Az Informatikai és Hírközlési Minisztérium ajánlása a közigazgatásban alkalmazható hitelesítési rendekre

2005. december 7.

1. Bevezetés

Ez a dokumentum az elektronikus közigazgatásban alkalmazható hitelesítési rendekre fogalmaz meg ajánlásokat. Az ajánlás a mértékadó nemzetközi dokumentumok elemzése, a közigazgatás igényeinek és a hazai kereskedelmi hitelesítésszolgáltatók gyakorlatának felmérése, majd ennek nyomán az alternatív lehetőségek körében meghozott - szakmai konszenzuson alapuló – döntések eredményeként jött létre.

1.1 A dokumentum célja

Ezt a dokumentumot az Informatikai és Hírközlési Minisztérium az alábbi két kormányrendelet alapján teszi közzé:

- „Az elektronikus ügyintézést lehetővé tevő informatikai rendszerek biztonságáról, együttműködési képességéről és egységes használatáról" szóló 195/2005. (IX. 22.) Korm. rendelet 3. § (1) bekezdésében foglaltak alapján, az elektronikus ügyintézést lehetővé tevő informatikai rendszerek biztonságának, együttműködési képességének és egységes használatának támogatása érdekében,
- „A közigazgatási hatósági eljárásokban felhasznált elektronikus aláírásokra és az azokhoz tartozó tanúsítványokra, valamint a tanúsítványokat kibocsátó hitelesítésszolgáltatókra vonatkozó követelményekről" szóló 195/2005. (IX. 22.) Korm. Rendelet 11. § (1) bekezdésében említett közigazgatási felhasználásra vonatkozó követelményeknek megfelelő hitelesítési rendekre vonatkozó ajánlásként.

A dokumentum elsődleges célja a közigazgatás és ügyfelei számára tanúsítványokat kibocsátó hitelesítés-szolgáltatók támogatása a közigazgatási felhasználásra vonatkozó követelményeknek megfelelő hitelesítési rendek megadásával. Ennek érdekében nem csupán néhány közigazgatási felhasználásra alkalmas minta hitelesítési rend került meghatározásra. A jelen dokumentumban meghatározott hitelesítési rendek változtatás nélkül alkalmazhatók a különböző felhasználói köröknek és különböző célokra alkalmazható tanúsítványokat kibocsátó hitelesítés-szolgáltatók számára. Ezek a hitelesítési rendek egyben teljeskörűen lefedik az igényeket, köztük a közigazgatási alkalmazhatóságban érintett valamennyi felhasználói körnek, minden lehetséges célra kibocsátandó tanúsítványhoz van alkalmas hitelesítési rend, mindez különböző biztonsági szinten. Miután egy hitelesítés-szolgáltató eldöntötte, hogy mely felhasználói körnek, milyen célú tanúsítványokat, milyen biztonsági szinten kíván kibocsátani, a jelen dokumentumból a megfelelő hitelesítési rendeket kiválaszthatja, magára nézve kötelezőnek fogadhatja el. Ezután már csak a szolgáltatási szabályzatait kell ezen hitelesítési rendekkel összhangban elkészíteni ahhoz, hogy magas szintű, közigazgatási felhasználásra alkalmas szabályzatai legyenek.

A dokumentum másodlagos célja a közigazgatási felhasználásra vonatkozó követelményeknek megfelelő hitelesítési rendek egységesítése, az elektronikus ügyintézést lehetővé tevő informatikai rendszerek együttműködési képességének javítása érdekében. Feltételezve azt, hogy a hitelesítés-szolgáltatók elfogadják ezen hitelesítési rendeket, és saját szolgáltatási szabályzataikat ezekhez igazítják, a jelenlegi helyzet (melyben minden hitelesítés-szolgáltató különböző hitelesítési rendeket definiált, s ehhez illesztette saját szolgáltatási szabályzatait) nagymértékben egyszerűsödik, egyúttal a szolgáltatási szabályzatok könnyebben összehasonlíthatóak lesznek.

1.2 Alapfogalmak

A hitelesítési rendek egyértelmű értelmezéséhez szükséges fogalmakat valamennyi hitelesítési rend (az 1.6 pontban) külön-külön tartalmazza, az önálló felhasználhatóság érdekében.

1.3 Figyelembe vett jogszabályok és mértékadó dokumentumok

A jelen ajánlásban meghatározott hitelesítési rendek az alábbi jogszabályoki elvárásokon és mértékadó nemzetközi dokumentumokon alapulnak:

- 2004. évi CXL. törvény a közigazgatási hatósági eljárás és szolgáltatás általános szabályairól [1],
- 194/2005. (IX. 22.) kormányrendelet a közigazgatási hatósági eljárásokban felhasznált elektronikus aláírásokra és az azokhoz tartozó tanúsítványokra, valamint a tanúsítványokat kibocsátó hitelesítésszolgáltatókra vonatkozó követelményekről [2],
- 193/2005. (IX. 22.) kormányrendelet az elektronikus ügyintézés részletes szabályairól [3],
- 195/2005. (IX. 22.) kormányrendelet az elektronikus ügyintézést lehetővé tevő informatikai rendszerek biztonságáról, együttműködési képességéről és egységes használatáról [4],
- ETSI TS 101 456 Szabályozási követelmények a minősített tanúsítványokat kibocsátó hitelesítés-szolgáltatók számára (Műszaki specifikáció) [5],
- ETSI TS 102 042 Szabályozási követelmények a nyilvános kulcsú tanúsítványokat kibocsátó hitelesítés-szolgáltatók számára (Műszaki specifikáció) [6].

1.4 A dokumentum hatóköre (a meghatározott hitelesítési rendek köre)

Egy hitelesítési rend olyan szabálygyűjtemény, mely egy tanúsítvány felhasználhatóságát határozza meg egy közös biztonsági követelményekkel rendelkező közösség és/vagy alkalmazások egy osztálya számára.

A nyilvános kulcsú infrastruktúra elektronikus közigazgatásban való alkalmazhatósága különböző közösség- és alkalmazás-osztályokat igényel, melyekhez különböző hitelesítési rendek készítendők. Az egyes hitelesítési rendek igen hasonlók egymáshoz, a bennük megfogalmazott szabályok többsége valamennyiükre nézve közös. Ugyanakkor eltérő hitelesítési rendekre (szabálygyűjteményekre) van szükség az alábbi okok miatt:

- [1], [2] és [3] részben eltérő szabályokat határoz meg a közigazgatási hatóságokra és az ügyfelekre, de a nem természetes személyeknek kibocsátott tanúsítványokra is különleges szempontok vonatkoznak.
- [1], [2] és [3] direkt módon megkülönbözteti a minősített és a fokozott biztonságú elektonikus aláírásokat, melyek mögött eltérő biztonsági és garanciális követelmények húzódnak. Az azonosítás/hitelesítés és a titkosítás szintén igényelhet több biztonsági/garanciális szintet, összhangban a minősített és a fokozott biztonságú aláírásokkal, valamint a [6]-ban leírt különböző szintekkel.

A fentiek alapján a különböző hitelesítési rendek egy közös szabálygyűjteményből származnak, az alábbi eltérések figyelembe vételével:

- a közigazgatás ügyfeleire [Ü], a közigazgatás köztisztviselőire [K], az ügyfelek által működtetett automatizmusokra[1] [ÜA], valamint a közigazgatást képviselő automatizmusokra[2] [KA] vonatkozó eltérő szabályok,

[1] pl. hitelesítő és titkosító szerverekre

[2] pl. hitelesítő és titkosító szerverekre, valamint szervezeti aláírást automatikusan létrehozó informatikai eszközökre

- a legmagasabb, a közepes és a legalacsonyabb biztonsági szinten eltérő szabályok, melyek megkülönböztetése a hordozóeszköz alapján lehetséges: a legmagasabb szint biztonságos aláírás-létrehozó eszközt, a közepes szint kriptográfiai hardver eszközt vár el a magánkulcsok tárolására és aktivizálására, míg a legalacsonyabb szint teret ad a tisztán szoftveres megoldásoknak is.

Ugyanakkor nem minden felhasználói kör igényli az összes biztonsági szintet. Az automatizmusok (szerverek) számára elegendőnek tűnik a legalacsonyabb (és legolcsóbb) szint, a szoftveres megvalósítás.

1.5 A meghatározott hitelesítési rendek

A fentieket összefoglava, a magyar elektronikus közigazgatásban az alábbi hitelesítési rendekre van szükség:

- Biztonságos aláírás-létrehozó eszköz alkalmazását megkövetelő **m**inősített **h**itelesítési **r**endekre, ezen belül:
  - Közigazgatási, ügyfélhez kapcsolódó, biztonságos aláírás-létrehozó eszköz használatát megkövetelő, aláírás célú tanúsítványokhoz tartozó, minősített hitelesítési rend
    /Azonosító: [MHR_Ü], OID: 0.2.216.1.100.42.101.**1**.2.1/
  - Közigazgatási, köztisztviselőhöz kapcsolódó, biztonságos aláírás-létrehozó eszköz használatát megkövetelő, aláírás célú tanúsítványokhoz tartozó, minősített hitelesítési rend
    /Azonosító: [MHR_K], OID: 0.2.216.1.100.42.101.**2**.2.1/
- Kriptográfiai hardver eszköz alkalmazását megkövetelő **e**gységesített **h**itelesítési **r**endekre, ezen belül:
  - Közigazgatási, ügyfélhez kapcsolódó, kriptográfiai hardver eszköz használatát megkövetelő, egységesített hitelesítési rend
    /Azonosító: [EHR+_Ü], OID: 0.2.216.1.100.42.101.**3**.2.1/
  - Közigazgatási, köztisztviselőhöz kapcsolódó, kriptográfiai hardver eszköz használatát megkövetelő, **e**gységesített **h**itelesítési **r**end
    /Azonosító: [EHR+_K], OID: 0.2.216.1.100.42.101.**4**.2.1/
- Kriptográfiai hardver eszköz alkalmazását nem megkövetelő egységesített hitelesítési rendekre, ezen belül:
  - Közigazgatási, ügyfélhez kapcsolódó, egységesített hitelesítési rend
    /Azonosító: [EHR_Ü], OID: 0.2.216.1.100.42.101.**5**.2.1/
  - Közigazgatási, ügyfél által működtetett automatizmushoz kapcsolódó, egységesített hitelesítési rend
    /Azonosító: [EHR_ÜA], OID: 0.2.216.1.100.42.101.**6**.2.1/
  - Közigazgatási, köztisztviselőhöz kapcsolódó, egységesített hitelesítési rend
    /Azonosító: [EHR_K], OID: 0.2.216.1.100.42.101.**7**.2.1/
  - Közigazgatási, közigazgatást képviselő automatizmushoz kapcsolódó, egységesített hitelesítési rend
    /Azonosító: [EHR_KA], OID: 0.2.216.1.100.42.101.**8**.2.1/

A minősített hitelesítési rendek megfelelnek az európai szabványosítás keretében kidolgozott, [5]-ban definiált “QCP+SSCD” minősített hitelesítési rendnek. Ugyanakkor számos helyen tovább pontosítják, illetve konkretizálják a “QCP+SSCD” követelményeit, a magyar közigazgatáson belüli egységes és biztonságos felhasználhatóság, valamint a hazai jogszabály előírásoknak való megfelelőség érdekében. A két minősített hitelesítési rendet az 1. számú melléklet tartalmazza.

A kriptográfiai hardver eszköz használatát megkövetelő, egységesített hitelesítési rendek megfelelnek az európai szabványosítás keretében kidolgozott, [6]-ban definiált “NCP+” egységesített hitelesítési rendnek. Ugyanakkor számos helyen tovább pontosítják, illetve konkretizálják az “NCP+” követelményeit, a magyar közigazgatáson belüli egységes és biztonságos felhasználhatóság, valamint a hazai jogszabály előírásoknak való megfelelőség érdekében. A két ilyen hitelesítési rendet a 2. számú melléklet tartalmazza.

A kriptográfiai hardver eszköz használatát nem megkövetelő, egységesített hitelesítési rendek megfelelnek az európai szabványosítás keretében kidolgozott, [6]-ban definiált “NCP” egységesített hitelesítési rendnek. Ugyanakkor számos helyen tovább pontosítják, illetve konkretizálják az “NCP” követelményeit, a magyar közigazgatáson belüli egységes és biztonságos felhasználhatóság, valamint a hazai jogszabály előírásoknak való megfelelőség érdekében. A négy ilyen hitelesítési rendet a 3. számú melléklet tartalmazza.

1.6 A különböző hitelesítési rendek összehasonlítása

Az azonos mellékletbe kerülő (azonos biztonsági szintet képviselő, de eltérő felhasználói körnek szóló) hitelesítési rendek közötti eltéréseket az egyes mellékletek bevezetői tartalmazzák (az 1.1 alfejezetekben).

Az alábbi táblázat azt tekinti át, hogy a különböző mellékletbe kerülő, eltérő biztonsági szintet képviselő hitelesítési rendek milyen meghatározó nemzetközi dokumentumokon alapulnak.

legmagasabb biztonsági szintet elváró hitelesítési rendek	közepes biztonsági szintet elváró hitelesítési rendek	legalacsonyabb biztonsági szintet elváró hitelesítési rendek
azonosítók: [MHR_Ü], [MHR_K] sorszámok: (1,2)	azonosítók: [EHR+_Ü], [EHR+_K] sorszámok: (3, 4)	azonosítók: [EHR_Ü], [EHR_ÜA] [EHR_K] [EHR_KA] sorszámok: (5,6,7,8)
ETSI TS 101 456 ([5]): “QCP+SSCD” biztonságos aláírás-létrehozó eszköz használatát megkövetelő, minősített hitelesítési rend	ETSI TS 102 042 ([6]): „NCP+” kriptográfiai hardver eszköz használatát megkövetelő, egységesített hitelesítési rend	ETSI TS 102 042 ([6]): „NCP” kriptográfiai hardver eszköz használatát nem megkövetelő, egységesített hitelesítési rend

Végül az alábbi táblázat az eltérő biztonsági szintet képviselő hitelesítési rendek közötti különbségeket tekinti át.

	azonosító: **MHR**_x sorszám: (1,2)	azonosító: **EHR+**_x sorszám: (3,4)	azonosító: **EHR**_x sorszám: (5,6,7,8)
Általában (1)	BALE minősítésű eszközt vár el a magánkulcsok hordozására és aktivizálásra.	BALE minősítéssel nem feltétlenül rendelkező kriptográfiai hardver eszközt vár el a magánkulcsok hordozására és aktivizálásra	Nem vár el kriptográfiai hardver eszközt a magánkulcsok hordozására és aktivizálásra
Általában (2)	A hitelesítés-szolgáltató biztosít (BALE) eszköz ellátást is.	A hitelesítés-szolgáltató biztosít (kriptográfiai hardver) eszköz ellátást is.	A hitelesítés-szolgáltató nem biztosít eszköz ellátást.
1.3.3 Előfizetők és alanyok	Alanyok csak természetes személyek lehetnek	Alanyok csak természetes személyek lehetnek	Alanyok lehetnek az elektronikus ügyintézésben közreműködő automatizmusok (eszközök) is.
3.1.1 Név típusok	---	---	Az eszköz tanúsítványokra más névkonvenció érvényes.
4.10.2 A szolgáltatás rendelkezésre állása, a tanúsítványtár és a kikötések/ feltételek folyamatos elérhetősége	**99,9%**-os rendelkezésre állás, ahol az eseti szolgáltatás-kiesések nem haladhatják meg a **3** órát.	**99%**-os rendelkezésre állás, ahol az eseti szolgáltatás-kiesések nem haladhatják meg a **24** órát.	**99%**-os rendelkezésre állás, ahol az eseti szolgáltatás-kiesések nem haladhatják meg a **24** órát.
5.2.1 Bizalmi munkakörök b) Az alábbi munkakörök tartoznak a bizalmi munkakörök közé:	1. Az informatikai rendszeréért általánosan felelős vezető, 2. Biztonsági tisztviselő 3. Rendszer-adminisztrátor 4. Rendszerüzemeltető 5. Független rendszervizsgáló 6. Regisztrációs felelős	1. --- 2. Biztonsági tisztviselő 3. Rendszer-adminisztrátor és üzemeltető 5. Független rendszervizsgáló 6. Regisztrációs felelős	1. --- 2. Biztonsági tisztviselő 3. Rendszer-adminisztrátor és üzemeltető 5. Független rendszervizsgáló 6. Regisztrációs felelős

5.2.1 Bizalmi munkakörök e) pont	A bizalmi munkakört betöltő személynek munkaviszonyban kell állnia a HSz-szel.	---	---
5.2.4 Egymást kizáró munkakörök	2 és 6 nem lehet 5 3 nem lehet 2 és 5 1 nem lehet 2 és 5	2 nem lehet 5	2 nem lehet 5
5.3.1 Képzettségre, gyakorlatra és biztonsági ellenőrzésre vonatkozó követelmények c) pont	1-et olyan személynek kell betöltenie, aki szakirányú felsőfokú végzettséggel és legalább három év, az informatikai biztonsággal összefüggésben szerzett szakmai gyakorlattal rendelkezik.	---	---
5.3.1 Képzettségre, gyakorlatra és biztonsági ellenőrzésre vonatkozó követelmények d) pont	Bizalmi munkakört csak erkölcsi bizonyítvánnyal rendelkező személyek tölthetnek be.	---	---
5.3.7 Szerződéses viszonyban foglalkoztatottakra vonatkozó követelmények	A bizalmi munkakört betöltő személynek munkaviszonyban kell állnia a HSz-szel.	---	---
5.7.1 Váratlan esemény és kompromittálódás kezelési eljárások c) pont	Rendkívüli üzemeltetési helyzet bekövetkezése esetén haladéktalanul értesíteni kell az NHH-t és az érintetteket.	---	---

6.1.7 A kulcs használat célja (az X.509 v3 kulcshasználati mező tartalmának megfelelően)	minősített aláíráshoz tartozó tanúsítvány kulcshasználati mezője kritikus, és a mezőben kizárólag a "NonRepudiation" bit van „true” értékre beállítva	fokozott biztonságú aláíráshoz tartozó tanúsítvány kulcshasználati mezője kritikus, és a mezőben a "NonRepudiation" bit „true” értékre van beállítva, s ezen kívül legfeljebb a "DigitalSignature” bit lehet még "true” értékre beállítva	fokozott biztonságú aláíráshoz tartozó tanúsítvány kulcshasználati mezője kritikus, és a mezőben a "NonRepudiation" bit „true” értékre van beállítva, s ezen kívül legfeljebb a "DigitalSignature” bit lehet még "true” értékre beállítva
8.1 Az ellenőrzések körülményei és gyakorisága	**Évente külső** megfelelőségi auditot kell végrehajtani.	A megfelelőségi ellenőrzéseket **2 évente** meg kell ismételni. Ezek az ellenőrzések lehetnek **belső** auditok is.	A megfelelőségi ellenőrzéseket **2 évente** meg kell ismételni. Ezek az ellenőrzések lehetnek **belső** auditok is.
9.2 Anyagi felelősségvállalás c) A felelősség-biztosítási szerződésnek egy biztosítási esemény vonatkozásában káreseményenként:	a tanúsítványban, illetve a SzSz-ban vállalt felelősségvállalási érték legalább **ötszöröséig** kell fedezetet biztosítania az összes károsultnak okozott károkra.	a tanúsítványban, illetve a SzSz-ban vállalt felelősségvállalási érték legalább **háromszorosáig** kell fedezetet biztosítania az összes károsultnak okozott károkra.	a tanúsítványban, illetve a SzSz-ban vállalt felelősségvállalási érték legalább **háromszorosáig** kell fedezetet biztosítania az összes károsultnak okozott károkra.

1.7 Mellékeletek

A 8 hitelesítési rend az alábbi 3 mellékletben található:

- 1. számú melléklet: Közigazgatási, biztonságos aláírás-létrehozó eszköz használatát megkövetelő, aláírás célú tanúsítványokhoz tartozó, minősített hitelesítési rendek (1.-2.)
- 2. számú melléklet: Közigazgatási, kriptográfiai hardver eszköz használatát megkövetelő, egységesített hitelesítési rendek (3.-4.)
- 3. számú melléklet: Közigazgatási, kriptográfiai hardver eszköz használatát nem megkövetelő, egységesített hitelesítési rendek (5.–8.)