NEMZETI MÉDIA- ÉS HÍRKÖZLÉSI HATÓSÁG

1088 Budapest, Reviczky utca 5. • Levélcím: 1433 Budapest, Pf. 198
Telefon: (+36 1) 429 8600 • Fax: (+36 1) 267 2612

E-szolgáltatás-felügyeleti Osztály

Iktatószám: EF/26838-13/2011
Tárgy: Határozat
Ügyintéző: Bajusz János
Telefon: (1) 429-8613

Melléklet: 2 db.

A Nemzeti Média- és Hírközlési Hatóság (továbbiakban: Hatóság) a **Digitoll Informatikai és Szolgáltató Kft.** (székhely: 1124 Budapest, Stromfeld Aurél út 9.), mint *az elektronikus aláírásról szóló 2001. évi XXXV. törvény* (továbbiakban: Eat.) 6. § (1) bekezdésének hatálya alá tartozó elektronikus aláírással kapcsolatos szolgáltatást nyújtó (továbbiakban: Szolgáltató) vonatkozásában hivatalból indult eljárásban meghozta a következő

h a t á r o z a t o t .

A Hatóság az Eat. 18. § szerinti hatáskörében eljárva az Eat. 6. § (1) bekezdés szerinti elektronikus aláírással kapcsolatos szolgáltatások (továbbiakban: Szolgáltatások) nyújtása során felhasználható biztonságos kriptográfiai algoritmusokat, valamint a hozzájuk tartozó paramétereket a jelen határozat **1. számú mellékletében foglaltaknak** megfelelően

á l l a p í t j a m e g .

A Hatóság

k ö t e l e z i

a Szolgáltatót, hogy a jelen határozat jogerőre emelkedésétől számított **30 napon belül** az Eat. 6. § (1) bekezdés hatálya alá tartozó elektronikus aláírással kapcsolatos szolgáltatásainak nyújtása során használt algoritmusokat és paramétereket a jelen határozat **1. számú mellékletének megfelelően** állítsa be. A jelen határozatban foglaltak teljesülését a Hatóság az Eat. 17. § (1) bekezdés b) pontja, valamint 20. § (1) bekezdése, illetve *a közigazgatási hatósági eljárás és szolgáltatás általános szabályairól szóló 2004. évi CXL. törvény* 88. § (1) bekezdése alapján ellenőrizni fogja, és a határozat nem, vagy nem megfelelő teljesítése esetén a Szolgáltatóval, illetve annak vezető tisztségviselőjével szemben az Eat. 21-23. § szerinti szankciókat alkalmazhatja.

Jelen határozat ellen annak közlésétől számított **tizenöt napon belül** a Nemzeti Média- és Hírközlési Hatóság Elnökének címzett, de az elsőfokú határozatot hozó szervnél benyújtott fellebbezésnek van helye, amelynek a határozat végrehajtására halasztó hatálya van. A benyújtott fellebbezéshez csatolni kell a fellebbezési illeték összegének megfelelő, **5000.-Ft**, azaz **ötezer forint** értékű illetékbélyeget. A fellebbezés elektronikus úton történő benyújtására jelenleg nincsen lehetőség.

Az eljárás során további eljárási költség nem merült fel.

I n d o k o l á s

A Hatóság az Eat. 18. § szerinti hatáskörében hivatalból eljárást indított az Eat. 6. § (1) bekezdése szerinti elektronikus aláírással kapcsolatos szolgáltatások nyújtása során alkalmazható biztonságos kriptográfiai algoritmusok, illetve az ezekhez tartozó paraméterek megállapítására. Erről a Szolgáltatót a **EF-26838-1/2011** számú, **2011. szeptember 12**-én kelt levelében értesítette, melynek mellékleteként, nyilatkozattétel céljából megküldte jelen határozat tervezetét. Az eljárás megindítására azért került sor, mert a European Telecommunications Standards Institute (ETSI) ETSI TS 102 176-1 v 2.1.1 (2011-07) számon, „Electronic Signatures and Infrastructures (ESI); Algorithms and Parameters for Secure Electronic Signatures; Part 1: Hash functions and asymmetric algorithms" címmel közzétette a biztonságos elektronikus aláírások létrehozására ajánlott kriptográfiai algoritmusok és paraméterek jegyzékét, melynek nyomán a Hatóság jelenleg hatályos, **HL-21917-9,-10,-11,-12,-13,-14/2008 számú** határozatainak felülvizsgálata vált indokolttá. Az Eat. 18. § a Hatóság feladatává teszi az elektronikus aláírással kapcsolatos szolgáltatások nyújtása során alkalmazható biztonságos kriptográfiai algoritmusok és paraméterek meghatározását és határozat formájában történő közlését.

Az eljárás lefolytatására az Eat. 17. § (2) bekezdése alapján *a közigazgatási hatósági eljárás és szolgáltatás általános szabályairól szóló 2004. évi CXL. törvény* (továbbiakban: Ket.) rendelkezéseinek megfelelően került sor.

Az eljárás során a Hatóság felhasználta a fent hivatkozott ETSI TS 102 176-1 v 2.1.1 (2011-07) dokumentumot, amelyet az algoritmusok és paraméterek biztonságosságának megítélésében mértékadónak tekintett. A jelen határozat **1. számú melléklete** meghatározza a jelenleg biztonságosnak tekinthető algoritmusok és a hozzájuk tartozó paraméterek jegyzékét. Továbbá meghatározza azok felhasználhatósági idejét, illetve a határozat **2. számú melléklete** szerinti ajánlásokat rendeli irányadónak. Az ajánlások nem tartalmaznak normatív előírásokat, a tájékoztatás, illetve a felkészülés célját szolgálják és a jelenlegi ismeretek alapján kerültek megfogalmazásra. A Hatóság új határozatot fog hozni abban az esetben, ha a mellékletben meghatározott bármely algoritmus adott paraméterekkel való felhasználása már nem biztonságos. Ennek érdekében az Eat. 18. §-ban írt kötelezettségének megfelelően a Hatóság figyelemmel fogja

kísérni az elektronikus aláírással kapcsolatos technológia és kriptográfiai algoritmusok fejlődését, valamint az európai szabványosítás területén folyó munkát.

A fellebbezési jogra a Ket. 98. § és 99. § (1) bekezdése, valamint az Eat. 17. § (5) bekezdése az irányadó, a fellebbezési illeték mértékét *az illetékekről szóló 1990. évi XCIII. törvény (továbbiakban: Illetéktv.)* 29. § (2) bekezdése alapján állapítottam meg, a megfizetés módjára az Illetéktv. 73. § (1) bekezdés rendelkezése az irányadó. A határozat meghozatalára az Eat. 18. §, valamint a Ket. 71. § (1) bekezdés és 72. § (1) bekezdése alapján került sor. A Hatóság hatáskörét és illetékességét a jelen eljárásban a Ket. 22. § (1) bekezdése, valamint az Eat. 18. § alapozza meg.

Budapest, 2011. szeptember 27.

Aranyosné dr. Börcs Janka
a Nemzeti Média- és Hírközlési Hatóság Hivatala
főigazgatója nevében és megbízásából

dr. Sylvester Nóra
osztályvezető

Határozatot kapják:

1. Digitoll Informatikai és Szolgáltató Kft.
   (1124 Budapest, Stromfeld Aurél út 9.)
2. Irattár helyben

Az elektronikus aláírással kapcsolatos szolgáltatások területén alkalmazható kriptográfiai algoritmusokról és paraméterekről szóló határozat 1. számú melléklete

Az alábbi táblázatok megadják az Eat. hatálya alá tartozó szolgáltatók által nyújtott elektronikus aláírással kapcsolatos szolgáltatások területén alkalmazható, a kapcsolódó mértékadó szabványok és egyéb dokumentumok, kiemelten az ETSI TS 102 176-1 V 2.1.1 (2011-07) (továbbiakban: [ALGO]) szerinti kriptográfiai algoritmusokat, valamint az algoritmusok paramétereire vonatkozó követelményeket.

Tartalomjegyzék

1. Megfelelő kriptográfiai algoritmuskészletek

Egy, a következő táblázatban felsorolt kriptográfiai algoritmuskészlet az alábbi komponensekből áll:

a) aláíró algoritmus paraméterekkel
b) kulcselőállítási algoritmus
c) feltöltő módszer
d) kriptográfiai lenyomatképző függvény

Az elektronikus aláírások biztonságát esetlegesen kedvezőtlenül befolyásoló egymásrahatások miatt a biztonságos elektronikus aláírás céljára használható kriptográfiai algoritmuskészlet komponensei és paraméterei kizárólag a táblázatokban megadott kombinációkban alkalmazhatók.

Kriptográfiai algoritmuskészlet rövid neve	Lenyomatképző függvény rövid neve	Feltöltő algoritmus rövid neve	Aláíró algoritmus rövid neve	Alkalmazható
sha1-with-rsa	sha1	Az RSA aláíró algoritmus használata esetén a feltöltő algoritmus a 3. fejezetbeli listából választható	rsa	2011.12.31-ig
sha1-with-dsa	sha1	nem szükséges	dsa	2011.12.31-ig
ripemd160-with-rsa	ripemd160	Az RSA aláíró algoritmus használata esetén a feltöltő algoritmus a 3. fejezetbeli listából választható	rsa	2011.12.31-ig
ripemd160-with-dsa	ripemd160	nem szükséges	dsa	2011.12.31-ig
sha224-with-rsa	sha224	Az RSA aláíró algoritmus használata esetén a feltöltő algoritmus a 3. fejezetbeli listából választható	rsa	2. számú melléklet szerint
sha256-with-rsa	sha256	Az RSA aláíró algoritmus használata esetén a feltöltő algoritmus a 3. fejezetbeli listából választható	rsa	2. számú melléklet szerint
rsa-pss with mgf1SHA1Identifier	mgf1-SHA1		rsa	2. számú melléklet szerint
rsa-pss with mgf1-SHA224Identifier	mgf1-SHA224		rsa	2. számú melléklet szerint
rsa-pss with mgf1-SHA256Identifier	mgf1-SHA256		rsa	2. számú melléklet szerint
sha1-with-ecdsa	sha1	nem szükséges	ecdsa-Fp vagy ecdsa-F2m	2011.12.31-ig
sha1-with-ecgdsa	sha1	nem szükséges	ecgdsa-Fp vagy ecgdsa-F2m	2011.12.31-ig
sha224-with-ecdsa	sha224	nem szükséges	ecdsa-Fp vagy ecdsa-F2m	2. számú melléklet szerint
sha256-with-ecdsa	sha256	nem szükséges	ecdsa-Fp vagy ecdsa-F2m	2. számú melléklet szerint
sha384-with-ecdsa	sha384	nem szükséges	ecdsa-Fp vagy ecdsa-F2m	2. számú melléklet szerint
sha512-with-ecdsa	sha512	nem szükséges	ecdsa-Fp vagy ecdsa-F2m	2. számú melléklet szerint
ecdsa-with-RIPEMD160	ripemd160	nem szükséges	ecdsa-Fp vagy ecdsa-F2m	2011.12.31-ig

1. táblázat: Megfelelő kriptográfiai algoritmuskészletek

2. Megfelelő kriptográfiai lenyomatképző függvények

A kriptográfiai lenyomatképző függvényekkel szembeni követelményeket az Eat. 2. § 26. pontja határozza meg. Eszerint a kriptográfiai lenyomatképző függvény megfelelően biztonságos, ha az alábbi tulajdonságok teljesülnek rá vonatkozóan:

- Egy adott elektronikus dokumentum lenyomatának ismeretében gyakorlatilag nem lehetséges a lenyomatból a dokumentumot visszaállítani.
- Egy adott elektronikus dokumentum és az ebből a dokumentumból készült lenyomat ismeretében gyakorlatilag nem lehetséges olyan másik elektronikus dokumentumot előállítani, amely az eredetitől eltér, azonban a belőle származtatott lenyomat azonos volna a már ismert lenyomattal.
- Gyakorlatilag lehetetlen két olyan, egymástól különböző elektronikus dokumentumot előállítani, amelyek lenyomata azonos.

A jelen határozat alapján megfelelőnek minősíthető kriptográfiai lenyomatképző függvényeket a következő táblázat sorolja fel. A harmadik oszlopban találhatók az egyes függvényekhez kapcsolódó normatív hivatkozások, a hivatkozott dokumentumok teljes címe a 7. fejezetben található meg. A negyedik oszlopban található hivatkozás azt jelzi, hogy az [ALGO] adott fejezetében hol találhatók meg az adott függvényre vonatkozó bővebb információk.

Lenyomat-képző függvény rövid neve	Elfogadás dátuma	Normatív hivatkozás	Meghatározás az [ALGO] alapján	Alkalmazható
sha1	2001.01.01	ISO/IEC 10118-3 [1], FIPS Publication 180-3 [2]	5.2.1	2011.12.31-ig
ripemd160	2001.01.01	ISO/IEC 10118-3 [1]	5.2.2	2011.12.31-ig
sha224	2004.	FIPS Publication 180-3 [2]	5.2.3	2. számú melléklet szerint
sha256	2004.	ISO/IEC 10118-3 [1], FIPS Publication 180-3 [2]	5.2.4	2. számú melléklet szerint
whirlpool	2004.	ISO/IEC 10118-3 [1]	5.2.5	2. számú melléklet szerint
sha384	2007.03.31	FIPS Publication 180-3 [2]	5.2.6	2. számú melléklet szerint
sha512	2007.03.31	FIPS Publication 180-3 [2]	5.2.7	2. számú melléklet szerint

2. Táblázat: Megfelelő lenyomatképző függvények

3. Megfelelő feltöltő algoritmusok

Bizonyos algoritmusok alkalmazásánál megfelelő feltöltő algoritmusok használata is szükséges (ld: 1. Táblázat). Ilyen például az RSA aláíró algoritmus. A megfelelő feltöltő algoritmusok listája a következő táblázatban található. A feltöltő algoritmusnak legalább *MinSaltEntropy* bitnyi valódi véletlenszámot, vagy bemeneti entrópiát kell tartalmaznia. A véletlenszám generálási módszerek és paraméterek leírását lásd a 6. fejezetben. A negyedik oszlopban találhatók az egyes függvényekhez kapcsolódó normatív hivatkozások, a hivatkozott dokumentumok teljes címe a 7. fejezetben található meg. A feltöltő algoritmusokkal kapcsolatban további információkat az [ALGO] 7.2 fejezet tartalmaz.

Feltöltő algoritmus rövid neve	Véletlenszám generálási módszer	Véletlenszám generálási paraméter	Normatív hivatkozás	Alkalmazható
emsa-pkcs1-v1.5[1]	-	-	RFC 3447 [3]	2. számú melléklet szerint
emsa-pkcs1-v2.1	-	-	RFC 3447 [3], 9.2. fejezet	2. számú melléklet szerint
emsa-pss	trueran vagy pseuran	MinSaltEntropy	RFC 3447 [3], 9.1. fejezet	2. számú melléklet szerint
iso9796-ds2	trueran vagy pseuran	MinSaltEntropy	ISO/IEC 9796-2 [4]	2. számú melléklet szerint
iso9796-din-rn	trueran vagy pseuran	MinSaltEntropy	DIN 66291-1 [5]	2. számú melléklet szerint
iso9796-ds3	-	-	ISO/IEC 9796-2 [4]	2. számú melléklet szerint

3. Táblázat: Megfelelő feltöltő algoritmusok

[1] Az emsa-pkcs1-v1.5 használata új rendszerekben már nem javasolt, mivel előreláthatólag a jövőben kivezetésre kerül.

4. Megfelelő aláíró algoritmusok

A jelen határozat kiadásának idején megfelelőnek tartott aláíró algoritmusok listáját a következő táblázat tartalmazza. A második oszlopban hivatkozott kulcselőállítási algoritmusokkal kapcsolatban lásd az 5. fejezetet. A harmadik oszlopban találhatók az egyes függvényekhez kapcsolódó normatív hivatkozások, a hivatkozott dokumentumok teljes címe a 7. fejezetben található meg. A negyedik oszlopban található hivatkozás azt jelzi, hogy az [ALGO] melyik fejezetében találhatók meg az adott függvényre vonatkozó bővebb információk.

Aláíró algoritmus rövid neve	Kulcs és paraméter előállítási algoritmusok	Normatív hivatkozás	Meghatározás az [ALGO] alapján	Alkalmazható
rsa	rsagen1	RFC 3447 [3]	6.1.2.1	2. számú melléklet szerint
dsa	dsagen1	FIPS Publication 186-3 [6], ISO/IEC 14888-3:2006 [7]	6.1.2.2	2. számú melléklet szerint
ecdsa-Fp	ecgen1	ANSI X9.62 [8]	6.1.2.3	2. számú melléklet szerint
ecdsa-F2m	ecgen2	ANSI X9.62 [8]	6.1.2.4	2. számú melléklet szerint
ecgdsa-Fp	ecgen1	ISO/IEC 1488-3 [9]	6.1.2.5	2. számú melléklet szerint
ecgdsa-F2m	ecgen2	ISO/IEC 1488-3 [9]	6.1.2.6	2. számú melléklet szerint

4. Táblázat: Megfelelő aláíró algoritmusok

5. Megfelelő kulcselőállítási algoritmusok

A jelen határozat kiadásának idején megfelelőnek minősíthető kulcselőállítási algoritmusokat a következő táblázat tartalmazza. A második oszlopban hivatkozott aláíró algoritmusokkal kapcsolatban lásd a 4. fejezetet. A véletlenszám generálási módszerek és paraméterek leírását lásd az 6. fejezetben. A hatodik oszlopban találhatók az egyes algoritmusokhoz kapcsolódó normatív hivatkozások, a hivatkozott dokumentumok teljes címe a 7. fejezetben található meg. A hetedik oszlopban található hivatkozás azt jelzi, hogy az [ALGO] adott fejezetében találhatók meg az adott algoritmusra vonatkozó bővebb információk.

Rövid név	Aláíró algoritmus	Véletlenszám generálási módszer	Véletlenszám generálási paraméter	Elfogadás dátuma	Normatív meghatározás	Meghatározás az [ALGO] alapján	Alkalmazható
rsagen1	rsa	trueran vagy pseuran	EntropyBits vagy SeedEntropy	2001.01.01		6.2.2.1	2. számú melléklet szerint
dsagen1	dsa	trueran vagy pseuran	EntropyBits vagy SeedEntropy	2001.01.01	FIPS Publication 186-3 [6]	6.2.2.2	2. számú melléklet szerint
ecgen1	ecdsa-Fp, ecgdsa-Fp	trueran vagy pseuran	EntropyBits vagy SeedEntropy	2001.01.01.		6.2.2.3 6.2.2.5	2. számú melléklet szerint
ecgen2	ecdsa-F2m, ecgdsa-F2m	trueran vagy pseuran	EntropyBits vagy SeedEntropy	2001.01.01.		6.2.2.4 6.2.2.6	2. számú melléklet szerint

5. Táblázat: Megfelelő kulcselőállítási algoritmusok

6. Megfelelő véletlenszám generálási módszerek

A kulcselőállítási algoritmusok és bizonyos kriptográfiai algoritmuskészletek szükségessé teszik véletlenszámok generálását is. A véletlenszám generálási módszereknek és a kulcselőállítási algoritmusoknak együttesen biztosítaniuk kell, hogy egy kritpográfiai kulcs találgatással való megfejtésének az esélye azonos legyen egy EntropyBits, illetve SeedEntropy bithosszúságú véletlenszám eltalálálásának esélyével. A véletlenszámokkal és generálásukkal kapcsolatos további információk az [ALGO] 8.1 és 8.2 fejezetében és E Mellékletében, valamint a [10] szabványban találhatók.

A következő táblázat a megfelelő véletlenszám generálási módszerek felsorolását tartalmazza. A harmadik oszlopban található paraméter a generálandó véletlenszám hosszát determinálja bitekben kifejezve. Az ötödik oszlop tartalmazza az [ALGO] azon fejezetének megjelölését, amely az adott véletlenszám generálási módszerrel kapcsolatban további információt tartalmaz.

Rövid megnevezés	Jellemző	Generátor paraméter	Elfogadás dátuma	[ALGO] hivatkozás	Alkalmazható
trueran	nem determinisztikus véletlenszám generátor (NRNG)	EntropyBits	2001.01.01	8.2.1	2. számú melléklet szerint
pseuran	determinisztikus véletlenszám generátor (DRNG)	SeedEntropy	2001.01.01	8.2.2	2. számú melléklet szerint

6. Táblázat: Megfelelő véletlenszám generálási módszerek

7. Dokumentumjegyzék

[1] ISO/IEC 10118-3 (2004): "Information technology - Security techniques - Hash functions - Part 3: Dedicated hash functions"

[2] FIPS Publication 180-3 (2008): "Secure Hash Standard (SHS)"

[3] IETF RFC 3447 (2003): "Public-Key Cryptography Standards (PKCS) #1: RSA Cryptography Specifications Version 2.1"

[4] ISO/IEC 9796-2 (2002): "Information technology - Security techniques - Digital signature schemes giving message recovery - Part 2: Integer factorization based mechanisms" (nem keverendő össze az ISO/IEC 9796-2 (1997): „Mechanisms using a hash-function” című dokumentummal)

[5] DIN V 66291-1: "Chip cards with digital signature application/function according to SigG and SigV - Part 1: Application interface"

[6] FIPS Publication 186-3 (2008): "Digital Signature Standard (DSS)"

[7] ISO/IEC 14888-3 (2006): "Information technology - Security techniques - Digital signatures with appendix - Part 3: Discrete logarithm based mechanisms"

[8] ANSI X9.62 (2005): "Public Key Cryptography for the Financial Services Industry: The Elliptic Curve Digital Signature Algorithm (ECDSA)"

[9] ISO/IEC 15946-2 (withdrawn): "Information technology - Security techniques – Cryptographic techniques based on elliptic curves - Part 2: Digital signatures"

[10] ISO/IEC 18031 (2005): "Information technology - Security techniques - Random bit generation"

2. számú melléklet az EF/26838-8,9,10,11,12,13/2011 számú határozatokhoz

Az elektronikus aláírással kapcsolatos szolgáltatások területén alkalmazható kriptográfiai algoritmusokról és paraméterekről szóló határozat 2. számú melléklete

Tartalomjegyzék

1. Bevezetés

A következő táblázatok tájékoztató jelleggel tartalmazzák a jelen határozat 1. számú mellékletében meghatározott kriptográfiai algoritmusok felhasználási idejére vonatkozó ajánlásokat. A melléklet célja az elektronikus aláírások és a kapcsolódó szolgáltatások felhasználása kapcsán érdekeltek (szolgáltatók, aláírók, érintett felek, szoftverfejlesztők, stb.) tájékoztatása, illetve a kriptográfiai algoritmusok területén várható fejlődés előrejelzése. A táblázatok összeállítása minden esetben a jelenleg rendelkezésre álló ismeretek alapján történt, így nem zárható ki, hogy a jelenlegi ajánlásokhoz képest a felhasználási idők hosszabbodnak, vagy rövidülnek. A táblázatok csak azon algoritmusok és paraméterek vonatkozásában tartalmaznak ajánlásokat, amelyek esetében a jelenlegi ismeretek alapján ilyen ajánlás tehető. Amennyiben egy adott algoritmus, vagy egy adott paraméter vonatkozásában a táblázatok nem tartalmaznak a felhasználási időre vonatkozó ajánlást, az azt jelenti, hogy a jelenlegi ismeretek alapján ilyen ajánlás nem fogalmazható meg, azonban nem jelenti azt, hogy az adott algoritmus, vagy az adott paraméter nem volna ajánlott, vagy a biztonsága kétséges volna. A Hatóság az Eat. 18. § szerinti feladat- és hatáskörében folyamatosan figyelemmel kíséri a kriptográfia területén bekövetkező fejlődést, és szükség esetén a biztonságosnak tekinthető kriptográfiai algoritmusokról és paraméterekről új határozatban fog rendelkezni. Az elektronikus aláírással kapcsolatos szolgáltatások nyújtóinak és az egyéb érdekelteknek azonban szintén követniük kell az algoritmusok biztonságát érintő változásokat, és szükség esetén meg kell tenniük a megfelelő intézkedéseket az elektronikus aláírások és a kapcsolódó szolgáltatások megbízhatóságának fenntartására akkor is, ha a Hatóság ez ügyben még nem hozott új határozatot.

A jelen mellékletben szereplő felhasználási időkre vonatkozó ajánlások nem jelentenek kötelezően betartandó előírást sem az elektronikus aláírással kapcsolatos szolgáltatások nyújtói, sem az egyéb érintettek számára. A szolgáltatók számára a jelen határozat 1. számú mellékletében foglaltak alkalmazása kötelező. A jelenleg biztonságosnak minősülő kriptográfiai algoritmusok és paraméterek felhasználási idejének meghatározásánál a szolgáltatóknak és egyéb érdekelteknek azonban indokolt figyelembe venniük a jelen mellékletben felsorolt ajánlások mellett a felhasználás tervezett célját és időtávját, az informatikai környezet adottságait, valamint azt is, hogy a kriptográfiai algoritmusok biztonságának meggyengülése adott esetben rendkívüli intézkedéseket (például tanúsítványok lejárat előtti visszavonása, aláírás-létrehozó adatok cseréje, aláírás-létrehozó eszközök cseréje) tehetnek szükségessé. Minél hosszabb a tervezett felhasználási idő, annál inkább indokolt a kriptográfiai algoritmusok várható meggyengülésére már előre felkészülni (más, erősebb algoritmusok, vagy paraméterek választásával, vagy a migráció lehetőségének megfelelő biztosításával)

A jelen dokumentum is erősen támaszkodik az elektronikus aláírással kapcsolatos szolgáltatások területén mértékadó szabványjellegű és egyéb dokumentumokra, kiemelten az ETSI TS 102 176-1 V 2.2.2 (2011-07) (továbbiakban: [ALGO]) dokumentumra. A táblázatokban használt megnevezések és rövidítések jelentése azonos a jelen határozat 1. számú mellékletében alkalmazottal.

2. Kriptográfiai algoritmuskészletek

A következő táblázatban található felhasználási időkre vonatkozó ajánlások a jelen határozat kiadásakor rendelkezésre álló ismeretek alapján megállapított becslések arra vonatkozóan, hogy az adott kriptográfiai algoritmuskészlet a megjelölt év végéig az adott célra alkalmazva előreláthatólag a követelményeknek megfelel. Tekintettel a kriptográfia fejlődésére és a számítási erőforrások gyors növekedésére, a határozat nem tartalmaz 6 évnél hosszabb felhasználási időkre vonatkozó ajánlásokat, amennyiben egy algoritmuskészlet a jelenlegi ismeretek szerint ennél hosszabb ideig is megfelelő lehet, akkor az a táblázatban a „legalább 2017" jelöléssel szerepel. Az ajánlások szerepeltetésének célja az, hogy megkönnyítse a szolgáltatók, illetve a szolgáltatásokat igénybe vevők, valamint az érintett felek számára a megfelelő kriptográfiai algoritmuskészlet kiválasztását, a kiválasztás azonban a konkrét esetben elvégzett mérlegelés eredménye kell, hogy legyen. Fel kell hívni a figyelmet arra, hogy az ajánlott felhasználási idők a jövőben ismertté váló új tények hatására rövidülhetnek, vagy meg is hosszabbodhatnak. Az ezzel kapcsolatos fejlemények figyelemmel kísérése a szolgáltatók kötelessége, de a felhasználók és érintett felek számára is ajánlott. A megfelelő algoritmuskészletek körében bekövetkezett változások a Nemzeti Média- és Hírközlési Hatóság részéről új határozat kiadását vonják maguk után, azonban a szolgáltatóknak a szükségessé váló intézkedéseket már ezt megelőzően is meg kell tenniük, ha ez indokolt. A táblázat csak azokkal a kriptográfiai algoritmuskészletekkel kapcsolatban tartalmaz felhasználási időkre vonatkozó ajánlásokat, amelyekkel kapcsolatban a jelenlegi ismeretek alapján ilyen ajánlások már megfogalmazhatóak. Az ajánlott felhasználási időkkel kapcsolatban az [ALGO] 9.3 fejezete tartalmaz további információkat.

Kriptográfiai algoritmuskészlet rövid neve	Kulcshossz	Ajánlott felhasználási idő
sha1-with-rsa	-	használata nem ajánlott
sha224-with-rsa	1024	használata nem ajánlott
	1536	2012
	2048	2017
sha256-with-rsa	1024	használata nem ajánlott
	1536	2012
	2048	2017
rsa-pss with mgf1SHA1Identifier	1024	használata nem ajánlott
	1536	2012
	2048	2012
rsa-pss with mgf1SHA224Identifier	1024	használata nem ajánlott
	1536	2012
	2048	2017
rsa-pss with mgf1SHA256Identifier	1024	használata nem ajánlott
	1536	2012
	2048	2017
sha1-with-dsa	-	használata nem ajánlott
sha1-with-ecdsa	-	használata nem ajánlott
sha224-with-ecdsa	224	2017
sha256-with-ecdsa	256	legalább 2017

1. Táblázat: Kriptográfiai algoritmuskészletek felhasználási idejére vonatkozó ajánlások

3. Kriptográfiai lenyomatképző függvények

A következő táblázatban található felhasználási időkre vonatkozó ajánlások a jelen határozat kiadásakor rendelkezésre álló ismeretek alapján megállapított becslések arra vonatkozóan, hogy az adott lenyomatképző függvény a megjelölt év végéig az adott célra alkalmazva előreláthatólag a követelményeknek megfelel. Tekintettel a kriptográfia fejlődésére és a számítási erőforrások gyors növekedésére, a határozat nem tartalmaz 6 évnél hosszabb felhasználási időkre vonatkozó ajánlásokat, amennyiben egy függvény a jelenlegi ismeretek szerint ennél hosszabb ideig is megfelelő lehet, akkor az a táblázatban a „legalább 2017” jelöléssel szerepel. Az ajánlások szerepeltetésének célja az, hogy megkönnyítse a szolgáltatók, illetve a szolgáltatásokat igénybe vevők, valamint az érintett felek számára a megfelelő lenyomatképző függvény kiválasztását, a kiválasztás azonban a konkrét esetben elvégzett mérlegelés eredménye kell, hogy legyen. Fel kell hívni a figyelmet arra, hogy az ajánlott felhasználási idők a jövőben ismertté váló új tények hatására rövidülhetnek, vagy meg is hosszabbodhatnak. Az ezzel kapcsolatos fejlemények figyelemmel kísérése a szolgáltatók kötelessége, de a felhasználók és érintett felek számára is ajánlott. A megfelelő lenyomatképző függvények körében bekövetkezett változások a Nemzeti Média- és Hírközlési Hatóság részéről új határozat kiadását vonják maguk után, azonban a szolgáltatóknak a szükségessé váló intézkedéseket már ezt megelőzően is meg kell tenniük, ha ez indokolt. Amennyiben az elektronikus aláírás hosszú távú ellenőrizhetősége szükséges, akkor a szolgáltatók és a felhasználók számára az SHA-384, illetve SHA-512 használata ajánlott.

Lenyomatképző függvény rövid neve	Ajánlott felhasználási idő
sha1	használata nem ajánlott
ripemd160	használata nem ajánlott
sha224	2017
sha256	2017
whirlpool	legalább 2017
sha384	legalább 2017
sha512	legalább 2017

2. Táblázat: Lenyomatképző függvények felhasználási idejére vonatkozó ajánlások

4. Feltöltő algoritmusok

A következő táblázatban található felhasználási időkre vonatkozó ajánlások a jelen határozat kiadásakor rendelkezésre álló ismeretek alapján megállapított becslések arra vonatkozóan, hogy az adott feltöltő algoritmus a megjelölt paraméterek alkalmazása esetén a megjelölt év végéig előreláthatólag a követelményeknek megfelel. Tekintettel a kriptográfia fejlődésére és a számítási erőforrások gyors növekedésére, a határozat nem tartalmaz 6 évnél hosszabb felhasználási időkre vonatkozó ajánlásokat, amennyiben egy algoritmus a jelenlegi ismeretek szerint ennél hosszabb ideig is megfelelő lehet, akkor az a táblázatban a „legalább 2017” jelöléssel szerepel. Az ajánlások szerepeltetésének célja az, hogy megkönnyítse a szolgáltatók, illetve a szolgáltatásokat igénybe vevők, valamint az érintett felek számára a megfelelő feltöltő algoritmus kiválasztását, a kiválasztás azonban a konkrét esetben elvégzett mérlegelés eredménye kell, hogy legyen. Fel kell hívni a figyelmet arra, hogy az ajánlott felhasználási idők a jövőben ismertté váló új tények hatására rövidülhetnek, vagy meg is hosszabbodhatnak. Az ezzel kapcsolatos fejlemények figyelemmel kísérése a szolgáltatók kötelessége, de a felhasználók és érintett felek számára is ajánlott. A megfelelő feltöltő algoritmusok körében bekövetkezett változások a Nemzeti Média- és Hírközlési Hatóság részéről új határozat kiadását vonják maguk után, azonban a szolgáltatóknak a szükségessé váló intézkedéseket már ezt megelőzően is meg kell tenniük, ha ez indokolt. Az ajánlott felhasználási időkkel kapcsolatban az [ALGO] 9.3 fejezete tartalmaz további információkat.

Feltöltő algoritmus rövid név	MinSaltEntropy	Ajánlott felhasználási idő
emsa-pkcs1-v1.5	-	2017
emsa-pkcs1-v2.1	-	2017
emsa-pss	64	legalább 2017
iso9796-ds2	64	legalább 2017
iso9796-din-rn	64	legalább 2017
iso9796-ds3	-	legalább 2017

3. Táblázat: Feltöltő algoritmusok felhasználási idejére vonatkozó ajánlások

5. Kulcselőállítási algoritmusok

A következő táblázatokban található felhasználási időkre vonatkozó ajánlások a jelen határozat kiadásakor rendelkezésre álló ismeretek alapján megállapított becslések arra vonatkozóan, hogy az adott kulcselőállítási algoritmus a megjelölt paraméterek alkalmazása esetén a megjelölt év végéig az adott célra alkalmazva előreláthatólag a követelményeknek megfelel. Tekintettel a kriptográfia fejlődésére és a számítási erőforrások gyors növekedésére, a határozat nem tartalmaz 6 évnél hosszabb felhasználási időkre vonatkozó ajánlásokat, amennyiben egy algoritmus a jelenlegi ismeretek szerint ennél hosszabb ideig is megfelelő lehet, akkor az a táblázatban a „legalább 2017” jelöléssel szerepel. Az ajánlások szerepeltetésének célja az, hogy megkönnyítse a szolgáltatók, illetve a szolgáltatásokat igénybe vevők, valamint az érintett felek számára a megfelelő kulcsgenerálási algoritmus kiválasztását, a kiválasztás azonban a konkrét esetben elvégzett mérlegelés eredménye kell, hogy legyen. Fel kell hívni a figyelmet arra, hogy az ajánlott felhasználási idők a jövőben ismertté váló új tények hatására rövidülhetnek, vagy meg is hosszabbodhatnak. Az ezzel kapcsolatos fejlemények figyelemmel kísérése a szolgáltatók kötelessége, de a felhasználók és érintett felek számára is ajánlott. A megfelelő kulcselőállítási algoritmusok körében bekövetkezett változások a Nemzeti Média- és Hírközlési Hatóság részéről új határozat kiadását vonják maguk után, azonban a szolgáltatóknak a szükségessé váló intézkedéseket már ezt megelőzően is meg kell tenniük, ha ez indokolt. A táblázatokban az ajánlott felhasználási időket úgy kell érteni, hogy az adott algoritmusok adott paraméterekkel való felhasználása olyan kulcsok esetében ajánlott, amelyek tervezett élettartama nem haladja meg az ajánlott felhasználási időt. Az ajánlott felhasználási időkkel kapcsolatban az [ALGO] 9.3 fejezete tartalmaz további információkat.

A következő táblázat az RSA aláíró- és az rsagen1 kulcselőállítási algoritmus alkalmazása esetén irányadó paramétereket és ajánlott felhasználási időket tartalmazza. A paraméterek értelmezése az [ALGO] 6.1.2.1, illetve 6.2.2.1 fejezetében található.

Paraméter		Ajánlott felhasználási idő
MinModLen	1024	használata nem ajánlott
	1536	2012
	2048	2017
ErrProb	2^{-80}	2012
	2^{-100}	legalább 2017
SeedEntropy/EntropyBits	80	2012
	100	2017

4. Táblázat: Felhasználási időkre vonatkozó ajánlások az RSA és az rsagen1 algoritmusok alkalmazása esetén

A következő táblázat a DSA aláíró- és a dsagen1 kulcselőállítási algoritmus alkalmazása esetén irányadó paramétereket és ajánlott felhasználási időket tartalmazza. A paraméterek értelmezése az [ALGO] 6.1.2.2, illetve 6.2.2.2 fejezetében található.

Paraméter		Ajánlott felhasználási idő
pMinLen	1024	2012
	2048	2014
	3072	legalább 2017
qMinLen	160	2012
	224	2014
	256	legalább 2017
ErrProb	2^{-80}	2014
	2^{-100}	legalább 2017
SeedEntropy / EntropyBits	80	2014
	100	legalább 2017

5. Táblázat: Felhasználási időkre vonatkozó ajánlások a DSA és a dsagen1 algoritmusok alkalmazása esetén

A következő táblázat az ecdsa-Fp vagy ecgdsa-Fp aláíró- és az ecgen1 kulcselőállítási algoritmus alkalmazása esetén irányadó paramétereket és ajánlott felhasználási időket tartalmazza. A paraméterek értelmezése az [ALGO] 6.1.2.3, 6.1.2.5, illetve 6.2.2.3, 6.2.2.5 fejezetében található.

Paraméter		Ajánlott felhasználási idő
pMinLen	-	-
qMinLen	160	2012
	224	2014
	256	legalább 2017
r0min	104	2017
MinClass	200	2017
ErrProb	2^{-80}	2012
	2^{-100}	legalább 2017
SeedEntropy / EntropyBits	80	2012
	100	2017
	256	legalább 2017

6. Táblázat: Felhasználási időkre vonatkozó ajánlások az ecdsa-Fp és az ecgen1 algoritmusok alkalmazása esetén

A következő táblázat az ecdsa-F2m vagy ecgdsa-F2m aláíró- és az ecgen2 kulcselőállítási algoritmus alkalmazása esetén irányadó paramétereket és ajánlott felhasználási időket tartalmazza. A paraméterek értelmezése az [ALGO] 6.1.2.4, 6.1.2.6, illetve 6.2.2.4, 6.2.2.6 fejezetében található.

Paraméter		Ajánlott felhasználási idő
pmMinLen	-	-
qMinLen	160	2012
	224	2014
	256	legalább 2017
r0min	104	2017
MinClass	200	2017
ErrProb	2^{-80}	2012
	2^{-100}	legalább 2017
SeedEntropy / EntropyBits	80	2012
	100	2017
	256	legalább 2017

7. Táblázat: Felhasználási időkre vonatkozó ajánlások az ecdsa-F2m és az ecgen2 algoritmusok alkalmazása esetén