



NEMZETI FEJLESZTÉSI MINISZTERIUM

NÉMETH LÁSZLÓNÉ
miniszter

Szám: *IKF/19515 - 2/2012 - h74*

KIJELÖLÉSI OKIRAT

Az elektronikus aláírási termékek tanúsítását végző szervezetekről, illetve a kijelölésükre vonatkozó szabályokról szóló 9/2005. (VII. 21.) IHM rendelet alapján megállapítom, hogy

HUNGUARD Számítástechnikai-, informatikai kutató-fejlesztő és általános szolgáltató Kft.
1123 Budapest, Kékgolyó utca 6.

a lefolytatott ellenőrzés szerint megfelel a hivatkozott jogszabályban előírt feltételeknek, ezért írásban előterjesztett kérelme alapján

2015. december 31. napjáig

kijelölöm

az elektronikus aláírási termékek megfelelőségének tanúsítására, az alábbi, jelen okirat elválaszthatatlan részét képező mellékletben foglalt mértékadó előírások szerint.

A kijelölt tanúsító szervezet a tevékenységét mindenkor az arra vonatkozó alapvető követelmények következetes és pontos megtartásával, az ilyen tevékenységet ellátó szervezettől elvárható magas színvonalon köteles ellátni. A kijelölt tanúsító szervezet felelős az általa bevont közreműködőkért, akikre vele azonos feltételek vonatkoznak. A kijelölt tanúsító szervezet köteles a bizottság és a hírközlési hatóság által végzett ellenőrzés lefolytatásában közreműködni.

Budapest, 2012. december „*18*”.

Né
Németh Lászlóné

Melléklet: a mértékadó előírásokat tartalmazó lista

Melléklet a IKF/15515-2/2012 számú kijelölési okirathoz

Kijelölt szervezet
HUNGUARD Számítástechnikai-, Informatikai Kutató-fejlesztő és Általános Szolgáltató
Korlátolt Felelősségű Társaság
1123 Budapest, Kékgolyó u. 6.

Tevékenység jellege: az elektronikus aláírási termékek tanúsítása

A tevékenységre vonatkozó mértékadó előírások:

Jogszabályok, irányelvek:

- Az Európai Parlament és a Tanács 1999/93/EK számú Irányelve az elektronikus aláírással kapcsolatos közösségi keretrendszerrel
- 2001. évi XXXV. törvény az elektronikus aláírásról
- 45/2005. (III. 11.) Korm. rendelet a Nemzeti Hírközlési Hatóságnak az elektronikus aláírással kapcsolatos feladat- és hatásköréről, valamint eljárásának részletes szabályairól
- 78/2010. (III. 25.) Korm. rendelet az elektronikus aláírás közigazgatási használatához kapcsolódó követelményekről és az elektronikus kapcsolattartás egyes szabályairól
- 83/2012. (IV. 21.) Korm. rendelet a szabályozott elektronikus ügyintézési szolgáltatásokról és az állam által kötelezően nyújtandó szolgáltatásokról
- 85/2012. (IV. 21.) Korm. rendelet az elektronikus ügyintézés részletes szabályairól
- 114/2007. (XII. 29.) GKM rendelet a digitális archiválás szabályairól
- 3/2005. (III. 18.) IHM rendelet az elektronikus aláírással kapcsolatos szolgáltatásokra és ezek szolgáltatóira vonatkozó részletes követelményekről
- 9/2005. (VII. 21.) IHM rendelet az elektronikus aláírási termékek tanúsítását végző szervezetekről, illetve a kijelölésükre vonatkozó szabályokról
- 13/2005. (X. 27.) IHM rendelet a papíralapú dokumentumokról elektronikus úton történő másolat készítésének szabályairól
- 4/2006. (IV. 19.) IHM rendelet a Nemzeti Hírközlési Hatóságnak az elektronikus aláírással összefüggő nyilvántartással kapcsolatos tevékenységéért fizetendő díjakról
- 7/2002. (IV. 26.) MeHVM rendelet az elektronikus aláírással kapcsolatos szolgáltatási szakértő nyilvántartásba vételéről

Az elektronikus aláírási termékekkel szemben támasztott irányadó követelmények forrásai

Az alább részletezett általános követelmények konzisztens részrendszerét kell az egyes aláírási termékek tanúsítása során irányadónak tekinteni. A konzisztens részrendszert meghatározzák az aláírási termék specifikumai (pl. SmartCard, PC-ben szoftver, kriptográfiai hardver modul stb.), valamint a funkcióval és az alkalmazással szemben meghatározott kockázatelemzés.

- CEN 14167-1:2003 munkacsoport egyezmény: Security Requirements for Trustworthy Systems Managing Certificates for Electronic Signatures
- CWA 14169: 2004 Secure Signature-creation devices "EAL 4+"
- CWA 14170: 2004 Security requirements for signature creation applications
- CWA 14171: 2004 General guidelines for electronic signature verification
- CWA 14890-1:2004 Application Interface for smart cards used as Secure Signature Creation Devices - Part 1: Basic requirements

- CWA 14890-2:2004 Application Interface for smart cards used as Secure Signature Creation Devices - Part 2: Additional Services
- Mobile Signature Service Security Framework; ETSI TR 102 206 V1.1.3 2003-08

Tanúsítványt aláíró kriptográfiai modulra vonatkozó speciális irányadó követelmény rendszer:

ISO/IEC 19790 Information technology -- Security techniques -- Methodology for IT security evaluation (mely megfelel az amerikai FIPS PUB 140-2 szabványnak)

A NIST FIPS (Federal Information Processing Standard) kiadványai közül a FIPS-140-2 kiadvány határozza meg azt a szabványt, amelyet állami szervezeteknek kell az Egyesült Államokban felhasználniuk, ha kriptográfia alapú biztonsági rendszereket akarnak használni érzékeny, vagy értékes adatok védelmére, ennek európai szabványosítása az ISO/IEC 19790.

A Nemzeti Média- és Hírközlési Hatóság iránymutatásai (elérhetők az NMHH honlapján):

- Kriptográfiai algoritmusokra vonatkozó elvárások /A Nemzeti Média- és Hírközlési Hatóság határozatai/: EF-26838-8/2011, EF-26838-9/2011, EF-26838-10/2011, EF-26838-11/2011, EF-26838-12/2011, EF-26838-13/2011 számú határozat a felhasználható biztonságos kriptográfiai algoritmusokról, valamint a hozzájuk tartozó paraméterekről a mellékletekben foglaltaknak megfelelően.
- Ajánlás elektronikus archiválási szolgáltatások nyújtásához felhasznált megbízható rendszerekre vonatkozó biztonsági követelményekre, NHH, 2007.07.07.
- Ajánlás eljárásrendi követelményekre elektronikus aláírás felhasználásával végzett elektronikus archiválási szolgáltatások szolgáltatói számára, NHH, 2007.07.07.
- Elektronikus archiválási szolgáltatásokkal kapcsolatos hatósági tájékoztató, NHH, 2007.07.07.

Kapcsolódó hazai ajánlások:

- **A Közigazgatási Informatikai Bizottság 25. számú ajánlása:** a Magyar Informatikai Biztonsági Ajánlások (MIBA) ajánlóssorozata, amely három fő területre fókuszálva 12, önállóan is használható dokumentumban került megjelentetésre. A MIBA az ITB 8., 12., és 16. számú ajánlásait váltja fel, azok kibővítése és jelentős kiegészítése révén.
 - **A KIB 25. számú ajánlása: 25/2. kötet: Magyar Informatikai Biztonsági Értékelési és Tanúsítási Séma (MIBÉTS) 1.0 verzió**
 - A KIB 25. számú ajánlása: 25/2-1. segédlet: MIBÉTS - Modell és Folyamatok 1.0 verzió
 - A KIB 25. számú ajánlása: 25/2-2. segédlet: MIBÉTS – Útmutató a Megbízók számára 1.0 verzió
 - A KIB 25. számú ajánlása: 25/2-3. segédlet: MIBÉTS – Útmutató a Fejlesztők számára 1.0 verzió
 - A KIB 25. számú ajánlása: 25/2-4. segédlet: MIBÉTS – Útmutató Értékelőknek 1.0 verzió
 - A KIB 25. számú ajánlása: 25/2-5. segédlet: MIBÉTS – Értékelési módszertan 1.0 verzió
- **A Közigazgatási Informatikai Bizottság 26. számú ajánlása:** A Magyarországon elektronikus azonosításra, hitelesítésre, aláírásra és elektronikus azonosítók hordozására alkalmas eszközök követelményei (HUNeID) 1.0 verzió
- **A Közigazgatási Informatikai Bizottság 28. számú ajánlása:** Az E-Közigazgatási Keretrendszer projekt eredményeként létrehozott Követelménytár alábbi részhalmaza /mely alapvetően a KIB 25-ös – MIBÉTS -ajánlás továbbfejlesztése:
 - IT biztonsági követelmények

- Biztonsági tervezési útmutató
- IT biztonsági követelményrendszer - biztonsági szintek követelményei
- IT biztonsági Követelményrendszer érvényesítésének módja
- IT biztonsági szintek és biztonsági kategorizálási minta
- Útmutató az IT biztonsági szintek meghatározásához
- Termékek, szolgáltatások értékelésének, auditjának előkészítése
 - Termékekre vonatkozó értékelési módszertan
 - Összetett termékekre vonatkozó értékelési módszertan
 - Rendszerekre vonatkozó értékelési módszertan
 - Létező tanúsítások megfeleltetése - Technikai leírás
 - Útmutató rendszer-integrátorok számára
 - Útmutató rendszer-értékelők számára
 - Útmutató tanúsítók számára
 - Útmutató akkreditorok számára

A tanúsítást támogató egyéb dokumentumok:

MSZ ISO/IEC 15408-1:2002 (=Common Criteria)

Informatika. Biztonságtechnika. Az informatikai biztonságértékelés közös szempontjai. 1. rész: Bevezetés és általános modell (idt ISO/IEC 15408-1:1999)

MSZ ISO/IEC 15408-2:2003

Informatika. Biztonságtechnika. Az informatikai biztonságértékelés közös szempontjai. 2. rész: A biztonság funkcionális követelményei (idt ISO/IEC 15408-2:1999)

MSZ ISO/IEC 15408-3:2003

Informatika. Biztonságtechnika. Az informatikai biztonságértékelés közös szempontjai. 3. rész: A biztonság garanciális követelményei (idt ISO/IEC 15408-3:1999)

ISO/IEC 18045:2005:

Information technology -- Security techniques -- Methodology for IT security evaluation

A Közös értékelési módszertan (CEM) a Közös szempontok (CC) társdokumentuma. Célja, hogy leírja azokat a tevékenységeket, melyeket egy értékelő elvégez egy CC szerinti értékelés folyamán.

MSZ ISO/IEC 17799, továbbá az ennek megfelelő MSZ ISO/IEC 27001:2006

Ez a szabvány, amely „Az informatikai biztonság menedzselésének eljárásrendje”, azoknak ad ajánlásokat, akik a saját szervezetük körében a biztonság kezdeményezéséért, megvalósításáért és megtartásáért felelnek. Arra tervezték, hogy közös alapot szolgáltatson a szervezetek hatékony biztonságmenedzselési gyakorlatához és átfogja az informatikai biztonság minden területét.

A fenti lista nem teljes, folyamatos aktualizálása szükséges, amit a Tanúsítónak kell elvégezni.