MAGYAR KÖZTÁRSASÁG
GAZDASÁGI ÉS KÖZLEKEDÉSI
MINISZTÉRIUM
MINISZTER

Szám: 113/2007

KIJELÖLÉSI OKIRAT

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

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

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

2009. december 31. napjáig

k i j e l ö l ö m

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, 2007. április 27.

GAZDASÁGI ÉS KÖZLEKEDÉSI MINISZTÉRIUM * KÖZLEKEDÉSI MINISZTER

Dr. Kóka János

Melléklet

Melléklet a 113/2007. 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

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
194/2005. (IX. 22.) Korm. rendelet a közigazgatási hatósági eljárásokban felhasznált elektronikus aláírásokra és az azokhoz tartozó tanúsítványokra, valamint a tanúsítványokat kibocsátó hitelesítésszolgáltatókra vonatkozó követelményekről
195/2005. (IX. 22.) Korm. rendelet az elektronikus ügyintézést lehetővé tevő informatikai rendszerek biztonságáról, együttműködési képességéről és egységes használatáról
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
12/2005. (X. 27.) IHM rendelet az elektronikus ügyintézési eljárásban alkalmazható dokumentumok részletes technikai szabályairól
13/2005. (X. 27.) IHM rendelet a papíralapú dokumentumokról elektronikus úton történő másolat készítésének szabályairól
7/2002. (IV. 26.) MeHVM rendelet az elektronikus aláírással kapcsolatos szolgáltatási szakértő nyilvántartásba vételéről
2/2002 (IV. 26.) MeHVM irányelv a minősített elektronikus aláírással kapcsolatos szolgáltatásokra és ezek szolgáltatóira vonatkozó biztonsági követelményekről
4/2006. (IV. 19.) IHM rendelet a Nemzeti Hírközlési Hatóságnak az elektronikus aláírással összefüggő nyilvántartással kapcsolatos tevékenységéért fizetendő díjakról

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 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

Tanúsítványt aláíró kriptográfiai modul

FIPS PUB 140-2 3. level egy részhalmaza

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

A szoftver elektronikus aláírási termékek tanúsításához – az értékelési folyamat nyomonkövetéséhez, értékelés eredményeinek felhasználásához – a MIBÉTS módszertan kiadott alapdokumentumai is szükségesek:

1. számú MIBÉTS kiadvány:	A MIBÉTS általános modellje (v. 0.96, 2004 február)
2. számú MIBÉTS kiadvány:	Az értékelés és tanúsítás folyamatainak szabályozása (v. 0.9, 2003 szeptember)
3. számú MIBÉTS kiadvány:	Az értékelés módszertana (5 kötet) (v. 0.9, 2003 október és november szeptember)
5. számú MIBÉTS kiadvány:	Módszertani útmutató az értékelés megbízói számára (v. 0.9, 2004 február)
6. számú MIBÉTS kiadvány:	Módszertani útmutató az értékelés fejlesztői számára (v. 0.9, 2004 április)
7. számú MIBÉTS kiadvány:	Módszertani útmutató az értékelők számára (v. 0.9, 2004 április)
8. számú MIBÉTS kiadvány:	Módszertani útmutató a tanúsítók számára (v. 0.9, 2004 május)

Nem tartoznak közvetlenül az elektronikus aláírási termékek tanúsításának normatív dokumentumai közé az általános informatikai biztonsággal kapcsolatos követelmények, de az aláírásra kerülő dokumentumok adott informatikai környezetben keletkeznek, az aláírások aktivizálása, ellenőrzése folyamatában - az aláírás-létrehozó eszközön kívül - közreműködik az általános informatikai környezet, ezért annak biztonságát meghatározó dokumentumok az aláírás területén is meghatároznak szempontokat. Különösen fontossá teszi ezt a tényt, hogy egyrészt ezen a területen is kiadásra kerültek magyar szabványok, másrészt Magyarország 2003.09.19.-én csatlakozott a CCRA megállapodáshoz (Common Criteria Recognition Arrangement, Arrangement on the Recognition of Common Criteria Certificates in the field of Information Technology Security - Megállapodás a Közös szempontok szerinti tanúsítványok elfogadásáról az informatikai biztonság területén), melyből az informatikai biztonság területén feladatok és előírások vonatkoznak ránk, többek között az, hogy kötelező érvénnyel el kell fogadni a CC tanúsítványokat, illetve a CCRA egyezményt aláíró tagállamoknak, bár nem tartanak fenn CC informatikai biztonsági értékelési kapacitást, mégis kifejezetten elő kell segíteniük (érdekelteknek kell lenniük) a tanúsított termékek és védelmi profilok használatában.

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)

CEM

A Közös értékelési módszertan (CEM) a Közös követelményrendszer (CC) társdokumentuma. Célja, hogy leírja azokat a tevékenységeket, melyeket egy értékelő elvégez egy CC szerinti értékelés folyamán (Common Methodology for Information Technology Security Evaluation, CEM-97 Part 1: Introduction and general model, CEM-97 Part 2: Evaluation Methodology).

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 szolgáltasson 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.