Nemzeti Adatvédelmi és
Információszabadság Hatóság

Ügyszám: NAIH/2015/5080/J

Ügyintéző: dr. Bíró János

Hiv. szám: BM/11279-28/2015.

Dr. Felkai László részére
közigazgatási államtitkár

Belügyminisztérium

robert.lupocz@bm.gov.hu
szkhat@bm.gov.hu

Tisztelt Közigazgatási Államtitkár Úr!

A biztonsági okmányok védelmének rendjéről szóló 86/1996. (VI. 14.) Korm. rendelet módosításáról szóló kormányrendelet közigazgatási egyeztetés keretében véleményezésre megküldött tervezetéhez Hatóságunk a következő észrevételt teszi:

A tervezet 1. melléklete az okmányinformatikai védelmi kategóriák, és az azokra irányadó általános biztonsági, védelmi követelmények között kitér a tárolt adatot védő titkosítás megengedett algoritmusainak meghatározására. Ez a tervezet szerint a kiemelt okmányinformatikai védelmi kategóriában „legalább RSA", fokozott okmányinformatikai védelmi kategóriában „legalább 3DES".

A titkosítási algoritmusok ilyetén meghatározása azt feltételezi, hogy létezik egy jogszabályban , vagy egyéb, nyilvános és általánosan elfogadott jegyzékben meghatározott lista, amely a titkosítási algoritmusokat erősség szerint rangsorolja. Ilyen listáról azonban nincs tudomásunk, továbbá kérdéses, hogy lehet-e minden esetben egzakt módon rangsorolni a titkosító algoritmusokat egyéb paraméterek, például kulcshossz megadása nélkül. Ezért véleményünk szerint helyesebb lenne, ha a tervezet egyértelműen meghatározná, hogy az egyes védelmi kategóriákban mely titkosítási algoritmusok használhatók.

Budapest, 2015. szeptember „ „

Üdvözlettel:

Dr. Péterfalvi Attila
elnök
c. egyetemi tanár

1125 Budapest,
Szilágyi Erzsébet fasor 22/C.

Tel.: +36 1 391-1400
Fax: +36 1 391-1410

ugyfelszolgalat@naih.hu
www.naih.hu