
  -> csökken a biztonság, könnyebb az adathalászat és egyéb visszaélés
- A tanúsítványban feltüntetett adatok valódiságát a hitelesítés szolgáltató garantálja, a weboldal üzemeltetője ellenőrizetlenül bármit állíthat magáról a weboldalon.
- A szakma jelentős része ellenezte a változtatást, de egy alkalmazás felhasználói felületének megtervezése teljesen a fejlesztő hatáskörébe tartozik

DESIGNING THE NEW eIDAS 2 BROWSER UI
Chris Bailey, Entrust
September 2021, CA Day

Recital (39): Any processing of personal data should be lawful and fair. It should be transparent to natural persons ***. The principle of transparency *** concerns, in particular, information to the data subjects on the identity of the controller

Recital (42): *** [T]he controller should be able to demonstrate that the data subject has given consent to the processing operation.*** For consent to be informed, the data subject should be aware at least of the identity of the controller and the purposes of the processing for which the personal data are intended.

Article 4 –Definitions:

'Personal data' means any information relating to an identified or identifiable natural person ('data subject'); an identifiable natural person is one who can be identified, directly or indirectly, in particular by reference to an identifier such as a name, an identification number, location data, [or] an online identifier

Article 13 –Information to be provided where personal data are collected from the data subject:

1. Where personal data relating to a data subject are collected from the data subject, the controller shall, at the time when personal data are obtained, provide the data subject with all of the following information: (a) the identity and the contact details of the controller***

Összefoglalva az előzményeket

- A felhasználók érdeke a biztonságos, egységes szabályok szerint működő internet
- A böngészők a kezdetek óta támadják az EU által kezdeményezett változásokat
  - nem akarnak változtatni az általuk kialakított rendszeren
  - biztonsági aggályokat fogalmaznak meg
  - nem értenek egyet a követelményekkel
  - nem akarnak fejleszteni
  - nem akarnak precedenst teremteni
  - más elképzeléseik vannak az internet jövőjéről
- A rendszeres kommunikáció beindult, létrejöttek a hivatalos kapcsolatok
- Kevés a konkrét eredmény (ETSI auditok elfogadása)
- Kedvezőtlen változások (felhasználói felület változása)

Mit hoz(6) az eIDAS 2?

- A böngészők ellenállása és a kedvezőtlen változások indokolták a követelmények beemelését a Rendelet tervezetbe.
- A böngészők lobby-ereje nem lebecsülendő – a kiegészítések teljesen kimaradtak a legújabb javaslatból
- Jó hír, hogy továbbra is folyamatosak az egyeztetések (06-29 ETSI – Root Programs – ACAB'C megbeszélés)
- Mi lehet a megoldás?
  - Együttműködés a böngészőkkel – kompromisszumos megoldás kidolgozása
  - Meglévő nyílt forráskód alapon egyedi böngésző változat kifejlesztése
  - Teljesen új böngésző kifejlesztése
  - Elvek és az önrendelkezési lehetőség feladása – követelmények törlése a tervezetből

MELASZ

Köszönöm a figyelmet!

- *dr. Szőke Sándor*
- *Microsec Zrt.*
- *szoke.sandor@microsec.hu*