Videotechnológiás azonosítás

Lehetőségek, kockázatok, mellékhatások

Paulik Tamás
PKI szakértő
Microsec zrt.
paulik.tamas@microsec.hu

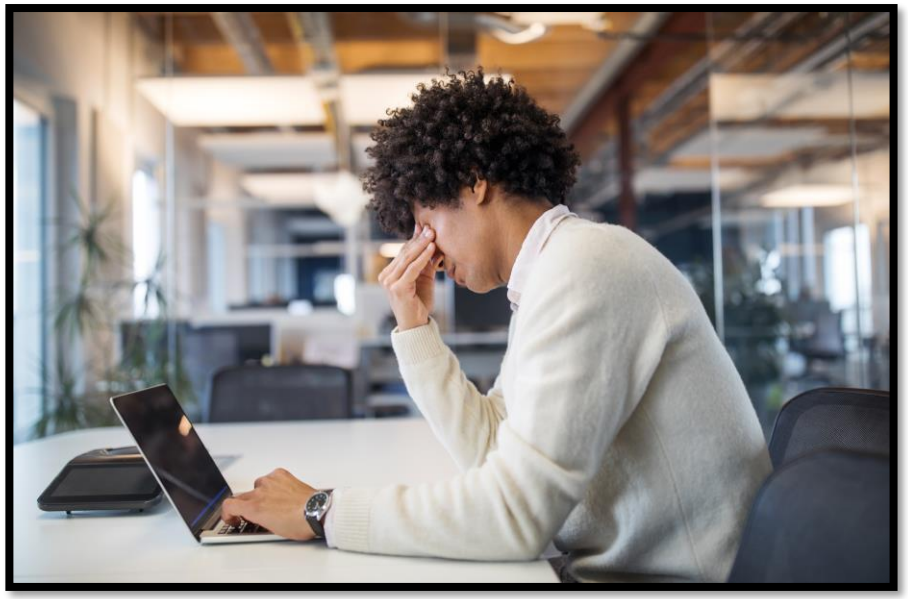
EURÓPAI CYBER-BIZTONSÁGI HÓNAP

A videoazonosításról általában

- Bizalmi szolgáltató (pl. elektronikus aláírások tanúsítványát kibocsátó szolgáltató) meg kell győződjön arról, hogy a megfelelő személynek állítja ki a tanúsítványt → személyazonosítás
- Az Európai Unióban a bizalmi szolgáltatásokról a 910/2014/EU rendelet (röviden: eIDAS rendelet) szól, amelyben a személyazonosítás (egyelőre) nem bizalmi szolgáltatás, hanem kapcsolódó tevékenység
- a személyazonosítás szempontjából az eIDAS négyféle lehetőséget ad:
  - A) Személyes jelenlét
  - B) eIDAS 8. cikk szerinti azonosítási rendszer (eID)
  - C) Minősített elektronikus aláírás A) vagy B) szerint kibocsátott tanúsítványa
  - D) nemzeti szinten elismert egyéb azonosítási módszerek (pl. videotechnológia)

Problémák a „hagyományos” metódusokkal

- Mindegyik eddigi lehetőség rendelkezik bizonyos korlátokkal
  - A) Személyes jelenlét
    - Kényelmetlen, az ügyfélnek el kell jutnia az irodához
    - Külföldi ügyfelek esetén szinte megoldhatatlan
  - B) eIDAS 8. cikk szerinti azonosítási rendszer (eID)
    - Magyarország nem rendelkezik bejelentett eID rendszerrel
  - C) Minősített elektronikus aláírás A) vagy B) szerint kibocsátott tanúsítványa
    - Használható lenne külföldi ügyfelek esetén, de ritka a sikeres azonosítás
    - Az elektronikus aláírás maga is minősített kell legyen, tehát nem elég hozzá minősített tanúsítvány, hanem MALE eszköz is szükséges
    - A bizalmi szolgáltatónak ellenőriznie kell, hogy a tanúsítvány valóban A) vagy B) szerint lett kiadva – Hogyan?
      - Tanúsítványból általában nem derül ki
      - Másik bizalmi szolgáltató szabályzatát kell elolvassa → Csak akkor jó, ha a másik szolgáltató vagy csak személyesen azonosít, vagy az adott tanúsítványtípusnál leírja, hogy személyes találkozás során került kibocsátásra



A videoazonosításról általában

- 2020 előtt Magyarországon csak az A), B) és C) pontok szerinti azonosítás volt megengedett
  - Versenyelőnyben voltak azok a külföldi szolgáltatók, ahol engedélyezett volt a videós azonosítás
- COVID-19 hatására rengeteg minden kerül át a digitális térbe, fontos személyes kontaktus csökkentése → itt is alkalmazható
- 541/2020. (XII. 2.) Korm. rendelet: engedélyezi a videoazonosítást
- NEM Pmt. szerinti átvilágítás! (pl. lakcím bekérése nem feltétlenül történik meg, jogi személynél fő tevékenység nem kerül rögzítésre stb.)
- Magyar e-személyi leolvasása sem videoazonosítás

Az ETSI szerepe

- ETSI = European Telecommunications Standards Institute = Európai Telekommunikációs Szabványintézet
- A bizalmi szolgáltatások tárgykörében az ETSI TC ESI (Electronic Signatures and Infrastructures Technical Committee) dolgozza ki és tartja naprakészen a releváns szabványokat
- Rengeteg eIDAS-aspektus szabványosításra került az ESI által, viszont a személyazonosítás témaköre mindeddig „érintetlen” volt
- 2020. 04. – STF (szakértői munkacsoport) megalakítása egy személyazonosításról szóló specifikáció és egy jelentés elkészítésére

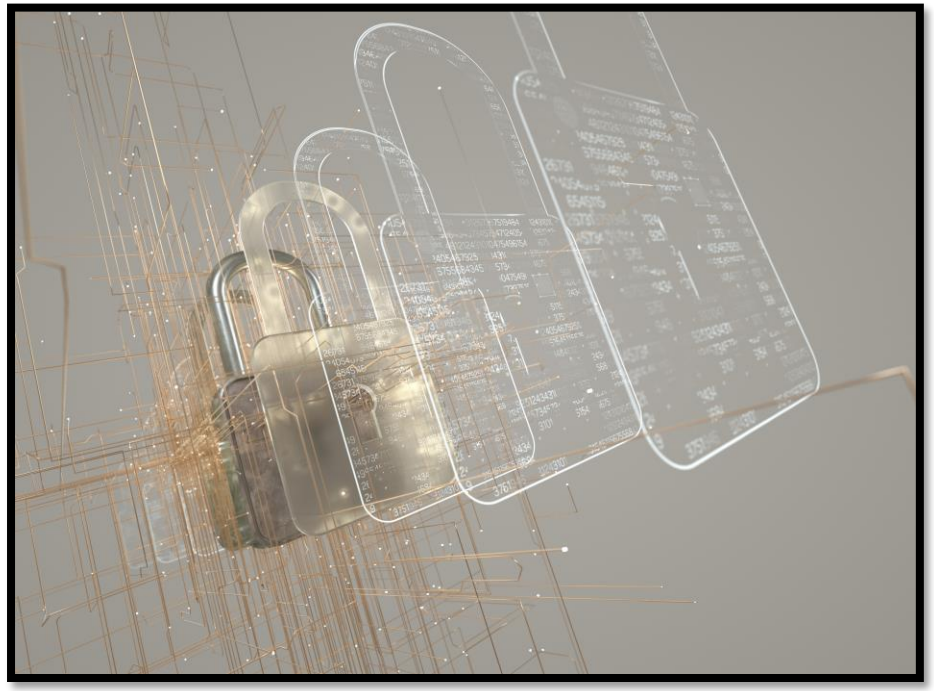
ETSI TS 119 461

- A munkacsoport legfontosabb eredménye az ***ETSI TS 119 461*** *-Policy and security requirements for trust service components providing identity proofing of trust service subjects* specifikáció megalkotása
- Technológiafüggetlen módon részletezi az eIDAS (és a hasonló keretrendszerek) szerinti bizalmi szolgáltatásokra vonatkozó azonosítás a lehető legszélesebb körben

Hogyan végezhető videoazonosítás?

- Nem bizalmi szolgáltatás → nem csak bizalmi szolgáltató végezheti, outsource-olható külső szolgáltatónak
- Az ETSI specifikáció különböző forgatókönyveket állít fel:
  - Személyes jelenléttel történő azonosítás
  - eID autentikációs azonosítás
  - Digitális aláírás tanúsítvánnyal
  - **Valós idejű távoli azonosítás**
    - Manuális
    - Hibrid
    - Automatizált
  - **Nem-valós idejű távoli azonosítás**
    - Manuális
    - Hibrid
    - Automatizált

Mennyire biztonságos?



- Valós idejű azonosítás általánosan biztonságosabb
- Nem-valós idejű esetén további biztonsági metrikák – pl. véletlenszerű „kihívások” kellenek → az eredményt utólag ellenőrizni kell!
- A TS 119 461 dokumentum B melléklete több támadási formát, és az ellenük alkalmazandó intézkedéseket is tartalmazza

Mennyire biztonságos?

- Fontos kérdések:
- A kamera és a sávszélesség mennyire kell jó minőségű legyen? Jelenthet ez korlátot az azonosításban?
  - Jellemzően nem jelent korlátot; átlagos okostelefon (min. 2 Mpixel kamera) és sávszélesség (min. 1,5 Mbps) általában elegendő
- Azonosítás során lehet-e problémás a biztonsági elemek ellenőrzése átlagos felbontással?
  - Manuálisan lehet kevésbé alapos, mint a fizikai ellenőrzés, viszont megoldás az algoritmikus segítség (pl. MI-technológia) alkalmazása

Néhány támadás és ellenintézkedés

Támadás	Ellenintézkedés
Fantáziadokumentumok bemutatása [T_DOC_FANTASY]	Autoritatív információforráshoz való hozzáférés (pl. PRADO), biztonsági elemek ellenőrzése
MI-generált videó az azonosított arca helyett [T_FACE_AI]	Élővideó-detektálás, *presentation attack* felismerése, deepfake elleni technológia
Kép bemutatása az eredeti dokumentum helyett [T_DOC_IMAGE]	A fénykép nem elfogadható bizonyítéktípus, videó szükséges helyette
Hamisított dokumentumok [T_DOC_FAKE]	Biztonsági elemek vizsgálata kötelező, hibrid megoldás ajánlott
Eljárásbeli/policy hiba [T_POLICY_FLAW]	A szolgáltatónak ismernie kell az adott azonosítási kontextust, követelményeket

A videoazonosítás előnyei és hátrányai

- Kényelmes, nem szükséges hozzá fizikailag is eljutni a szolgáltatóhoz
- COVID-fertőzésveszély teljes elkerülése
- Fontos a megfelelő, biztonságos működés – szoftveres, policy stb. követelmények → megfelelőség-értékelés kiemelt szerepe

A videoazonosítás jövője

- 2020 július – elindult az eIDAS rendelet felülvizsgálata
- 24. cikk tervezett módosítása:

  „(1a) E rendelet hatálybalépésétől számított 12 hónapon belül a Bizottság végrehajtási jogi aktusok útján a személyazonosság és az attribútumok ellenőrzése tekintetében minimális műszaki előírásokat, szabványokat és eljárásokat állapít meg az (1) bekezdés c) pontjával összhangban. Ezeket a végrehajtási jogi aktusokat a 48. cikk (2) bekezdésében említett vizsgálóbizottsági eljárással összhangban kell elfogadni.”;

  - Azaz: a TS 119 461 követelményei valószínűleg jogszabály által kötelezően alkalmazandók lesznek valamennyi bizalmi szolgáltató számára

A videoazonosítás jövője

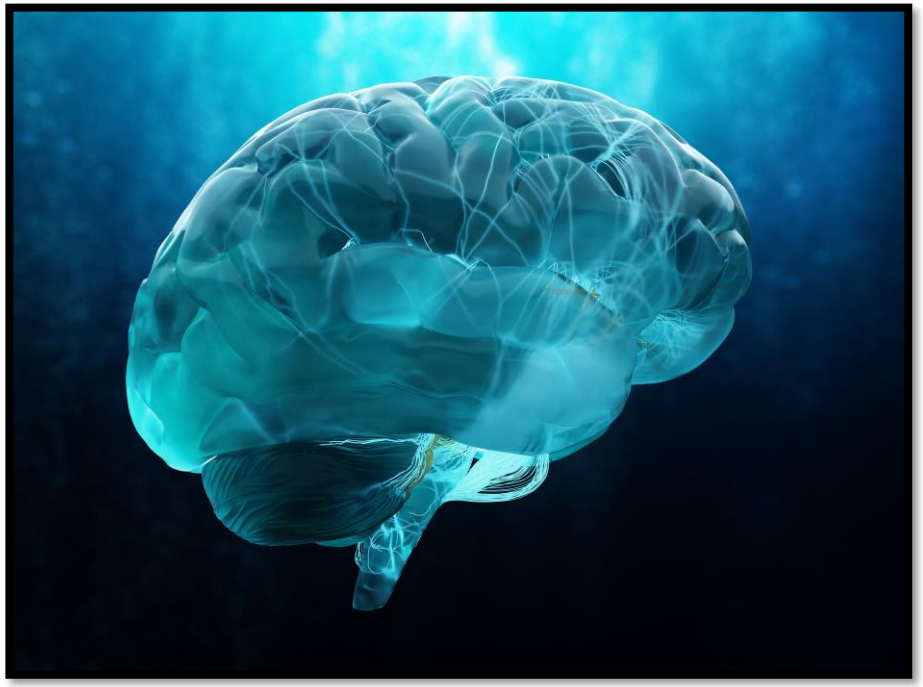
- *„Az (…) adatokat a minősített bizalmi szolgáltató közvetlenül vagy harmadik fél révén ellenőrzi az alábbi módok valamelyikén:*

  (…)

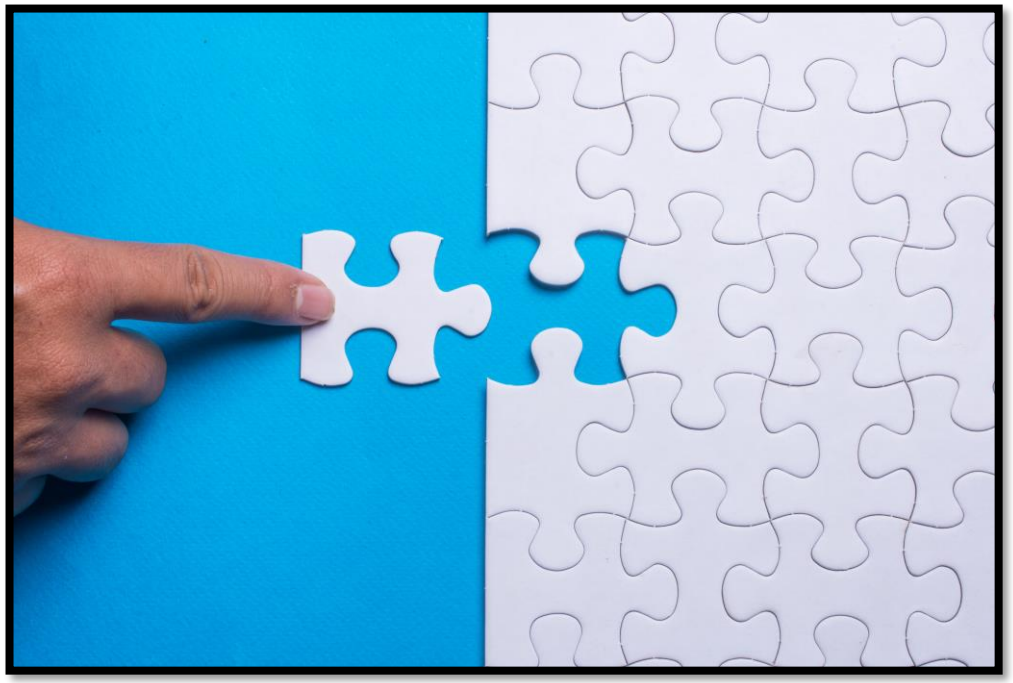
  b) minősített elektronikus attribútumtanúsítványokkal vagy minősített elektronikus aláírás vagy minősített elektronikus bélyegző a), ***c)*** *vagy d) ponttal összhangban kibocsátott tanúsítványával;”*

- c) = videoazonosítás (változott a sorrend)

- Azaz: megoldódni látszik az aláírás alapján történő ellenőrzés egy része, mivel így nem csak személyesen vagy eID alapján kiadott tanúsítványokra érvényes, hanem videósra is, viszont probléma marad az ugyanígy, minősített aláírással kiadott tanúsítványok alapján való azonosítás lehetőségének hiánya



Konklúzió



- A videoazonosítás sokkal kényelmesebb, viszont nagyobb kockázatot is hordoz, mint a hagyományos, személyes azonosítás
- Fontos, hogy kellően biztonságosan működő szolgáltatót válasszunk, aki a megfelelő körültekintéssel jár el
- Fontos, hogy nemzetközi (legalábbis EU) szinten egységes, egyértelmű követelmények legyenek megfogalmazva a szolgáltatókra nézve – ETSI, ill. eIDAS-módosítás szerepe

Köszönöm a figyelmet!

Paulik Tamás

PKI szakértő

Microsec zrt.

paulik.tamas@microsec.hu

EURÓPAI CYBER-BIZTONSÁGI HÓNAP