TCS

Megbízható tanúsítványszolgáltatás

Bajnok Kristóf
NIIF Intézet

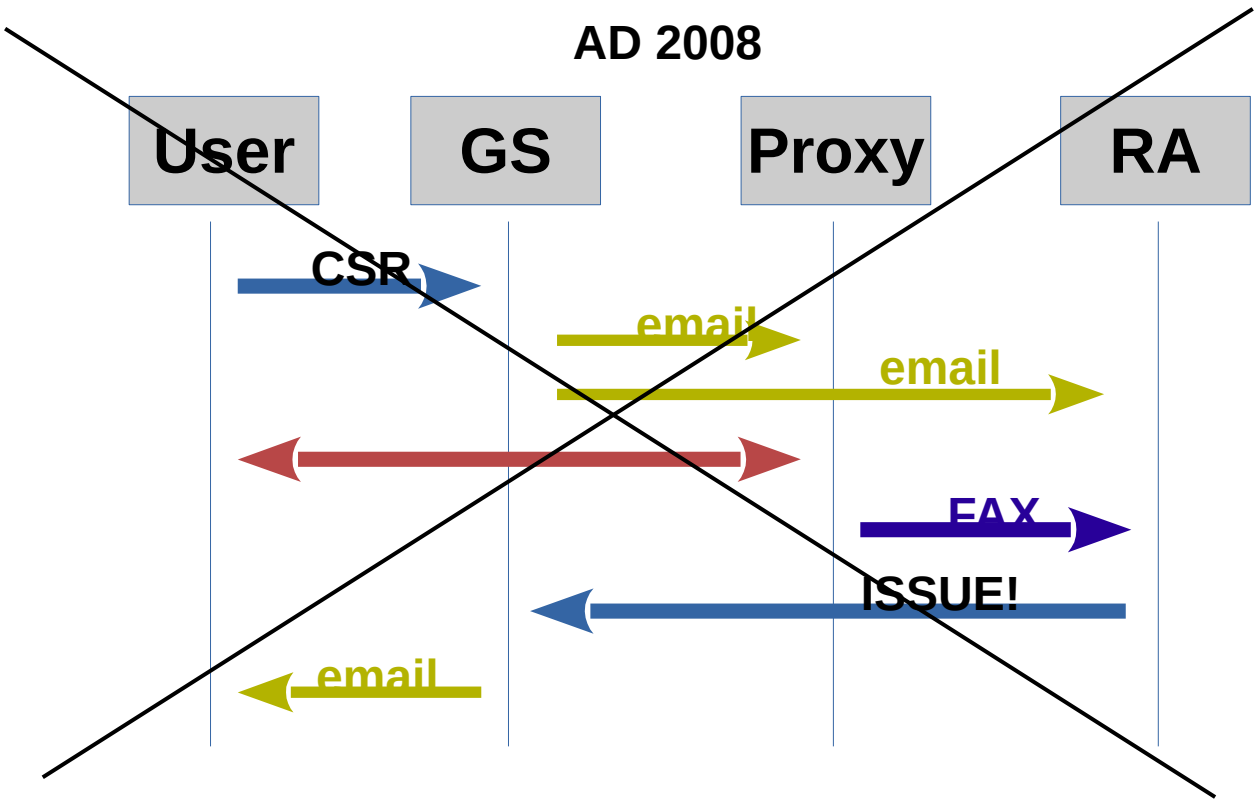
HBONE Workshop
2015. november 18.

TCS koncepció

- Szabaduljunk meg a tanúsítványokkal kapcsolatos figyelmeztetésektől
- Használjunk megbízhatónak tekintett CA-kat akadémiai környezetben
- Terena / GÉANT szerződést köt egy világszerte ismert CA-val, az NIIFI szerződést köt a GÉANT-tal, az intézmény szerződést köt a NIIFI-vel

Történelem

- **GlobalTrust** (2008-2010)
  - Csak szervertanúsítvány
  - Központosított működés
- **Comodo** (2010-2015)
  - Néhány más típus, külön nemzeti előfizetéssel
  - Nemzeti portál , de központi beavatkozást nem igényel
- **DigiCert** (2015-)



Újdonságok a DigiCert szolgáltatásában

- Közvetlen kapcsolat a CA és az intézmény között
  - Az intézmények közvetlenül a DigiCert portálján keresztül nyújthatják be az igényeiket
  - A domain és az intézmény validálását a DigiCert végzi
  - Az adminisztrátorok és a felhasználók kijelölését az első kijelölt adminisztrátor végzi
- Nem csak egyszerű szervertanúsítványok
  - Extended Validation
  - Grid tanúsítványok: kliens/szerver
  - Személyes tanúsítványok
  - Hivatalos dokumentum-aláíró tanúsítványok
  - Code Signing tanúsítványok
  - SAML azonosítás (személyes tanúsítványokná

Szerződés és problémái

- Technikailag közvetlen kapcsolat az intézmény és a CA között
- Jogilag ugyanez: Intézmény → NIIFI → Géant → DigiCert
- NIIF **nem** tanúsítványszolgáltató
  - nem tud felelősséget vállalni sem az intézmény, sem a DigiCert tevékenységéért
- DigiCert előírt felhasználási feltételek szerződéses elfogadtatását várja el
  - 1. melléklet
  - CPS
  - CA Browser Forum Extended Validation Guidelines
- Szerződés nélkül nem hozhatunk létre intézményi fiókot

Használat lépésről lépésre

- NIIF létrehozza az intézményt és az első adminisztrátor hozzáférését
- Az adminisztrátor jelszót generál magának, további adminisztrátorokat hív meg, hozzáférési szabályokat állít be
- Szervezet létrehozása és validálás kérése
- Domainek hozzáadása és validálás kérése
  - Domain validáció: validációs e-mail 7 fix e-mail címre (admin, administrator, hostmaster, postmaster, whois contact)
  - Aldomaineket nem kell külön validálni
- Igénylés (nem-SAML):
  - User (vagy admin) jogú felhasználó benyújt tanúsítvány igénylést
  - Admin jogú felhasználó jóváhagyja az igénylést

Számlázás

- Jelentősen átalakult a termékek köre és – sajnos – a NIIFI által fizetendő éves díj is
- Darabárak:
  - Szerver tanúsítvány: 7 ezer Ft/év
  - Személyes: 5 ezer Ft/év
  - Extra: 30 ezer Ft/év
- Két független díjplafon (flatrate)
  - Szervertanúsítványokért (kivéve wildcard) fizetendő max. éves díj 240 ezer Ft
    - EV szerver is beletartozik!
  - Személyes tanúsítványokért fizetendő max. éves díj 240 ezer Ft
  - Nem tartozik flatrate alá: Document Signing, Code Signing, WildCard

Tömeges tanúsítványváltási igény

- Heartbleed (2014. április)
- SHA1 deprecation
  - SHA1 tanúsítványok már most figyelmeztetést generálnak a Google böngészőiben
  - a Microsoft és a Mozilla eredetileg 2017-től tervezte, hogy nem fogadja el az SHA1 tanúsítványokat
  - újabb kutatások szerint már 2016-ban lehetséges lesz elérhető számítási kapacitással SHA1 ütközést ***generálni***, azaz tanúsítványt hamisítani, ezért a böngészők valószínűleg előrehozzák a váltás kikényszerítését
  - A Comodo lemaradt ebben a folyamatban, 2014 decemberében váltotta le a hibás köztes CA-t, így a Heartbleed során megújított tanúsítványok cserére szorulnak

https://wiki.niif.hu/TCS

GÉANT

Networks · Services · People

www.geant.org

This work is part of a project that has applied for funding from the European Union's Horizon 2020 research and innovation programme under Grant Agreement No. 691567 (GN4-1).