Nemzeti Adatvédelmi és
Információszabadság Hatóság

Ügyszám: NAIH/2017/4711/2/J,
4712/2/J,
4713/2/J
Ügyintéző: dr. Urbán Szilvia
Hivatkozási szám: BM/17655/2017.
Előadó: dr. Benedek Bulcsú

Dr. Felkai László közigazgatási államtitkár úr részére

Belügyminisztérium

Budapest

Tisztelt Közigazgatási Államtitkár Úr!

Az egységes elektronikuskártya-kibocsátási keretrendszerről szóló 2014. évi LXXXIII. törvény végrehajtásáról szóló előterjesztés tervezetét áttekintettem és az alábbi észrevételeket teszem.

1. Az egységes elektronikuskártya-kibocsátási keretrendszerről szóló 2014. évi LXXXIII. törvény (a továbbiakban: NEK tv.) 1. § (2) úgy rendelkezik, hogy a NEK keretein belül kibocsátott biztonsági okmányok esetében a *biztonsági okmányok védelmének rendjéről szóló kormányrendelet*[1] szerinti követelményeket is teljesíteni kell. A kormányrendelet melléklete sorolja fel a kötelezően kialakítandó biztonsági okmányokat, az egységes elektronikuskártyát azonban taxatíve nem említi. A NEK tv. tehát megengedi, hogy a NEK kártya ellásson akár biztonsági okmány funkciót is, azonban nyitva hagyja, hogy miféle okmányok lehetnek ezek.

A Korm. rendelet Tervezete (a továbbiakban: Tervezet) szűkíti a fenti kérdést a 2. § (2) bekezdésben azáltal, hogy kizárja a Tervezet hatálya alól az „A" (vagyis a legszigorúbb védelmi követelmények alá eső) okmányvédelmi kategóriát, így NEK kártyát nem lehet létrehozni semmilyen címen személyazonosság igazolására, fegyverviselés engedélyezésére, határátlépés engedélyezésére és a kártyák az arcképen kívül nem tartalmazhatnak biometrikus azonosító adatot (pl. ujjlenyomat). Ezáltal továbbra is lehetséges „B" és „C" okmányvédelmi kategóriába sorolt biztonsági okmányok előállítása NEK kártya formájában.

A 86/1996. (VI. 14.) Korm. rendelet 2. sz. mellékletében foglaltak szerint
„2. „B" védelmi kategória
Az e védelmi kategóriába tartozó biztonsági okmányok egyes főbb alkatrészeit kell a teljes vagy részleges hamisítás ellen védeni. A védelmi módszereknél a kémiai, technikai, technológiai és adminisztratív eljárásokat, valamint elektronikus biztonsági okmány esetében a digitális védelmi módszereket, eljárásokat differenciáltan kell alkalmazni.
3. „C" védelmi kategória
Az e védelmi kategóriába tartozó biztonsági okmányok hamisítása ellen, és annak felismerése érdekében legalább adminisztratív védelmi eljárásokat kell alkalmazni.

[1] 86/1996. (VI. 14.) Korm. rendelet

1125 Budapest,
Szilágyi Erzsébet fasor 22/C.
Tel.: +36 1 391-1400
Fax: +36 1 391-1410
ugyfelszolgalat@naih.hu
www.naih.hu

Elektronikus biztonsági okmány esetében az informatikai védelmet úgy kell kialakítani, hogy az elektronikusan tárolt adatok jellegétől és a használat során várható kockázattól függően „Kiemelt", „Fokozott" vagy „Alap" szintű informatikai védelmet kell biztosítani."

A Tervezet 3. sz. melléklete a kártya *fizikai specifikációjában* meghatározza, hogy „Minimálisan kötelező biztonsági elemek: biankó kártyák egyedileg számozott, szigorú számadású kezelése; fénymásolás elleni védelem (pl. védő alnyomat)" ami alapszinten kielégíti a „B" okmányvédelmi kategória kötelező fizikai védelmét. Az *Elektronikus adatjellemzők* pedig láthatóan túlteljesítik a „B" és „C" okmányvédelmi kategóriák követelményeit, úgyszintén a „Kiemelt" informatikai védelem elemeit is megvalósítják.

Mindez azért lényeges, mert a „B" okmányvédelmi kategóriájú okmány kibocsátása folyamatában a Nemzetbiztonsági Szakszolgálatnak is szerepe van, amit a 86/1996. (VI. 14.) Korm. rendelet 7-8-9. szakasza ír le, ennek aktusai, dokumentumai nem jelennek meg a Tervezet kártyakibocsátásról szóló mellékletében, a működtető szerv esetében azonban említésre kerülnek.

A NEK tv. nem tárgyalja a rendszerben alkalmazott kulcsok kezelésével kapcsolatos szabályokat, azt a végrehajtási rendeletre (Tervezet) bízza.

2. A Tervezet 3. sz. mellékletében (Kártyaspecifikáció) az alábbi pontosítások szükségesek:

1.1.6. Kulcsdiverzifikáció

Szintén a Működtető gondoskodik arról, hogy minden Megszemélyesítő megkapja az által megszemélyesített kártyákhoz tartozó mesterkulcs-készleteket, valamint az Elfogadók és Kibocsátók megkapják a kulcskészlet általuk kezelhető mesterkulcsokat.

A Hatóság szövegszerű javaslata:

*Szintén a Működtető gondoskodik arról, hogy minden Megszemélyesítő megkapja az **általa** megszemélyesített kártyákhoz tartozó mesterkulcs-készleteket, valamint az Elfogadók és Kibocsátók megkapják a **kulcskészletből az** általuk kezelhető mesterkulcsokat.*

A használt 128 bites AES kulcsok diverzifikálása CMAC alapú (AV2) Mifare kulcsdiverzifikációval történik Az alábbiak szerint

A Hatóság szövegszerű javaslata:

*A használt 128 bites AES kulcsok diverzifikálása CMAC alapú (AV2) **MIFARE** kulcsdiverzifikációval **történik az alábbiak** szerint*

A MIFARE kártya megnevezését a teljes mellékletben javaslom nagybetűvel megjeleníteni a szakirodalommal összhangban, mert valójában egy mozaikszóról van szó (MIkron FARE Collection System).

Diverzifikált kulcs neve (ld. Hiba! A hivatkozási forrás nem található.)

Itt a kulcsnév definíciója hibás, a Kártyaspecifikációt elkészítő, a Tervezetbe bedolgozó szervezet (valószínűleg a Nemzetbiztonsági Szakszolgálat Szakértői Intézete) tudja pontosítani a szöveget.

3. A Tervezet 2. sz. melléklete (A NEK kulcskezelési szabályai) 14. pontjában előírja: *A kulcs használójának biztosítania kell, hogy a kulcsról semmilyen másolat ne készüljön.*

Pontosítandó, hogy a mellékletet szerkesztő hogyan értette a tiltást, az vonatkozik-e a biztonságos informatikai rendszerekre kidolgozott Business Continuity Plan (BCP= Üzletmenet Folytonossági Terv) keretében előírt biztonsági mentésekre, tartalék üzemelési helyszíneken duplikált adatok esetére is, azaz a kulcsot használó szervezet informatikai rendszerén csak szigorúan egy példányban létezhet-e egy adott kulcs. Megjegyzendő, hogy az ilyen szigorú tiltás üzembiztonsági kockázatot jelenthet a kulcsok esetleges vétlen törlése, elérhetetlenné válása esetén.

A Tervezetet a személyes adatok védelme és a közérdekű adatok nyilvánossága szempontjából egyebekben nem kifogásolom.

Kérem a fenti észrevételek megfontolását, figyelembe vételét és a szükséges intézkedések megtételét.

Budapest, 2017. szeptember „30".

Üdvözlettel:

NEMZETI ADATVÉDELMI ÉS INFORMÁCIÓSZABADSÁG HATÓSÁG 1. sz.

Dr. Péterfalvi Attila
elnök
c. egyetemi tanár

Naih_Ügyfélszolgálat

Feladó: Naih_Ügyfélszolgálat <ugyfelszolgalat@naih.hu>
Küldve: 2017. szeptember 21. 12:10
Címzett: 'bulcsu.benedek@bm.gov.hu'; 'szkhat@bm.gov.hu'
Tárgy: NAIH-2017-4711-2-J;NAIH-2017-4712-2-J;NAIH-2017-4713-2-J
Mellékletek: NAIH-2017-4711-2-J-munkapéldány.pdf

Tisztelt Címzett!

Mellékelten megküldöm a Nemzeti Adatvédelmi és Információszabadság Hatóság levelét!

Üdvözlettel:

NAIH Ügyfélszolgálat