MICROSEC

E-aláírás az eIDAS korában

Réti Kornél, Microsec Zrt.

Bemutatkozás

MICROSEC Zrt:

- Legkorszerűbb PKI alapú technológiák és megoldások szállítója
- 1984-ben alakult magyar tulajdonú cég
- 1998-tól foglalkozunk elektronikus aláírással
- 2005-től minősített hitelesítés-szolgáltató
- A European Telecommunications Standards Institute (ETSI) tagja

Az előadó: Réti Kornél, reti.kornel@microsec.hu

- Kutató-fejlesztő mérnök, a Microsecnél 2009. óta
- Elektronikus aláírással kapcsolatos szolgáltatási szakértő
- Tagi képviselő az ETSI Electronic Signatures and Infrastructures (ESI) műszaki bizottságában
- Személyes érdeklődés: biztonságos elektronikus kézbesítés

Tematika

- Hol találkozhatunk e-aláírással?
- Mi az a PKI?
- Hogyan használhatjuk az e-aláírást?
- Mik az aktuális újdonságok?
- Bemutatók élőben

Elektronikus aláírás

- Biztonsági szintek:
  - Egyszerű
  - Fokozott biztonságú
  - Minősített
- A fokozott biztonságú (és a minősített) aláírás
  - Egyértelműen az aláíró személyéhez köthető
  - Kizárólag az aláíró tudja létrehozni
  - Az aláírt adatok észrevétlenül nem módosíthatók
  - ➢ A kézzel írott aláíráshoz hasonló tulajdonságú
- A törvény szerint a minősített tanúsítványon alapuló aláírással ellátott dokumentum teljes bizonyító erejű magánokirat

E-ALÁÍRÁS ALKALMAZÁSAI

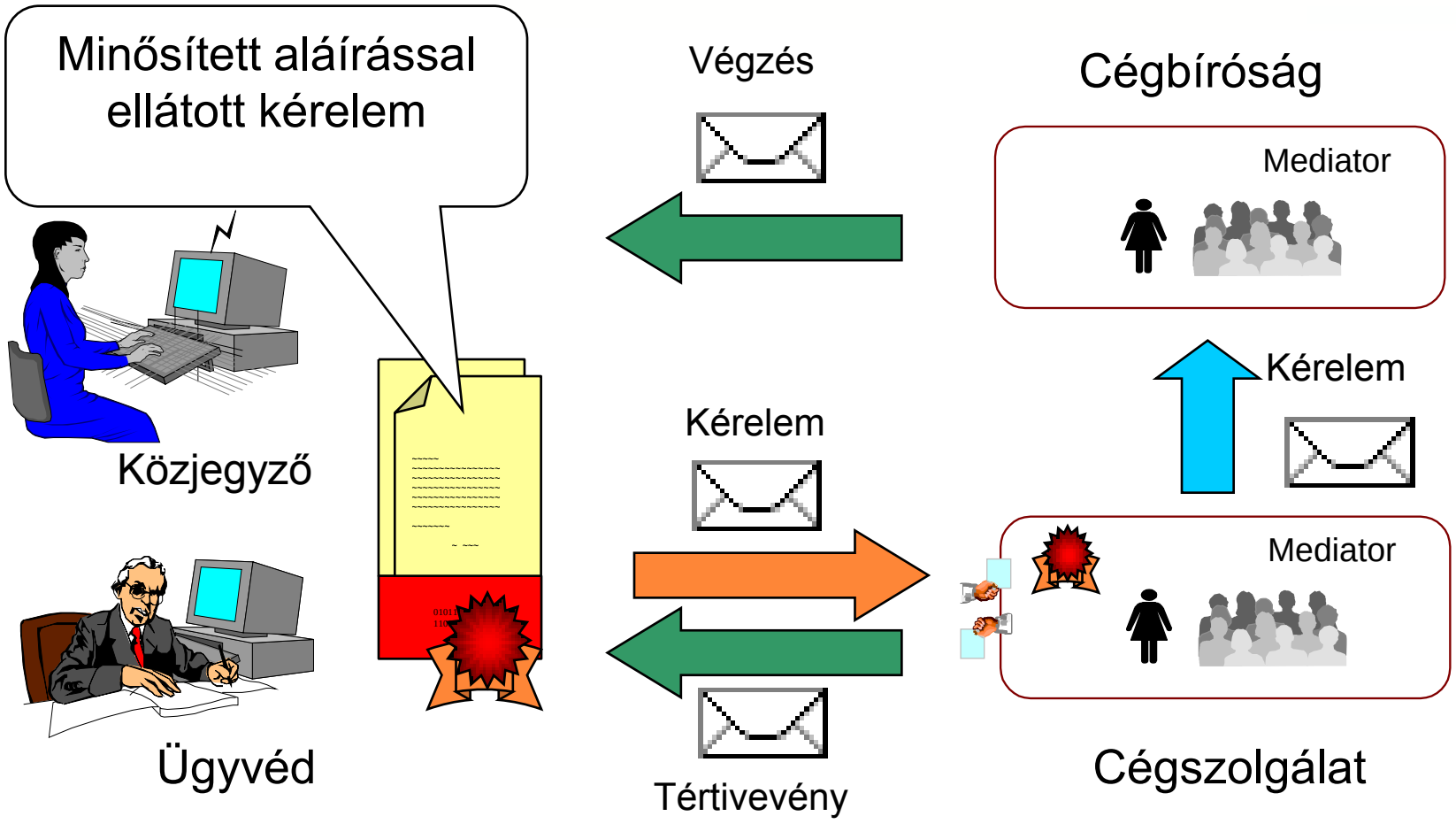
E-aláírás alkalmazásai

- Elektronikus számlázás
- Elektronikus cégeljárás, e-cégjegyzék
- Egyablakos ügyintézés (NAV + KSH + cégbíróságok közötti kommunikáció)
- Elektronikus archiválás
- Végrehajtási iratok kézbesítése, vagyonfelmérés
- Földhivatali tulajdoni lapok
- Elektronikus személyi igazolvány
- …

1) e-cégeljárás

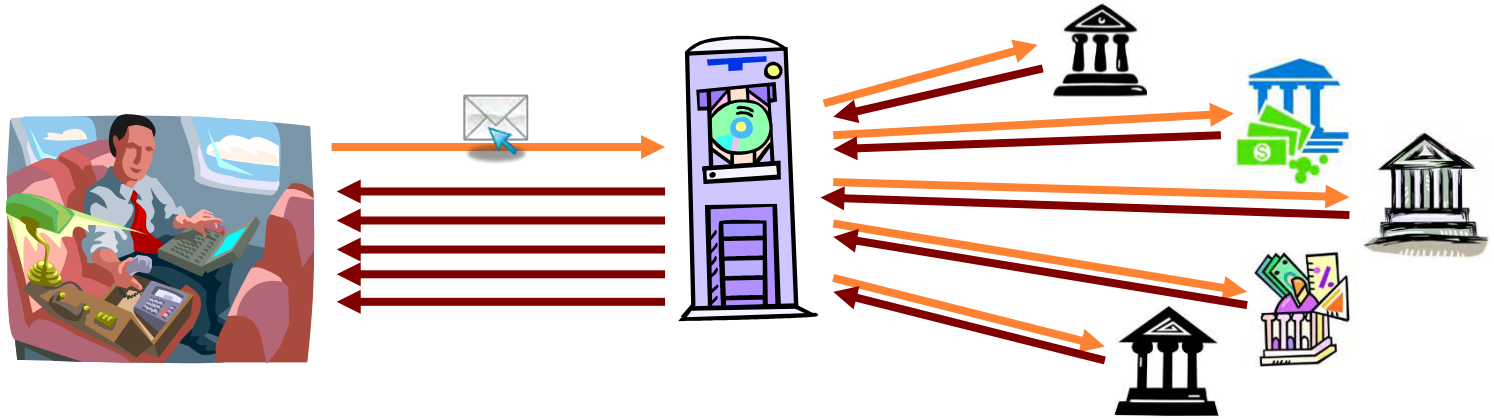
- Elektronikus ügyintézés fokozatos bevezetése:
  - 2005 – Kft. és Rt. bejegyezhető elektronikusan
  - 2006 – Valamennyi gazdasági társaság bejegyezhető e-úton
  - 2008 – Kötelező elektronikus eljárás. Formátuma: előre definiált sémájú XML nyomtatvány, mellékletek PDF-ben
  - Azóta – Egyre több szervezet kommunikál elektronikusan aláírt dokumentumokban a cégbíróságokkal (NAV, KSH, bankok...)
- A bejegyzési kérelmek elektronikusan (XAdES) aláírt e-akták, amit e-mailben küldenek be
- A cégbírósági végzések is elektronikusan (XAdES) aláírt e-akták, amit egy speciális kézbesítési rendszeren keresztül küldenek ki
- A cégnyilvántartás adatainak hitelességét az okirati bizonyítékok garantálják

1) e-cégeljárás



2) Hatósági megkeresések

- Microsec által fejlesztett e-kézbesítési rendszer
- Minden üzenet elektronikusan aláírt és titkosított
- Az üzenet átvételéről minden címzett elismervényt állít ki (aláírt elektronikus tértivevény)
- Kézbesítési vélelem egy adott határidő letelte után az át nem vett üzenetekre is beáll
  (a bírósági végrehajtásról szóló törvény teszi lehetővé)



2) Hatósági megkeresések

- Egyre több szereplő használja a rendszert:
  - Magyar Bírósági Végrehajtói Kamara ↔ pénzintézetek (2009-)
  - Magyar Bírósági Végrehajtói Kamara ↔ végrehajtást kérők (2011-) (VHKIR)
  - Magyar Bírósági Végrehajtói Kamara ↔ végrehajtási ügyekben érintett felek (2012-) (VIEKR)
  - Cégbíróságok ↔ pénzintézetek (2014-) (CEVR)

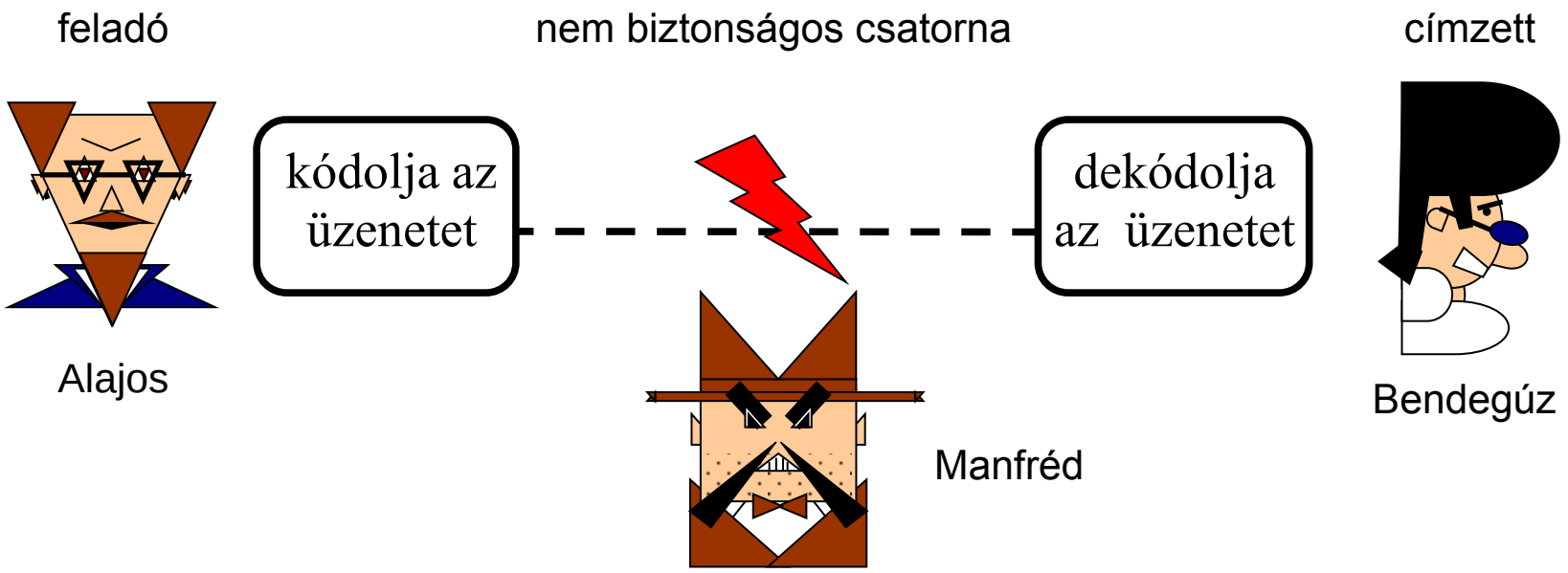
- Statisztikák:
  - Havi kb. 460 000 kézbesített irat (2016-os átlag)
  - 70-90% megtakarítás a papír alapú folyamatokhoz képest
  - Több mint 40 MFt/hó megtakarítás a résztvevő felek számára együttesen

MICROSEC

A NYILVÁNOS KULCSÚ INFRASTRUKTÚRA (PKI)

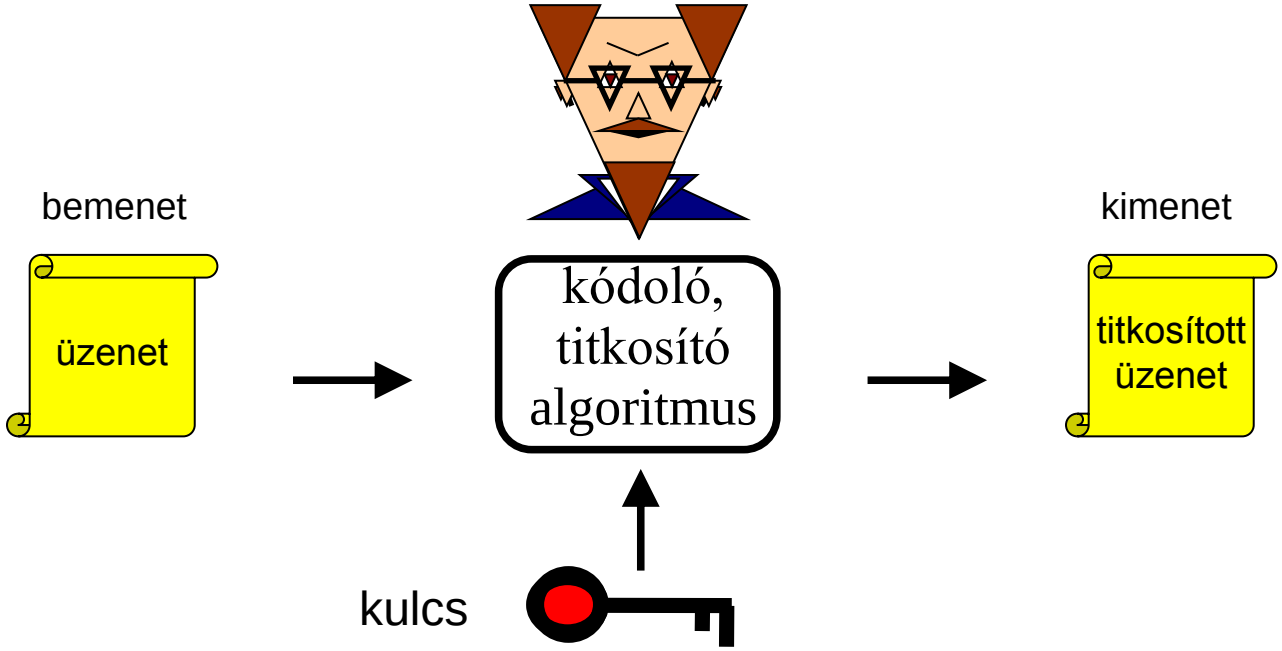
Kriptográfia fogalma

- Számítógépen tárolt, kezelt vagy küldött információk biztonságát kriptográfiai módszerekkel (kódolással) biztosíthatjuk
- A kriptográfia a titkosírásokkal, rejtjelezésekkel és ezek megfejtésével foglakozó tudományág



A kulcs

- A kódolásnak a gyakorlatban mindig két paramétere van: egy üzenet és egy kulcs
- A kódolásnak akkor is biztonságosnak kell lennie, ha a támadó ismeri a kódolási módszert, kivéve a kulcsot!
- A kódoló algoritmus nyilvános, csak a kulcsot kell titokban tartani

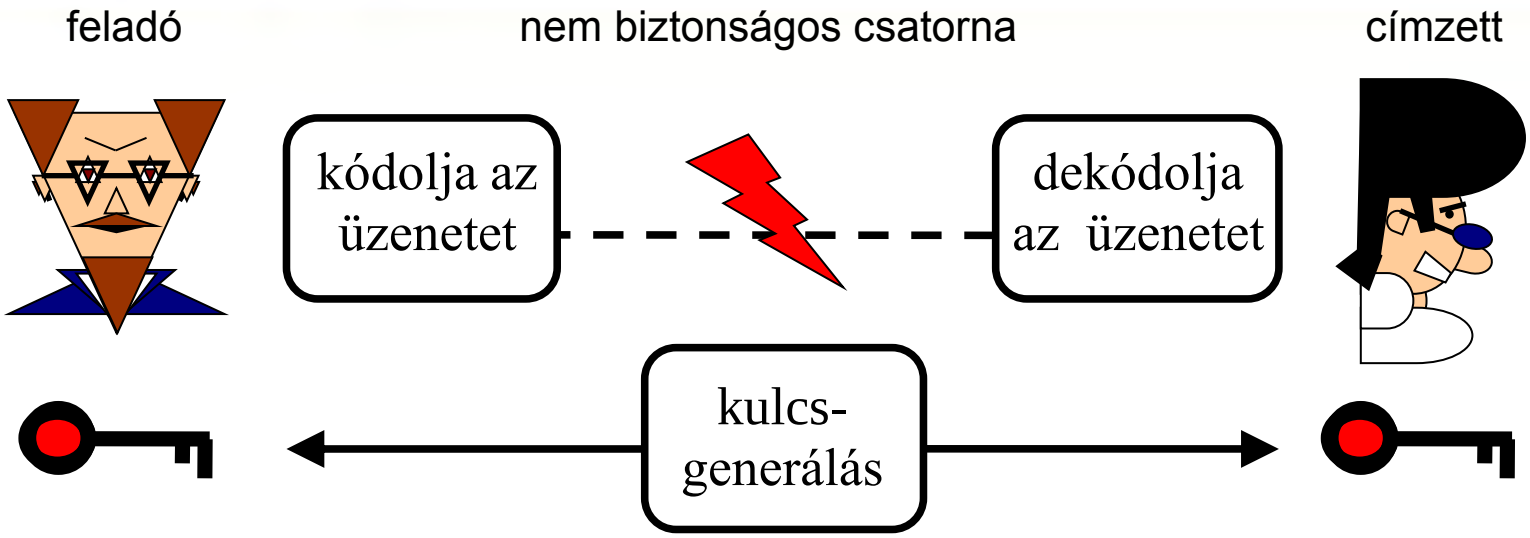


Két nagy terület

- Szimmetrikus kulcsú kriptográfia
  - angolul: symmetric key cryptography
  - kódolás és dekódolás ugyanazon kulccsal

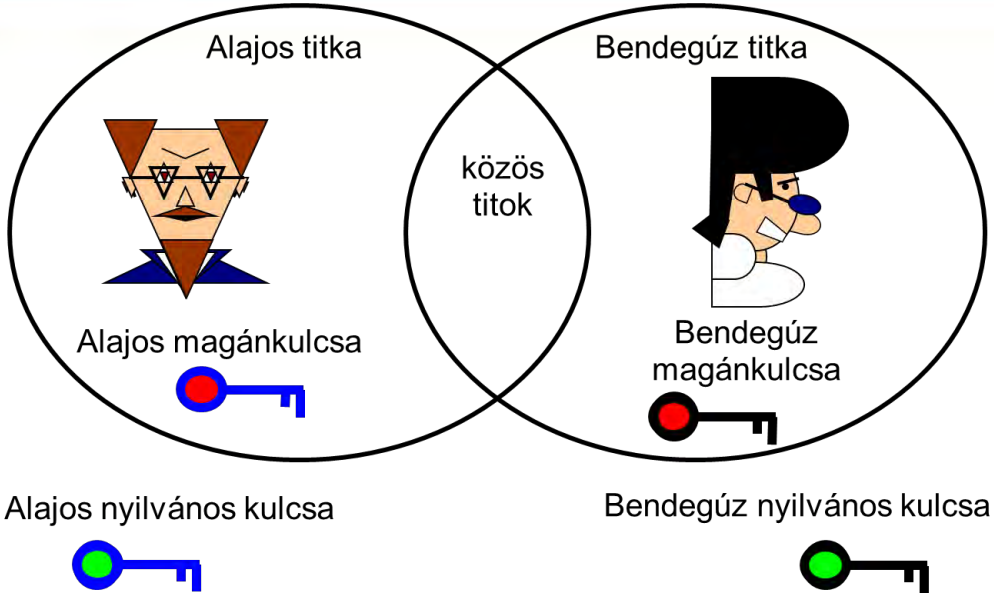
- Nyilvános kulcsú kriptográfia
  - más néven: aszimmetrikus kulcsú kriptográfia
  - angolul: public key cryptography
  - kódolás és dekódolás különböző kulccsal

Szimmetrikus kulcsú kódolás



- Kódoláshoz és dekódoláshoz ugyanazt a kulcsot használjuk.
- A kulcs az egymással kommunikáló felek **közös titka**.
- A kulcsban biztonságos csatornán kell megegyezniük. (kulcstovábbítás, kulcscsere)
- A **kulcsot** titkosan kell eljuttatnunk, nem szabad, hogy a támadó megismerje.

Aszimmetrikus kulcsú kódolás



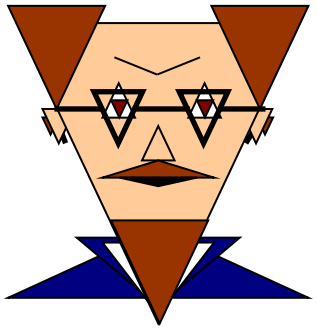
- Minden résztvevőnek van két kulcsa: **magánkulcs** (csak ő ismeri), **nyilvános kulcs** (bárki megismerheti)
- A két kulcs szorosan összetartozik. Amit az egyikkel kódolunk, csak a párjával fejthető vissza, és fordítva.
- A nyilvános kulcsot **hitelesen** kell eljuttatnunk

Titkosított üzenet küldése

feladó

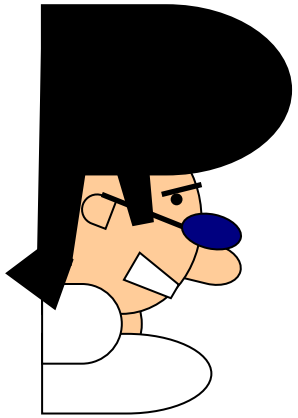
nem biztonságos csatorna

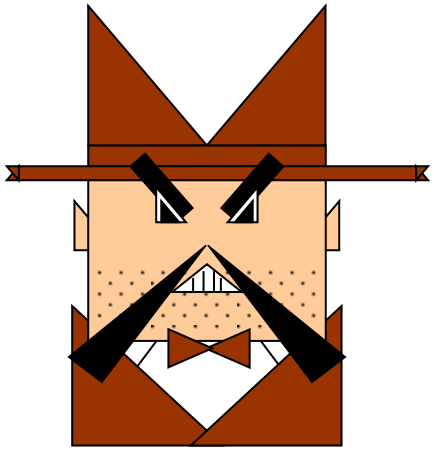
címzett



kódolja az üzenet

dekódolja az üzenet

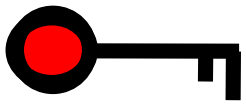




kódolás a címzett nyilvános kulcsával

„titkosítás”

dekódolás a címzett magánkulcsával



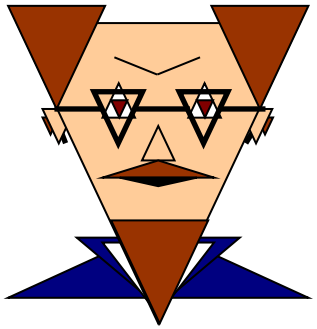
„visszafejtés” dekódolás

Aláírt üzenet küldése

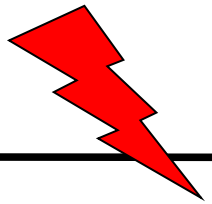
feladó

nem biztonságos csatorna

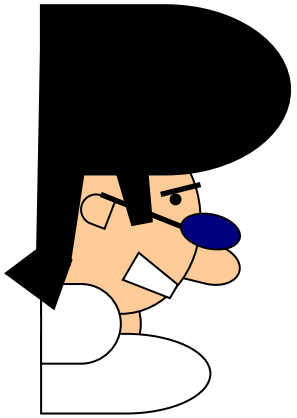
címzett

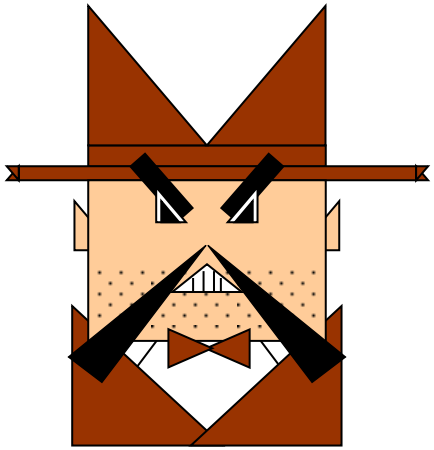


kódolja az üzenet

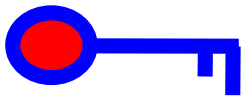


dekódolja az üzenet



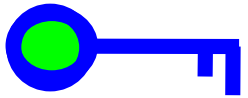


kódolás a feladó magánkulcsával



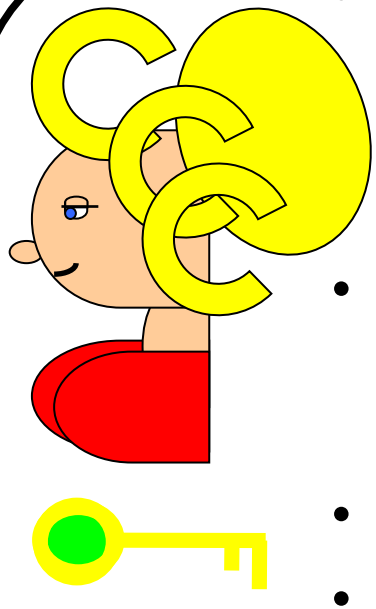
„aláírás”

dekódolás a feladó nyilvános kulcsával



„aláírás ellenőrzése”

Tanúsítvány



- Ez Cili nyilvános kulcsa, őnála van a hozzá tartozó magánkulcs.
- Ez a kulcs aláírások ellenőrzésére használható.
- …
- A fenti adatokat a Microsec ellenőrizte, és vállalja értük a felelősséget.

e-SZIGNÓ

- A hitelesítés-szolgáltató a saját magánkulcsával aláírja a tanúsítványt.
- A tanúsítvány ellenőrzéséhez a hitelesítés-szolgáltató nyilvános kulcsa kell.

PKI szolgáltatók

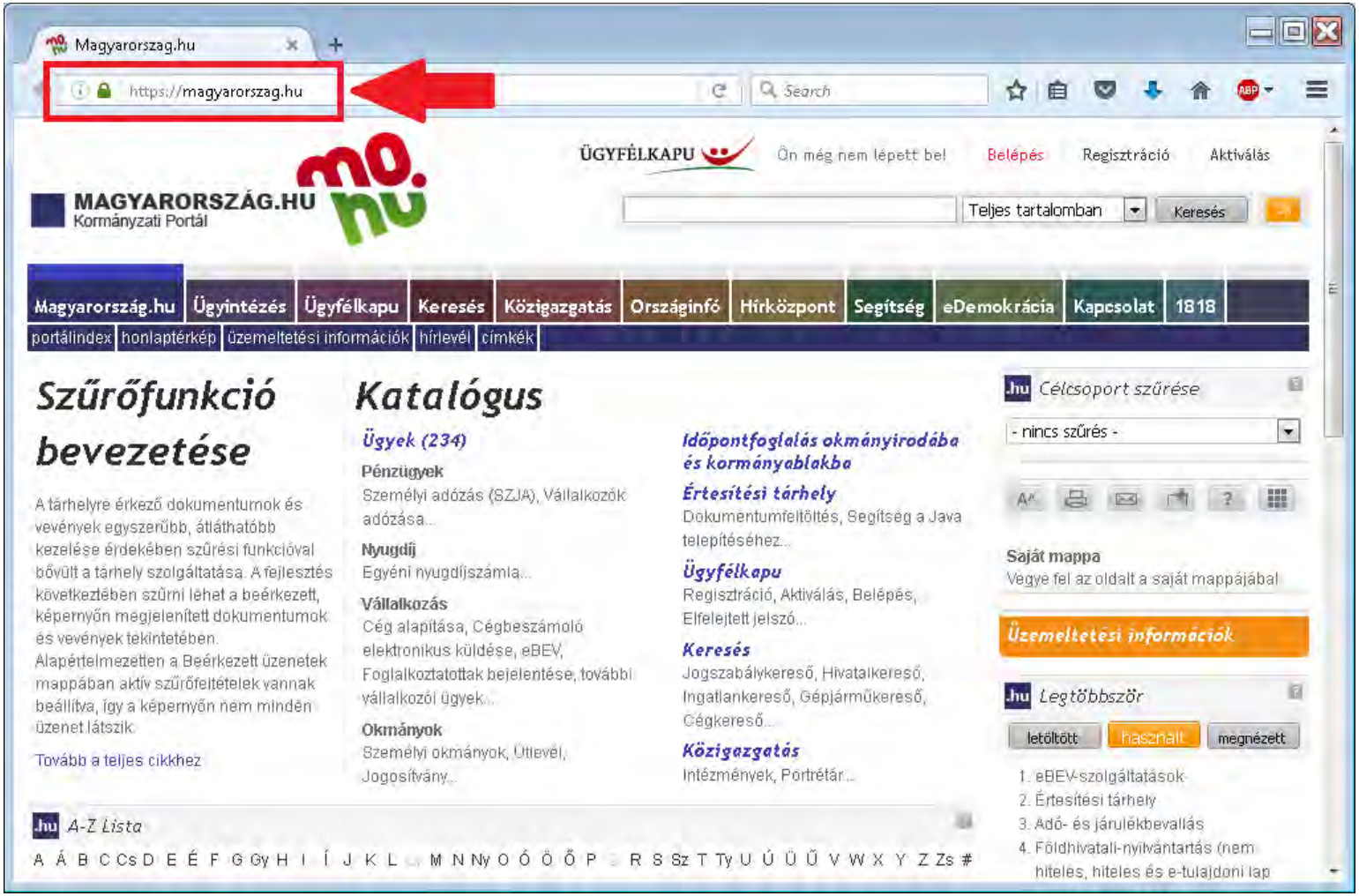
- A **hitelesítés-szolgáltató** olyan szervezet, amely tanúsítványokat bocsát ki, amelyben igazolja:
  - egy adott nyilvános kulcs egy adott személyhez tartozik,
  - a tanúsítványban feltüntetett adatokat ellenőrizte.
- A hitelesítés-szolgáltató biztonságos rendszert üzemeltet, hogy megbízható félként működhessen.
- A hitelesítés-szolgáltató mindezért felelősséget vállal,
- Szükség esetén visszavonja a tanúsítványt (pl.: adatváltozás esetén, vagy ha az ügyfél jelenti, hogy elvesztette a magánkulcsát)

- Az **időbélyegzés szolgáltató**k aláírt igazolásokat bocsátanak ki arról, hogy egy adott dokumentum egy adott időpontban létezett: időbélyeg.

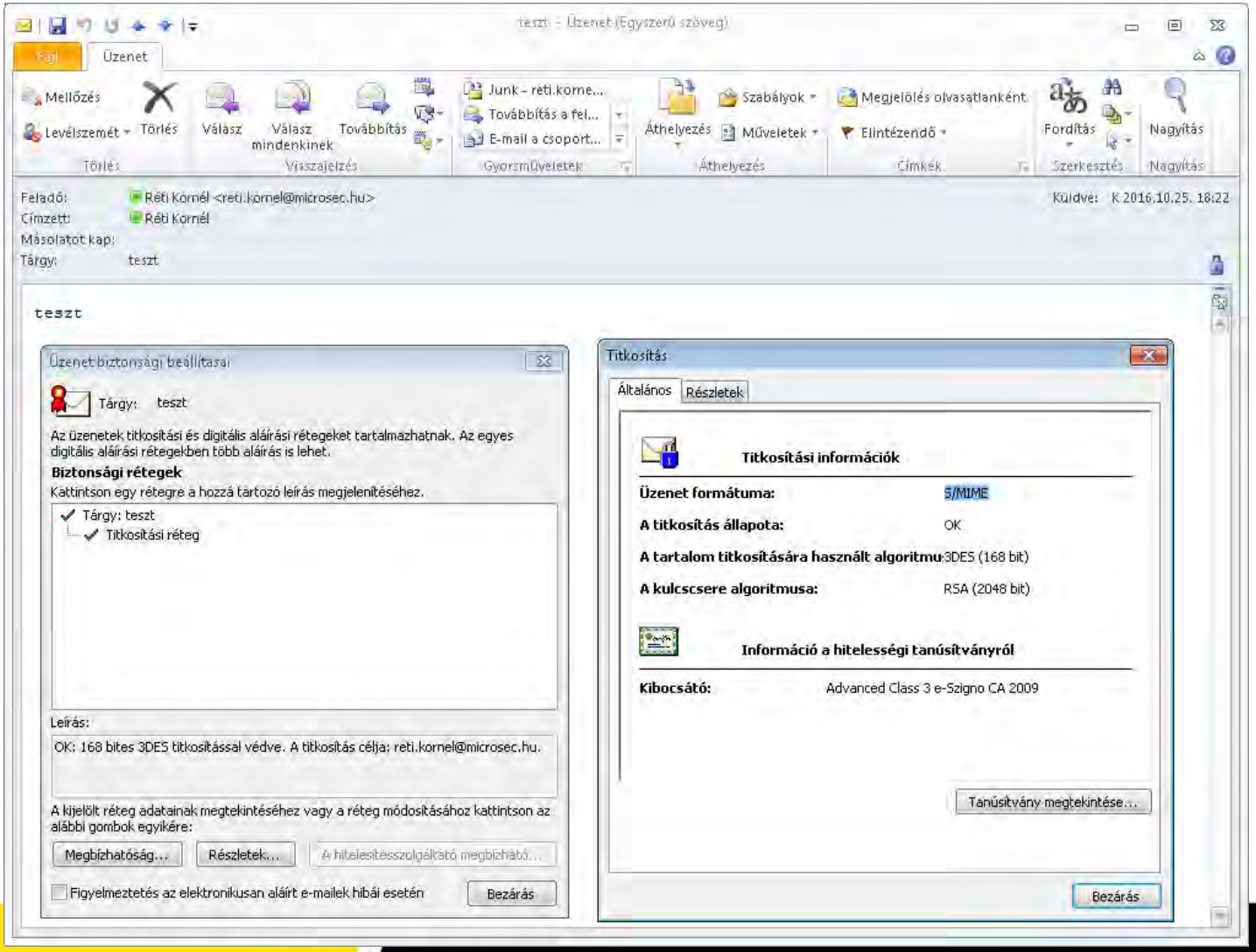
PKI további alkalmazásai

- SSL weboldal-hitelesítés
- Email titkosítás
- VPN, RDP, SSH, ...

MICROSEC PKI – SSL weboldal-hit.



PKI – email titkosítás



Azonosítás és aláírás

Azonosítás

- Jellemzően szinkron kommunikációban használjuk
  (pl. online, telefonon)
- Csak a kommunikáció során nyújt hitelességet
- A személyazonosságot csak a partner számára igazolja
- Hardvereszközt használunk a nagyobb biztonsághoz
- Előzetes regisztráció szükséges (pl. személyesen)

Aláírás

- Jellemzően aszinkron kommunikációban használjuk
  (pl. e-mail, tárolt irat)
- A kommunikáció vége után is hitelességet nyújt
- Külső személyek előtt is bizonyítékként használható
- Hardvereszközt használunk a nagyobb biztonsághoz
- Előzetes regisztráció szükséges (pl. személyesen)

E-ALÁÍRÁS A GYAKORLATBAN

Hogyan lesz e-aláírásom?

- Szerződést kötök egy hitelesítés-szolgáltatóval (HSZ)
- A HSZ személyesen azonosít engem az igazolványom alapján és ellenőrzi az adataimat
- A HSZ előkészíti a kulcspáromat egy aláíró eszközön és kibocsátja a tanúsítványomat
- Átveszem az eszközt a kulccsal és tanúsítvánnyal együtt
- Aktiválom az eszközt, beállítom a PIN kódot

E-aláírás használata

- Aláíró eszköz:

  Chipkártya+olvasó vagy USB token vagy mobiltelefon

- Aláíró alkalmazás

e-SZIGNO

Adobe PDF

...

Kvíz kérdések

1) Egy aláírt kölcsönszerződésben utólag megnövelem az összeget. Szerezhetek-e így több pénzt?
2) Miből lehet megállapítani, hogy egy dokumentumot ki írt alá?
3) Mi történik, ha valaki megszerezte a titkos aláíró kulcsomat? Mi ilyenkor a teendő?
4) Találtam egy személyi igazolványt. Igényelhetek-e ezzel tanúsítványt az illető nevében?
5) Mi történik, ha lejár a tanúsítványom? Érvénytelenné válnak az aláírásaim?

Kvíz válaszok

1) Nem, mivel kimutatható a dokumentumon az utólagos módosítás, így az érvénytelen.
2) Az aláírás a tanúsítványban lévő nyilvános kulccsal ellenőrizhető, a tanúsítvány pedig tartalmazza az aláíró nevét (és akár egyéb adatait is).
3) A titkos kulcs birtokában az illető tudna az én nevemben aláírni. Ilyenkor vissza kell vonni a tanúsítványt (a HSZ által), így többé nem lehet vele érvényes aláírást létrehozni.
4) Nem, mert a HSZ a személyes azonosítás során észreveszi a hamis igazolványt (a munkatársai okmányellenőrző képzésben részesültek).
5) Nem, amennyiben időbélyeg szerepel rajtuk. Ekkor utólag bizonyítható, hogy érvényes tanúsítvánnyal készültek.

AKTUÁLIS FEJLEMÉNYEK

Jogszabályi változások

- Új jogszabályok:
  - **eIDAS** rendelet: AZ EURÓPAI PARLAMENT ÉS A TANÁCS 910/2014/EU RENDELETE (2014. július 23.) az elektronikus azonosításról és a bizalmi szolgáltatásokról
  - Magyarországon: 2015. évi CCXXII. törvény az elektronikus ügyintézés és a bizalmi szolgáltatások általános szabályairól (Eüt.)

- Előzmények:
  - Az Európai Parlament és a Tanács 1999/93/EK irányelve (1999. december 13.) az elektronikus aláírásra vonatkozó közösségi keretfeltételekről
  - Magyarországon: 2001. évi XXXV. törvény az elektronikus aláírásról

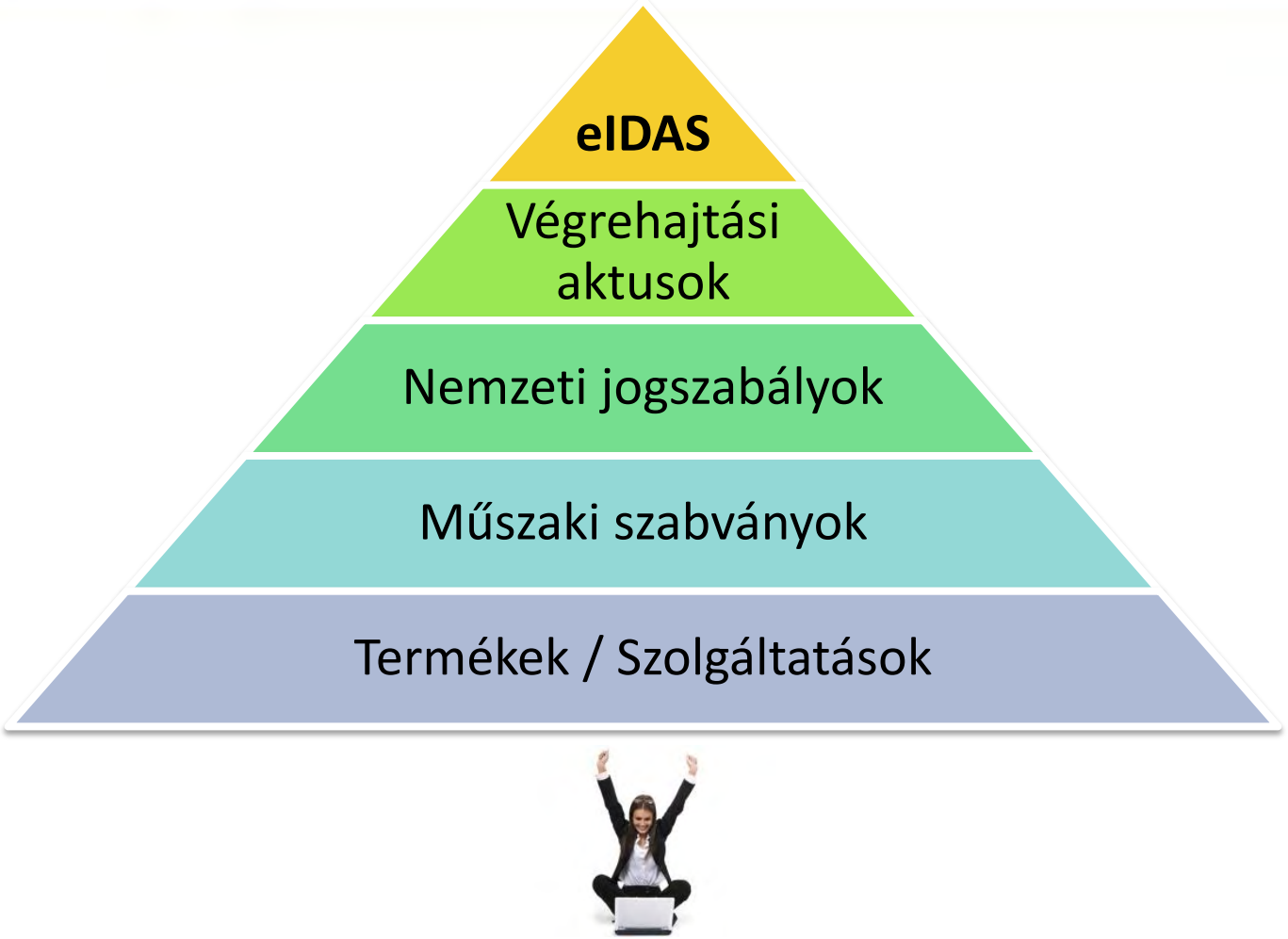
eIDAS rendelet

- electronic IDentification, Authentication and Signatures
- Az egész EU-n belül egységes jogi hátteret teremt az elektronikus azonosítás, elektronikus aláírás és a bizalmi szolgáltatások számára
- Célja a határokon átívelő elektronikus tranzakciók elősegítése, a biztonságuk és a beléjük vetett bizalom növelése, az egységes digitális piac megteremtése
- Kötelező érvényű, minden EU tagállamban közvetlenül alkalmazható, nem kell külön beemelni a nemzeti jogszabályok közé
- Két fő területet szabályoz:
  - Elektronikus azonosítás a közigazgatásban
  - Bizalmi szolgáltatások

eIDAS változások

- Szélesebb területet szabályoz EU szinten
  - De az elektronikus dokumentumok és aláírások elismerését megtartja (és kiegészíti, a korábbi direktívához képest)
- Az e-azonosítás és e-aláírás terén is előírja a tagállamok közötti kölcsönös elismerést
  - De más-más a megközelítés, az elismerés feltételrendszere
- A közigazgatásban használható e-azonosításra illetve e-aláírásra vonatkozik a kötelező elismerés
  - De várható, hogy ezt a magánszektor is követni fogja
- Bevezeti az elektronikus bélyegző fogalmát
  - Azt igazolja, hogy a dokumentum az adott jogi személytől (szervezettől) származik
- Megnyitja a lehetőséget a távoli (pl. webes vagy mobil alapú) aláírások előtt

A jéghegy csúcsa



Aláírás jogi szintjei

- **Egyszerű** elektronikus aláírás
  - Csak egy utalás az aláíró személyére
  - *Pl. név a levél végén*
  - Nem biztonságos, könnyen hamisítható
- **Fokozott biztonságú** elektronikus aláírás
  - Védi a dokumentum sértetlenségét és lehetővé teszi az aláíró hitelesítését
  - *Pl. PKI alapú digitális aláírás*
  - A kézzel írott aláíráshoz hasonló tulajdonságokkal rendelkezik
- **Minősített** elektronikus aláírás
  - Fokozott biztonságú + MALE + minősített tanúsítvány
  - *Pl. minősített HSZ-től beszerzett PKI alapú digitális aláírás*
  - A kézzel írott aláírással egyenértékű, kölcsönösen elismert

Minősített aláírás

- Fokozott biztonságú
  - PKI technológiával készült (kriptográfia alapú)
- Minősített aláírás-létrehozó eszközzel készült
  - Rajta van a MALE eszközök EU listáján
  - Common Criteria tanúsítással rendelkezik
- Minősített tanúsítványon alapul
  - Megfelel az eIDAS-ban leírt követelményeknek
  - Minősített bizalmi szolgáltató bocsátotta ki
    - Megfelel az eIDAS-ban leírt követelményeknek
    - Akkreditált megfelelőségértékelő szervezet bevizsgálta
    - Felügyeleti szerv a minősített státuszt megadta
    - Rajta van a tagállami **bizalmi listán**

Gyakorlati változások

- Új bizalmi szolgáltatások, melyek lehetnek minősítettek is
  - Weboldal-hitelesítő tanúsítványok
  - Időbélyegzés
  - Archiválás
  - Biztonságos kézbesítés
  - Tárolt kulcsú aláírás
  - Aláírás-ellenőrzés
- Egyéb vonatkozások
  - biometrikus aláírás
  - e-személyi igazolvány
  - mobil aláírás
  - e-bélyegző (hamarosan)

Biometrikus aláírás

- Biometrikus aláírás
  - Érintésérzékeny felületen kézzel végzett aláírás, amelynek adatait az adott dokumentumhoz csatolják
  - Ezután a dokumentumot a szolgáltató a saját fokozott biztonságú elektronikus aláírásával láthatja el
- Tulajdonságok
  - A dokumentumon történt utólagos módosítás kimutatható, ha fokozott biztonságú aláírást is tartalmaz
  - Alkalmas az aláíró személy azonosítására
  - Nem kizárólag az aláíró tud ilyet létrehozni, mivel az első aláírás után a biometrikus adatok (aláírás-létrehozó adat) a szolgáltató birtokában is vannak
- További információ: MELASZ Állásfoglalás

E-személyi igazolvány

2016. január 1-től igényelhető az új típusú (elektronikus) személyazonosító igazolvány. Igénylése ingyenes.

Az új e-személyi 4 kártya egyszerre:

- úti okmány (ePass)
- elektronikus aláíró (eSig)
- azonosító kártya (eID)
- **eNEK**

Úti okmány: Ezen funkciójában egyenértékű a jelenlegi chip-es útlevéllel.

eNEK: Nemzeti Egységes Kártyarendszer – felhasználás: pl. közlekedési szolgáltatók

Mobil aláírás

1) Mobilon tárolt kulccsal

- A mobil eszközünk végzi az aláírási műveletet
- *Minősített tanúsítványon alapuló fokozott biztonságú* elektronikus aláírás hozható létre, amennyiben
  - Minősített tanúsítványt tárolunk a mobil eszközön
- A legtöbb mai okos telefon már támogatja

2) Felhőben tárolt kulccsal

- A mobil eszközt erős azonosításra használjuk, amely alapján a szolgáltató végzi az aláírási műveletet
- *Minősített* aláírás hozható létre, amennyiben
  - Minősített aláírás létrehozó eszközt használ a szolgáltató
  - Minősített tanúsítványt tárol a szolgáltató
  - Minősített bizalmi szolgáltatói státusszal rendelkezik
- Ilyen szolgáltatás még nem üzemel

DEMÓK

Aláírás e-Szignóval

- **e-Szignó**: a Microsec által fejlesztett, e-aláírások és e-akták létrehozására, ellenőrzésére szolgáló szoftver
- Az aláírás folyamata:
  - Kiválasztom az aláírandó fájlokat
  - Kiválasztom az aláíró tanúsítványomat
  - A program elkészíti az aláírást a kártyán tárolt titkos kulccsal, az aláírt fájlt kimenthetem a számítógépre
- Példák:
  - E-akta aláírása: dokumentumokat és aláírásokat tartalmazó konténerformátum (ld. pl. e-cégeljárás)
  - PDF aláírása: a PDF magában tudja foglalni az aláírást
- E-személyi segítségével *minősített aláírást* készítek, amely **teljes bizonyító erejű**

Aláírás webes felületen

- **MicroSigner**: A Microsec által fejlesztett, weboldalba integrálható aláíró megoldás (Java és ActiveX mentes)
- Az aláírás folyamata:
  - Webes felületen kezdeményezem az aláírást
  - Föltöltök egy kiválasztott dokumentumot
    - A dokumentumot a szolgáltató is előállíthatta volna
  - A szolgáltató előkészíti az aláírandó adatokat
  - A kliensoldali program jóváhagyást kér,. elvégzi az aláírást a kártyával, majd föltölti az aláírást a szolgáltatóhoz,
  - A szolgáltatónál előáll az aláírt dokumentum
- Példák:
  - PDF aláírása e-Személyivel
  - Több PDF kötegelt aláírása Microsec aláíró tokennel
- *Minősített aláírást* készítek, amely **teljes bizonyító erejű**

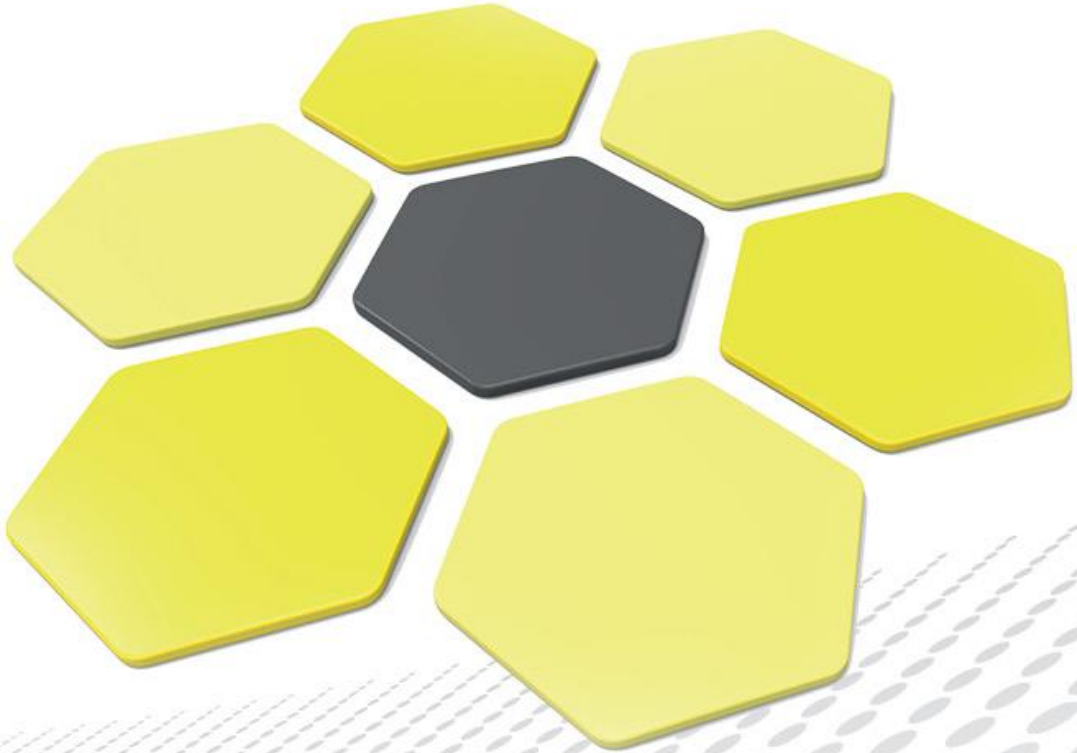
Mobil aláírás

- **PassBy[ME]**: a Microsec által fejlesztett, kétfaktoros autentikációs és dokumentum aláíró mobil applikáció
- Az aláírás folyamata:
  - Webes felületen kezdeményezem az aláírást
  - Föltöltök egy kiválasztott dokumentumot
    - A dokumentumot a szolgáltató is előállíthatta volna
  - A telefon letölti a szükséges adatokat, jóváhagyást kér
  - A telefonon tárolt kulccsal megtörténik az aláírás
  - A telefon föltölti az aláírást a szolgáltatóhoz, ahol előáll az aláírt dokumentum
- *Minősített tanúsítványon alapuló fokozott biztonságú* elektronikus aláírást készítek
- Az így előállított dokumentum a magyar jogszabályok értelmében **teljes bizonyító erejű magánokirat**

Összegzés

- A fokozott biztonságú elektronikus aláírás alapja a **PKI technológia**
- A fokozott biztonságú elektronikus aláírás a **kézi aláíráshoz hasonló** tulajdonságokkal bír
- Az aláíráshoz **kulcspár és tanúsítvány** szükséges, amelyet egy **hitelesítés-szolgáltató** bocsát ki
- Magyarországon a **minősített tanúsítvány**on alapuló aláírás teljes bizonyító erővel rendelkezik
- A minősített aláíráshoz biztonságos aláíró eszköz (chipkártya, token) is szükséges (pl. e-személyi)
- **Mobiltelefonnal** is létrehozható **teljes bizonyító erejű** elektronikus aláírás

Réti Kornél
PKI szakértő
Microsec Zrt.
reti.kornel@microsec.hu
www.microsec.hu



Köszönöm a figyelmet!