TANÚSÍTVÁNY

A **HUNGUARD** Számítástechnikai-, informatikai kutató-fejlesztő és általános szolgáltató Kft. a 9/2005. (VII.21.) IHM rendelet alapján, mint a Magyar Köztársaság Gazdasági és Közlekedési Miniszterének 113/2007 számú kijelölési okiratával kijelölt tanúsító szervezet

tanúsítja,

hogy az

Eracom Technologies Group, Eracom Technologies Australia, Pty. Ltd.

által előállított és forgalmazott

ProtectServer Orange (korábbi nevén CSA8000 Adapter)

hardver verzió: G revizió, Cprov förmver verzió:1.10

elektronikus aláírási termék

az 1. számú mellékletben részletezett feltételrendszer teljesülése esetén

megfelel*

minősített hitelesítés-szolgáltató által végzett alábbi tevékenységek biztonságos elvégzéséhez:

Elektronikus aláírás hitelesítés szolgáltatás keretén belül:
(Minősített) tanúsítvány aláíró kulcsok generálására, tárolására, (minősített) tanúsítványok aláírására, mentésére és helyreállítására;

Időbélyegzés szolgáltatás keretén belül:
Időbélyegző aláíró kulcsok generálására, tárolására, időbélyegző aláírására;

Aláírás-létrehozó eszközön az aláírás-létrehozó adat elhelyezése szolgáltatás keretén belül:
Az előfizetői (aláírói) kulcspár generálására;

A minősített hitelesítés-szolgáltató saját informatikai rendszerének biztonságos működtetésén belül:
Infrastrukturális és megbízható rendszervezérlési kulcsok generálására, tárolására és felhasználására.

Jelen tanúsítvány a HUNG-TJ-047-2009. számú értékelési jelentés alapján került kiadásra.
A tanúsítványt a Netlock Hálózatbiztonsági és Informatikai Szolgáltató Kft. kérésére állítottuk ki.
A tanúsítvány regisztrációs száma: **HUNG-T-047-2009.**
A tanúsítás kelte: 2009. június 26.
A tanúsítvány érvényességi ideje évenkénti felülvizsgálati eljárás mellett: 2012. június 26.
Mellékletek: feltételrendszer, követelmények, dokumentumok, összesen: 7 oldalon.

PH.

Endrődi Zsolt
Tanúsítási igazgató

dr. Szabó István
Ügyvezető igazgató

* Figyelembe véve azonban, hogy mind az ETSI TS 102 176-1 V2.0.0 és az azon alapuló HL-21917-9,10,11,12,13,14/2008 NHH határozatok a termék által használt SHA-1 algoritmust 2009-től nem ajánlják elektronikus aláírás felhasználására, amennyiben a Hatóság megtiltja ezen algoritmus használatát, vagy a szakirodalomban megjelennek gyengeségére vonatkozó konkrét adatok, akkor jelen tanúsítvány érvényességét a tanúsító szervezet visszavonja.

1. számú melléklet

A tanúsítvány érvényességi feltételei

A CSA8000 adapter egy bonyolult kriptográfiai eszköz, melyet fejlesztői úgy terveztek, hogy minél általánosabb feltételek között legyen használható, s a felhasználói igények minél szélesebb körét legyen képes kielégíteni. Ennek megfelelően számos biztonsági tulajdonság konfigurálható be, illetve ki rajta.

A FIPS 140-1-nek megfelelő módú működtetés (mely a biztonságra helyezi a hangsúlyt, sokszor a hatékonyság és a felhasználói kényelem rovására) számos konfigurációs beállítást megkövetel, s ezek betartása feltétele a tanúsítás érvényességének.

Amennyiben a CSA8000 adaptert egy minősített hitelesítés-szolgáltató kívánja felhasználni biztonságkritikus tevékenységeihez (az általa kibocsátott tanúsítványok aláírására, időbélyeg válaszai aláírására), további követelményeknek kell megfelelni, melyek a felhasználhatóságot tovább korlátozzák, kiegészítő feltételek betartását követelve meg.

Az alábbiakban összefoglaljuk azokat a feltételeket, melyek **együttes** betartása feltétele a Tanúsítvány érvényességének.

I. Általános érvényességi feltételek

Az alábbi feltételek minden felhasználási mód esetén (tehát a fejlesztő-gyártó cég által igen általánosra tervezett felhasználási kör egészében) szükségesek a megbízható és biztonságos működéshez.

1. A CSA8000 kriptográfiai modul szolgáltatásait igénybe vevő különböző munkaköröket (Admin, Admin Security Officer, Token Security Officer, Token User) betöltő személyek:
   - kompetensek, jól képzettek és megbízhatóak, valamint
   - betartják a különböző útmutatók (CSA8000 Adapter Installation Guide, Cprov Installation Guide, Cprov Administration Manual, Cprov Key Management Utility User Manual) által leírt, kötelező tevékenységeket.

II. A FIPS 140-1 megfelelőségből fakadó érvényességi feltételek

Az alábbi feltételek ahhoz elengedhetetlenek, hogy a CSA8000 adaptert megfeleljen a FIPS 140-1 3-as biztonsági szintjének.

2. A digitális aláírással kapcsolatos kriptográfiai funkcionalitást az alábbi algoritmusokra kell korlátozni: **DSA, RSA (PKCS #1), SHA-1**.

3. A következő biztonsági beállításokat kell alkalmazni (konfigurálni):
   - CKF_ENTRUST_READY ("Entrust Compliant" flag) kötelező értéke: **FALSE**
   - CKF_ALWAYS_SENSITIVE ("No Clear PINs" flag) kötelező értéke: **TRUE** (SET)
   - CKF_AUTH_PROTECTION ("Session Protection" flag) kötelező értéke: **TRUE** (SET)
   - CKF_MODE_LOCKED ("Lock Security Mode" flag) kötelező értéke: **TRUE** (SET)
   - CKF_NO_PUBLIC_CRYPTO ("No Public Cryptography" flag) kötelező értéke: **TRUE** (SET)

4. Az üzembe helyezés során a HIMK-ek számára új értékeket kell beállítani, a gyári beállítású alap (default) HIMK értéket törölni kell.

5. Az üzembe helyezés során az Adminisztrátori kriptográfiai tisztviselő gyári beállítású alap (default) azonosítóját és jelszavát le kell cserélni.

6. Az operátoroknak titokban kell tartaniuk saját PIN kódjukat.

7. Minden új slot konfigurálásánál a PIN kód hossza legalább 4 legyen.

III. A minősített hitelesítés- szolgáltatáshoz történő használhatóság kiegészítő feltételei

Egy minősített hitelesítés-szolgáltatónak a CSA8000 felhasználása során az alábbi kiegészítő feltételeket is be kell tartania:

8. RSA aláírási algoritmus használata esetén a minimális modulus hosszúság (MinModLen): 1020 bit legyen.

9. DSA aláírási algoritmus használata esetén a minimális p prímhosszúság (pMinLen) 1024 bit, a minimális q prímhosszúság (qMinLen) 160 bit legyen.

10. Digitálisan aláírni csak 8-cal osztható bithosszúságú blokkot lehet

11. A minősített tanúsítvány aláírására használt kulcsot csak a minősített tanúsítványok, illetve esetlegesen a rájuk vonatkozó visszavonási listák aláírására szabad felhasználni.

12. Bármilyen, biztonságos kriptográfiai modulban tárolt kulcs modulból történő exportálásakor a modulnak gondoskodnia kell a kulcs védelméről. Érzékeny kulcsadatok nem védett módon történő tárolása tilos. Minősített tanúsítvány aláíró kulcs csak további biztonsági mechanizmusok alkalmazása esetén tárolható és menthető. Ez megtehető például az alábbiak valamelyikével is:

- az "m az n-ből" technika alkalmazásával (melyet jelenleg a CSA8000 nem támogat, de szabványos felületén keresztül később megvalósítható), ahol m azon komponensek darabszáma a teljes n komponensből, amelynek ismeretében a kulcs inicializálása sikeresen elvégezhető. A hiba esetén alkalmazandó helyreállításra az m = 60% * n érték javasolt (azaz ha n=3, akkor m=2, ha n=4 akkor m=3, ha n=5 akkor m=3,…).
- az alábbi (CSA8000 által támogatott) módszerrel:
  - a mentés intelligens kártyákra (tokenekre) történnek,
  - a mentés kódolva van a triple-DES titkosító algoritmus alkalmazásával,
  - a mentés kódolására alkalmazott titkosító kulcs (Key Encryption Key) legalább két véletlen komponensből van előállítva, s ennek megfelelően legalább két erre felhatalmazott személy együttes jelenléte szükséges a magánkulcs helyreállításához.

13. Az időbélyegzéshez használt aláíró kulcsokat csak időbélyegek aláírására szabad használni.

14. Amennyiben az aláírás-létrehozó eszközön az aláírás-létrehozó adat elhelyezése szolgáltatás keretén belül az előfizetői (aláírói) kulcspár generálása az aláírás-létrehozó eszközön kívül (a CSA8000 kriptográfiai hardverben) történik, biztosítani kell, hogy az elektronikus aláírásra szolgáló aláírói kulcsok különbözzenek minden más funkcióra szolgáló kulcstól, mint például a titkosításra szolgálóktól.

15. Amennyiben az aláírás-létrehozó eszközön az aláírás-létrehozó adat elhelyezése szolgáltatás keretén belül az előfizetői (aláírói) kulcspár generálása az aláírás-létrehozó eszközön kívül (a CSA8000 kriptográfiai modulban) történik, biztosítani kell, hogy a CSA8000 kriptográfiai modul és az aláírás létrehozó eszköz között biztonságos útvonal legyen. Ennek az útvonalnak forráshitelesítést, sérthetetlenséget és bizalmasságot kell biztosítania megfelelő kriptográfiai mechanizmusok használatával.

16. A Tanúsítvány csak a jelenlegi hardver és förmver verzióra érvényes /hardver verzió: G revizió, Cprov förmver verzió:1.10/. Új förmver verzió upgradje csak az alábbi követelmények együttes teljesülése esetén lehetséges:
  - az új förmver verziót a fejlesztő-gyártó cég digitális aláírása hitelesíti,
  - az új förmver verziót értékelte egy FIPS 140 értékeléssel meghatalmazott (akkreditált) laboratórium, s erről egy új FIPS tanúsítvány is készül,
  - az új förmver verzió minősített hitelesítés-szolgáltatáshoz történő felhasználhatóságát egy erre kijelölt hazai tanúsító szervezet megfelelőségi tanúsítványba foglalja, s mint ilyen, az új verzió is bekerül a NHH biztonságos elektronikus aláírási termék nyilvántartásába.

IV. Egyéb, az érvényességet befolyásoló megjegyzések

17. A National Institute of Standards and Technology (NIST) által kibocsátott tanúsítványok visszavonásig érvényesek. Így a tanúsítványokban szereplő hardver, förmver és szoftver konfigurációk változatlan formában használhatók.

18. A FIPS 140-1 szerint tanúsított modulok továbbra is biztonságosnak tekinthetők. A FIPS 140-1 szerinti tanúsítványok azonban 2002. május 26. után nem adhatók ki.

19. Nyilvános források között jelenleg nem található olyan információ, mely befolyásolná a modul biztonságos működését. Ezt a vizsgálatot legalább 3 évente szükséges elvégezni.

2. számú melléklet
TERMÉKMEGFELELŐSÉGI KÖVETELMÉNYEK
A követelményeket tartalmazó dokumentumok

Az elektronikus aláírásról szóló 2001. évi XXXV. törvény

3/2005. (III.18.) IHM rendelet az elektronikus aláírással kapcsolatos szolgáltatásokra és ezek szolgáltatóira vonatkozó részletes követelményekről

FIPS 140-1: Security Requirements for Cryptographic Modules

Derived Test Requirements for FIPS 140-1

ETSI TS 101 456 v1.4.3 Policy Requirements for Certification Authorities Issuing Qualified Certificates

ETSI TS 102 176-1 V2.0.0 Algorithms and Parameters for Secure Electronic Signatures; Part 1: Hash functions and asymmetric algorithms

CEN 14167-1:2003 munkacsoport egyezmény: Security Requirements for Trustworthy Systems Managing Certificates for Electronic Signatures

3. számú melléklet
A tanúsításhoz figyelembe vett egyéb dokumentumok

Kérelem /a tanúsítás elvégzésére/

CEN 14167-2:2002 munkacsoport egyezmény: Cryptographic Module for CSP Signing Operation – Protection Profile (CMCSO-PP, HSM-PP)

CEN 14167-3:2003 munkacsoport egyezmény: : Cryptographic Module for CSP Key Genaration Services – Protection Profile (CMCKG-PP, HSM-PP)

FIPS 140-1 Validation Certificate No. 160 /CSA8000 Cryptographic Adapter/

ERACOM: CSA8000 Cryptographic Adapter, Hardware Revision: G, Firmware Version: 1.1, FIPS 140-1 Non-Proprietary Cryptographic Module Security Policy

CSA8000 Adapter Installation Guide /Version: A4, Date: 7 May 2001/

Cprov Installation Guide /Version: 3.0, Revision A6, Last Modified: 7 May 2001/

Cprov Administration Manual /Version: 3.0, Revision A7/ May 2001/

Cprov Key Management Utility User Manual /KMU Version: 3.0 Beta, Revision A1/ May 2001/

Eracom Technologies official notification about name change of CSA 8000 Adapter

Frequently Asked Questions for the Cryptographic Module Validation Program