Nemzeti Hírközlési Hatóság Hivatala

Informatikai Szabályozási Igazgatóság

**Molnár Sándor**
infokommunikációs divízió
igazgató részére

MÁV Informatika Kereskedelmi,
Szolgáltató és Tanácsadó Zrt.

*1012 Budapest,*
*Krisztina krt. 37/a*

Ügyiratszám: HL-21917-11/2008
Dátum: 2008. július 9.
Ügyintéző:
Tárgy: Határozat
Melléklet: 2 db

A Nemzeti Hírközlési Hatóság Hivatala (továbbiakban: Hatóság) a **MÁV Informatika Kereskedelmi, Szolgáltató és Tanácsadó Zrt. (székhely: 1012 Budapest, Krisztina krt. 37/a., Cg: 01-10-045838, nyilvántartja a Fővárosi Bíróság, mint Cégbíróság),** 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 (továbbiakban: Ket.)* 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.

A jelen eljárásban eljárási költség nem merült fel, így annak viseléséről rendelkezni nem kell.

Jelen határozat ellen annak közlésétől számított tizenöt napon belül a Nemzeti Hírközlési Hatóság Tanácsa 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 Forint értékű illetékbélyeget. A fellebbezés elektronikus úton történő benyújtására nincsen mód.

## Indokolás

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 **HL-21917-4/2008** számú, **2008. június 4**-én kelt levelében értesítette. Az eljárás megindítására azért került sor, mert a European Telecommunications Standards Institute (ETSI) ETSI TS 102 176-1 v 2.0.0 (2007-11) számon, „Electronic Signatures and Infrastructures (ESI); Algorithms and Parameters for Secure Electronic Signatures; Part 1: Hash functions and assymetric algorithms” címmel közzétette a biztonságos elektronikus aláírások létrehozására ajánlott kriptográfiai algoritmusok és paraméterek jegyzékét, melynek nyomán a Hatóság jelenleg is hatályos, **HL-20336-6, -7, -8 és -9/2005 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.) szabályai került sor.

Az eljárás során a Hatóság felhasználta a fent hivatkozott ETSI TS 102 176-1 v 2.0.0 (2007-11) 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, ugyanakkor nem tartalmaz normatív rendelkezéseket ezek felhasználhatósági idejével kapcsolatban. A **2. számú mellékletben** szereplő felhasználási időkre vonatkozó ajánlások csupán 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.

Az eljárási költség megállapítása a Ket. 153. § (1) és (2) bekezdése alapján történt.

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.

Az NHH Hivatalának Főigazgatója
nevében és megbízásából:

Dr. Sylvester Nóra
Igazgató

Kapják:

- Szolgáltató
- Jogerőre emelkedés után: Irattár helyben

1. számú melléklet a HL-21917-9/2008 számú határozathoz

**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 2.0.0 (2007-11) (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 név | Lenyomatképző függvény rövid név | Feltöltő algoritmus rövid név | Aláíró algoritmus rövid név |
|---|---|---|---|
| sha1-with-rsa | sha1 | Az RSA aláíró algoritmus használata esetén a feltöltő algoritmus a 2. fejezetbeli listából választható | rsa |
| sha1-with-dsa | sha1 | nem szükséges | dsa |
| ripemd160-with-rsa | ripemd160 | Az RSA aláíró | rsa |

| | | | |
|---|---|---|---|
| | | algoritmus használata esetén a feltöltő algoritmus a 2. fejezetbeli listából választható | |
| ripemd160-with-dsa | ripemd160 | nem szükséges | dsa |
| sha224-with-rsa | sha224 | Az RSA aláíró algoritmus használata esetén a feltöltő algoritmus a 2. fejezetbeli listából választható | rsa |
| sha256-with-rsa | sha256 | Az RSA aláíró algoritmus használata esetén a feltöltő algoritmus a 2. fejezetbeli listából választható | rsa |
| rsa-pss with mgf1SHA1Identifier | mgf1-SHA1 | | rsa |
| rsa-pss with mgf1-SHA224Identifier | mgf1-SHA224 | | rsa |
| rsa-pss with mgf1-SHA256Identifier | mgf1-SHA256 | | rsa |
| sha1-with-ecdsa | sha1 | nem szükséges | ecdsa-Fp vagy ecdsa-F2m |
| sha1-with-ecgdsa | sha1 | nem szükséges | ecgdsa-Fp vagy ecgdsa-F2m |
| sha224-with-ecdsa | sha224 | nem szükséges | ecdsa-Fp vagy ecdsa-F2m |
| sha256-with-ecdsa | sha256 | nem szükséges | ecdsa-Fp vagy ecdsa-F2m |
| sha384-with-ecdsa | sha384 | nem szükséges | ecdsa-Fp vagy ecdsa-F2m |
| sha512-with-ecdsa | sha512 | nem szükséges | ecdsa-Fp vagy ecdsa-F2m |
| ecdsa-with-RIPEMD160 | ripemd160 | nem szükséges | ecdsa-Fp vagy ecdsa-F2m |

**1. táblázat: Megfelelő kriptográfiai algoritmuskészletek**

## 2. Megfelelő kriptográfiai lenyomatképző függvények:

A kriptográfiai lenyomatképző függvényekkel szembeni követelményeket az Eat. 2. § 26. pont 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.

| Lenyomatképző függvény rövid neve | Elfogadás dátuma | Normatív hivatkozás | Meghatározás az [ALGO] alapján |
|---|---|---|---|
| sha1 | 2001. jan. 1. | ISO/IEC 10118-3 [1] és FIPS Publication 180-2 [2] | 5.2.1 |
| ripemd160 | 2001. jan. 1. | ISO/IEC 10118-3 [1] | 5.2.2 |
| sha224 | 2004. | FIPS Publication 180-2 [2] | 5.2.3 |
| sha256 | 2004. | ISO/IEC 10118-3 [1] és FIPS Publication 180-2 [2] | 5.2.4 |
| whirlpool | 2004. | ISO/IEC 10118-3 [1] | 5.2.5 |
| sha384 | 2007. márc. 31. | FIPS Publication 180-2 [2] | 5.2.6 |
| sha512 | 2007. márc. 31. | FIPS Publication 180-2 [2] | 5.2.7 |

**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 név | Véletlenszám generálási módszer | Véletlenszám generálási paraméterek | Normatív hivatkozás |
|---|---|---|---|
| emsa-pkcs1-v1.5[1] | - | - | RFC 3447 [3] |
| emsa-pkcs1-v2.1 | - | - | RFC 3447 [3], 9.2. fejezet |
| emsa-pss | trueran/pseuran | MinSaltEntropy | RFC 3447 [3], 9.1. fejezet |
| iso9796-ds2 | trueran/pseuran | MinSaltEntropy | ISO/IEC 9796-2 [4] |
| iso9796-din-rn | trueran/pseuran | MinSaltEntropy | DIN 66291-1 [5] |
| iso9796-ds3 | - | - | ISO/IEC 9796-2 [4] |

**3. Táblázat: Megfelelő feltöltő algoritmusok**

## 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] adott fejezetében találhatók meg az adott függvényre vonatkozó bővebb információk.

| Aláíró algoritmus rövid neve | Kulcs és paraméter előállítási algoritmusok | Normatív hivatkozás | Meghatározás az [ALGO] alapján |
|---|---|---|---|
| rsa | rsagen1 | RFC 3447 [3] | 6.1.2.1 |
| dsa | dsagen1 | FIPS Publication 186-2 [6], ISO/IEC 14888-3:2006 [7] | 6.1.2.2 |
| ecdsa-Fp | ecgen1 | ANSI X9.62 [8] | 6.1.2.3 |
| ecdsa-F2m | ecgen2 | ANSI X9.62 [8] | 6.1.2.4 |
| ecgdsa-Fp | ecgen1 | ISO/IEC 15946-2 (2002) [9] | 6.1.2.5 |
| ecgdsa-F2m | ecgen2 | ISO/IEC 15946-2 (2002) [9] | 6.1.2.6 |

**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

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

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 paraméterek | Elfogadás dátuma | Normatív meghatá-rozás | Meghatározás az [ALGO] alapján |
|---|---|---|---|---|---|---|
| rsagen1 | rsa | trueran pseuran | EntropyBits vagy SeedEntropy | 2001. jan. 01. | | 6.2.2.1 |
| rsagen2 | dsa | trueran pseuran | EntropyBits vagy SeedEntropy | 2001. jan. 01. | FIPS Publication 186-2 [6] | 6.2.2.2 |
| ecgen1 | ecdsa-Fp, ecgdsa-Fp | trueran pseuran | EntropyBits vagy SeedEntropy | 2001. jan. 01. | | 6.2.2.3 6.2.2.5 |
| ecgen2 | ecdsa-F2m, ecgdsa-F2m | trueran pseuran | EntropyBits vagy SeedEntropy | 2001. jan. 01. | | 6.2.2.4 6.2.2.6 |

**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 |
|---|---|---|---|---|
| trueran | nem determinisztikus véletlenszám generátor (NRNG) | EntropyBits | 2001. jan. 1. | 8.2.1 |
| pseuran | determinisztikus véletlenszám generátor (DRNG) | SeedEntropy | 2001. jan. 1. | 8.2.2 |

**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 180-2 (2002): "Secure Hash Standard" with Change Notice to include SHA-224
[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"
[6] FIPS Publication 186-2 (2000): "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 (2002): "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 a HL-21917-9/2008 számú határozathoz

**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 2.0.0 (2007-11) (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 5 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 2012” 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 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[2] | |
|---|---|---|---|
| | | Dokumentumok, időbélyegek aláírása | Tanúsítványok aláírása |
| sha1-with-rsa | 1024 | 2008 | 2009 |
| sha224-with-rsa | 1024 | 2008 | 2008 |
| | 1536 | 2009 | 2009 |
| | 2048 | legalább 2012 | legalább 2012 |
| sha256-with-rsa | 1024 | 2008 | 2008 |
| | 1536 | 2009 | 2009 |
| | 2048 | legalább 2012 | legalább 2012 |
| rsa-pss with mgf1SHA1Identifier | 1024 | 2008 | 2008 |
| | 1536 | 2009 | 2009 |
| | 2048 | legalább 2012 | legalább 2012 |
| rsa-pss with mgf1SHA224Identifier | 1024 | 2008 | 2008 |
| | 1536 | 2009 | 2009 |
| | 2048 | legalább 2012 | legalább 2012 |
| rsa-pss with mgf1SHA256Identifier | 1024 | 2008 | 2008 |
| | 1536 | 2009 | 2009 |
| | 2048 | legalább 2012 | legalább 2012 |
| sha1-with-dsa | 1024 | 2008 | 2009 |
| sha1-with-ecdsa | 163 | 2008 | 2009 |
| sha224-with-ecdsa | 224 | legalább 2012 | legalább 2012 |
| sha256-with-ecdsa | 256 | legalább 2012 | legalább 2012 |

**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 5 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 2012” 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 Hírközlési Hatóság részéről új határozat kiadását vonják maguk után, azonban a szolgáltatóknak a szükségessé váló intézkedéseket már ezt megelőzően

[2] A szolgáltató dönthet úgy, hogy az olyan algoritmuskészleteket, amelyek ajánlott felhasználási ideje 2008. év végéig tart, a szolgáltatás nyújtása során 2009. év végéig használja fel, azonban ebben az esetben megfelelően fel kell készülnie arra, hogy az algoritmuskészlet meggyengülése esetén a szükséges intézkedéseket haladéktalanul meg tudja tenni és ennek érdekében az előfizetőkkel is ennek megfelelően kell megállapodnia.

is meg kell tenniük, ha ez indokolt. A szolgáltatóknak ajánlott megfelelő tervezéssel felkészülni arra az esetre, ha az SHA-1 és a RIPEMD-160 meggyengülése a most látható időpont előtt bekövetkezne és ezért rövidtávú kiváltásuk válna szükségessé, a felhasználók számára pedig ajánlott, hogy elektronikus aláírást alkalmazó rendszereikben térjenek át legalább az SHA-224 illetve SHA-256 használatára. Amennyiben az elektronikus aláírás hosszú távú ellenőrizhetősége szükséges, akkor az SHA-384, illetve SHA-512 használata ajánlott.

| Lenyomatképző függvény rövid neve | Ajánlott felhasználási idő | |
|---|---|---|
| | Dokumentumok, időbélyegek aláírása | Tanúsítványok aláírása |
| sha1 | 2008 | 2009 |
| ripemd160 | 2009 | 2009 |
| sha224 | 2012 | 2012 |
| sha256 | 2012 | 2012 |
| whirlpool | legalább 2012 | legalább 2012 |
| sha384 | legalább 2012 | legalább 2012 |
| sha512 | legalább 2012 | legalább 2012 |

**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 megjelelölt 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 5 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 2012” 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 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 | - | 2012 |
| emsa-pkcs1-v2.0 | - | 2012 |
| emsa-pss | 64 | legalább 2012 |
| iso9796-ds2 | 64 | legalább 2012 |
| iso9796-din-m | 64 | legalább 2012 |
| iso9796-ds3 | - | legalább 2012 |

**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 5 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 2012” 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 Hírközlési Hatóság részéről ami 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[3] | 2008 |
| | 1536 | 2009 |
| | 2048 | 2012 |
| ErrProb | $2^{-80}$ | 2009 |
| | $2^{-100}$ | 2012 |
| SeedEntropy/EntropyBits | 80 | 2009 |
| | 100 | 2012 |

**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 | 2008 |
| | 1536 | 2009 |
| | 2048 | legalább 2012 |
| qMinLen | 160 | 2009 |
| | 224 | legalább 2012 |
| ErrProb | $2^{-80}$ | 2009 |
| | $2^{-100}$ | legalább 2012 |
| SeedEntropy/EntropyBits | 80 | 2009 |
| | 100 | legalább 2012 |

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

A következő táblázat az ecdsa-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, illetve 6.2.2.3 fejezetében található.

| Paraméter | | Ajánlott felhasználási idő |
|---|---|---|
| pMinLen | - | - |
| qMinLen | 160 | 2009 |
| | 224 | 2012 |
| r0min | 104 | 2012 |
| MinClass | 200 | 2012 |
| ErrProb | $2^{-80}$ | 2009 |
| | $2^{-100}$ | legalább 2012 |
| SeedEntropy/EntropyBits | 80 | 2009 |
| | 100 | 2012 |

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

[3] A kulcsokat előállító szolgáltató dönthet úgy is, hogy 1024 bites kulcshosszúságú RSA kulcsokat 2009 végéig tartó élettartammal bocsát ki, ebben az esetben azonban fel kell arra készülnie, hogy az algoritmus biztonságának meggyengülése esetén haladéktalanul megtegye a szükséges intézkedéseket, ideértve a még érvényes tanúsítványok visszavonását és a hozzájuk tartozó kulcsok cseréjét is.

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

| Paraméter | | Ajánlott felhasználási idő |
|---|---|---|
| pMinLen | - | - |
| qMinLen | 160 | 2009 |
| | 224 | 2012 |
| r0min | 104 | 2012 |
| MinClass | 200 | 2012 |
| ErrProb | $2^{-80}$ | 2009 |
| | $2^{-100}$ | legalább 2012 |
| SeedEntropy/EntropyBits | 80 | 2009 |

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

A következő táblázat az ecdsa-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, illetve 6.2.2.4 fejezetében található.

| Paraméter | | Ajánlott felhasználási idő |
|---|---|---|
| mMin | - | - |
| qMinLen | 160 | 2009 |
| | 224 | 2012 |
| r0min | 104 | 2012 |
| MinClass | 200 | 2012 |
| ErrProb | $2^{-80}$ | 2009 |
| | $2^{-100}$ | legalább 2012 |
| SeedEntropy/EntropyBits | 80 | 2009 |
| | 100 | 2012 |

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

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

| Paraméter | | Ajánlott felhasználási idő |
|---|---|---|
| mMin | - | - |
| qMinLen | 160 | 2009 |
| | 224 | 2012 |
| r0min | 104 | 2012 |
| MinClass | 200 | 2012 |
| ErrProb | $2^{-80}$ | 2009 |
| | $2^{-100}$ | legalább 2012 |
| SeedEntropy/EntropyBits | 80 | 2009 |
| | 100 | 2012 |

**8. Táblázat: Felhasználási időkre vonatkozó ajánlások az ecgdsa-F2m és az ecgen2 algoritmusok alkalmazása esetén**