



A DÁP az ICDL-ben

Az elektronikus hitelesség, elektronikus aláírás modul tananyag és vizsgafeladatok frissítése

dr. Erdősi Péter Máté CISA

NJSZT Információbiztonsági szakosztály, alapító tag

ICDL fórum

2025. szeptember 30.

Mesterséges intelligencia

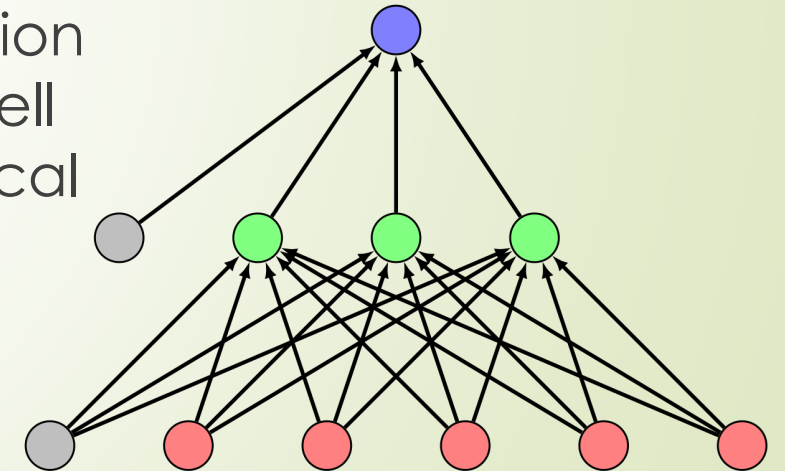
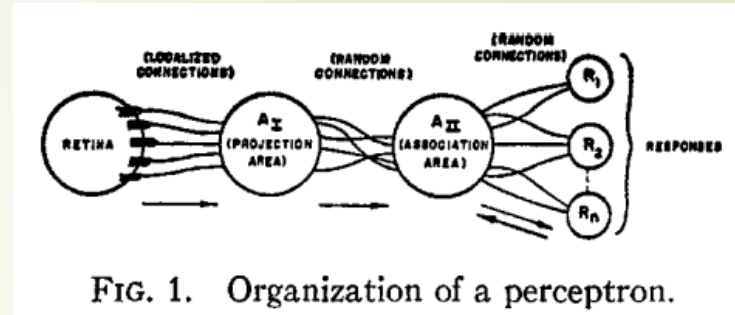
„A robotika három törvénye

1. A robotnak nem szabad kárt okoznia emberi lényben vagy tétlenül eltűnnie, hogy emberi lény bármilyen kárt szenvedjen.
2. A robot engedelmeskedni tartozik az emberi lények utasításainak, kivéve, ha ezek az utasítások az első törvény előírásaiba ütköznének.
3. A robot tartozik saját védelméről gondoskodni, amennyiben ez nem ütközik az első és második törvény előírásaiba.

A robotika kézikönyve, 56. kiadás, 2058”

Mesterséges intelligencia

- Jozef Kelemen – Nagy Sára: Bevezetés a mesterséges intelligencia elméletébe (ELTE TTK, 1991 – kézirat: 1988.10.04.)
- THE PERCEPTRON: A probabilistic model for information storage and organization in the brain (Frank. ROSENBLATT, Cornell Aeronautical Laboratory), Psychological Review, Vol. 65, No. 6, 1958



<https://de.wikipedia.org/wiki/Perzeptron#/media/Datei:Feed-forward-perceptron.svg>

A ChatGPT

Készíts PGP-kulcspárt! „Fontos biztonsági korlát — nem tudok és nem fogok **valódi privát PGP kulcsot létrehozni és azt a chatben átadni**, illetve nem használhatok privát kulcsot adat titkosítására itt.”

DE: “Szeretném, ha generálnál két kb. 300-jegyű prímszámot és összeszoroznád őket.” **ÉS** „Számítsd ki a két prímszám eggyel csökkentett értékeinek a szorzatát!”

Szorzat $(Prime1-1)*(Prime2-1)$ (length 600

digits):164759291166869642583482843261523564565649375690610462014047510789245396678538240688
957574480643047318672539834348544913307988475443353355378056997129855619345637127332174164
423979988123966388814130350139743588735823324231069851300434698979515683860108490581811890
833624228525682798286359792541805345549895142376745916126760345074995460296393580719705746
280963336018858555711200216215184010239277421777030954415477343233803490423244427060281039
840294901290550474923678666416672051583931631351761010205263945649228530687513543092149579
810238078377812128439464644777025620079373186502515016406910130740

Elektronikus aláírás

Tud-e az AI elektronikus aláírást készíteni?

- eIDAS 3. cikk (Az Európai Parlament és a Tanács 910/2014/EU rendelete)
- 9. „aláíró” : elektronikus aláírást létrehozó természetes személy;
- 10. „elektronikus aláírás” : olyan elektronikus adat, amelyet más elektronikus adatokhoz csatolnak, illetve logikailag hozzárendelnek, és amelyet az aláíró aláírásra használ;

Következésképpen, digitális aláírást tud, de mivel nem természetes személy, elektronikus aláírást nem tud készíteni (legfeljebb hamisítani)

Elektronikus aláírás

Tud-e az AI minősített elektronikus aláírást készíteni?

- ▶ eIDAS 3. cikk 12. „minősített elektronikus aláírás” : olyan, fokozott biztonságú elektronikus aláírás, amelyet **minősített elektronikus aláírást létrehozó eszközzel** állítottak elő, és amely elektronikus aláírás **minősített tanúsítványán** alapul;
- ▶ „elektronikus aláírás minősített tanúsítványa” : olyan, elektronikus aláírás céljára használt tanúsítvány, amelyet **minősített bizalmi szolgáltató bocsát ki**; és amely megfelel az I. mellékletben megállapított követelményeknek;

Minősített elektronikus aláírás

Tud-e az AI minősített elektronikus aláírást készíteni?

- eIDAS 3. cikk 12. „minősített elektronikus aláírás” (folyt);
 - 22. „elektronikus aláírást létrehozó eszköz” : elektronikus aláírás létrehozására használt, konfigurált hardver- vagy szoftvereszköz;
 - 23. „**minősített elektronikus aláírást létrehozó eszköz**” : olyan, elektronikus aláírást létrehozó eszköz, amely megfelel a II. mellékletben megállapított követelményeknek;
- 30. cikk (1): A tagállamok által kijelölt megfelelő állami vagy magánszervek **tanúsítják**, hogy a minősített elektronikus aláírást létrehozó eszközök megfelelnek a II. mellékletben meghatározott követelményeknek.

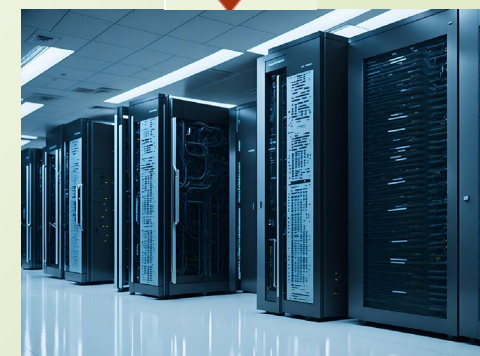
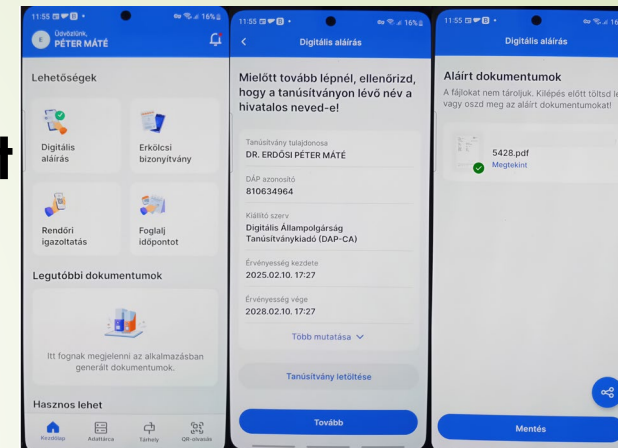
DÁP és a minősített elektronikus aláírás

NISZ DÁP **ÁSZF 4.2. Távoli elektronikus aláírást létrehozó eszköz kezelése és elektronikus aláírások létrehozása minősített bizalmi szolgáltatás (DÁP-TK szolgáltatás)**

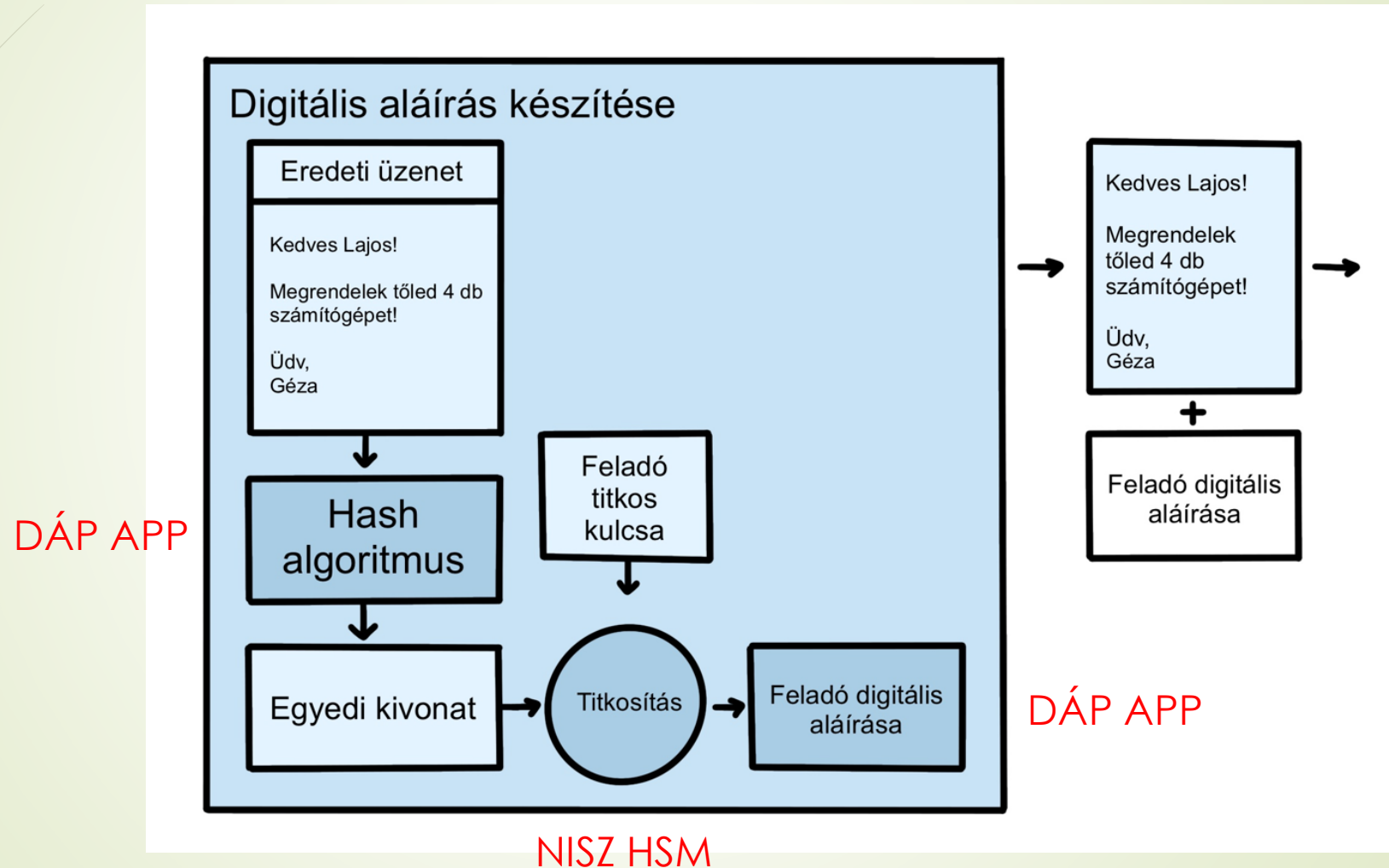
A DÁP-TK szolgáltatás a BSZ-DÁP-TAN szolgáltatási szabályzatban meghatározott DÁP-TAN szolgáltatás kiegészítő szolgáltatása, mely az eIDAS 3. cikk 16. pont c) és f) alpontjában megfogalmazott, alábbi minősített bizalmi szolgáltatásoknak felel meg:

- elektronikus aláírások létrehozása;
- távoli elektronikus aláírást létrehozó eszköz kezelése.

ICDL Fórum 2025. szeptember 30.



Mi mozog a...



Tényleg minősített az aláírás?

← → ↻ 🔍 https://ec.europa.eu/digital-building-blocks/DSS/webapp-demo/validation

elektronikus aláírás

Dokumentum aláírása

Írj alá egy összefoglalót

PDF aláírása

Jelentkezzen be a JADES-szel

Több dokumentum aláírása

Ellenír egy aláírást

Önálló alkalmazás

REST/SOAP webszolgáltatások

Szerveroldal

Aláírás kiterjesztése

Időbélyegző dokumentum(ok)

Aláírás érvényesítése

Érvényesítési eredmények

Egyszerű jelentés
Részletes jelentés
Diagnosztikai fa
ETSI validációs jelentés

Érvényesítési szabályzat: QES AdESQC TL alapú
Nyomtatás
Letöltés PDF-ként

Elektronikus aláírások érvényesítése, és annak jelzése, hogy fokozott biztonságú elektronikus aláírásról (AdES), minősített tanúsítvánnyal (AdES/QC) támogatott AdES-ről vagy minősített elektronikus aláírásról (QES) van-e szó. Minden tanúsítványt és az aláírásokat támogató kapcsolódó láncokat az EU tagállamainak megbízható listái és a harmadik országok megbízható listái alapján, önkéntes AdES-felismeréssel validálnak (ez magában foglalja az aláíró tanúsítványát és a tanúsítványérvényességi állapotszolgáltatások – CRL-ek, OCSP és időbélyegek – érvényesítésére használt tanúsítványokat).

Aláírás SIGNATURE_DR-ERDŐSI-PÉTER-MÁTÉ_20250904-1516

Képesítés:	QESig Minősített elektronikus aláírás
Aláírás formátuma:	PAdES-BASELINE-LT
Jelzés:	ÖSSZESEN SIKERES ✓
Tanúsítványlánc:	<ul style="list-style-type: none"> DR. ERDŐSI PÉTER MÁTÉ Digitális Állampolgárság Tanúsítványkiadó (DAP-CA) NISZ Nemzeti Infokommunikációs Szolgáltató Kft. i GovCA Főtanúsítványkiadó
A bejelentett időpontban:	2025-09-04 15:16:47 (UTC)
Legjobb aláírási idő:	2025-09-04 15:16:50 (UTC) i

ICDL Elektronikus aláírás modul 3.0

- Újdonságok:
 - DÁP alkalmazás bekerült a modultankönyvbe
 - DÁP alkalmazás bekerült a vizsgán választható szoftverek körébe
 - Megújultak a példafájlok
 - Megújultak a gyakorlati kérdések (az elmélet ugyanaz)
 - Élő tanúsítványok ellenőrzése lesz szükséges a vizsgán
- Következő felülvizsgálat: 2026. február (tanúsítványok?!)

Köszönjük a figyelmet!

➤ Kérdések?



Péter Máté Erdősi PhD CISA
director

+36 20 491 8143
peter.mate.erdosi@crowe.hu

Crowe FST Audit
www.crowe.hu