



TANÚSÍTVÁNY

A **HUNGUARD** Számítástechnikai-, informatikai kutató-fejlesztő és általános szolgáltató Kft. a 15/2001.(VIII. 27.) MeHVM rendelet alapján, mint a Magyar Köztársaság Informatikai és Hírközlési Miniszter 006/2002 számú kijelölési okirátával kijelölt terméktanúsító szervezet

tanúsítja,

hogy az

Eracom Technologies Group, Eracom Technologies Australia, Pty. Ltd
által előállított és forgalmazott

CSA8000 Adapter

hardver verzió: G revízió, Cprov förmver verzió: 1.10

elektronikus aláírási termék

az 1. számú mellékletben részletezett feltételrendszer teljesülése esetén

megfelel

a 2001. évi XXXV. törvényben szereplő
minősített elektronikus aláírások létrehozására alkalmazható
„3-as típusú biztonságos aláírási-létrehozó eszköz”-nek

mint

az adapterhez közvetlenül hozzáférő több felhasználó (aláíró)
közös biztonságos aláírási-létrehozó eszköze.

Jelen tanúsítvány a HUNG-TJ-007-2003. számú értékelési jelentés alapján került kiadásra.
Készült a Netlock Kft. megbízásából.

A tanúsítvány regisztrációs száma: **HUNG-T-007/2003.**

A tanúsítás kelte: 2003. május 16.

A tanúsítvány érvényességi ideje évenkénti felülvizsgálati eljárás mellett: 2006. május 16.

Mellékletek: feltételrendszer, követelmények, dokumentumok, összesen: 9 oldalon.

PH.

Tanúsítási igazgató:

Ügyvezető igazgató



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.

Tovább bonyolítja a helyzetet, hogy a CSA8000 adapter tervezett felhasználási módja **(több felhasználó közös aláíró eszköze)** igen szokatlan. Ennek engedélyezése további szigorításokat, extra feltételeket kíván 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 megfelelésből 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_CRYPT (“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. Valamennyi operátornak (Adminisztrátori kriptográfiai tisztviselő, Adminisztrátor, Token kriptográfiai tisztviselő, Token felhasználó) titokban kell tartaniuk saját PIN kódjukat.
7. Minden új slot konfigurálásánál biztosítani kell, hogy valamennyi operátor PIN kód hossza legalább 6 legyen. A hitelesítő adatokat bekérő alkalmazásnak ellenőriznie kell ezt, s csak a megfelelő hosszúságú PIN kód értékeket szabad továbbküldenie a CSA8000 felé.

III. A biztonságos aláírás-létrehozó eszközként történő használhatóság kiegészítő feltételei

Egy minősített aláírásokat létrehozó aláírónak 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 aláírások létrehozására használt magánkulcsot csak minősített aláírások létrehozására szabad felhasználni. (Nem szabad titkosításra, hitelesítésre és fokozott biztonságú aláírások létrehozására felhasználni.)



12. A minősített aláírások létrehozására használt magánkulcsot tilos menteni.
13. A minősített aláírások létrehozására használt magánkulcsot érvényességének lejártá után haladéktalanul törölni kell. /Ez az aláíró felelőssége, de az aláíró alkalmazásnak támogatást kell ehhez biztosítania./
14. Egy BALE-ként használt CSA8000 szerepkör kiosztásánál és felhasználói token inicializálásánál be kell tartani a következőket:

Minősített aláírásokat csak olyan helyi felhasználó hozhat létre, aki a Token felhasználó szerepkört tölti be. (csak helyi Token felhasználó lehet az „aláíró”).
/A CSA8000 az alábbi szerepköröket támogatja (a hagyományos adminisztrátori szerepkör háromfelé osztásával):

- Adminisztrátori kriptográfiai tisztviselő,
- Adminisztrátor,
- Token kriptográfiai tisztviselő,
- Token felhasználó./

Feltételezve, hogy az alábbi két lépésre már előzetesen sor került:

- az Adminisztrátori kriptográfiai tisztviselő inicializálta az Adminisztrátort, aki képes feladata ellátására,
- az Adminisztrátor inicializálja a felhasználói token Token kriptográfiai tisztviselőjének a PIN kódját,

egy minősített aláírások létrehozására alkalmas felhasználói token létrehozásánál az alábbi lépéseket kell egymást követően, legalább kettős személyi ellenőrzés alatt betartani, illetve végrehajtani:

1. A Token kriptográfiai tisztviselő inicializálja az aláíró felhasználói tokenét:
 - inicializálva a Token felhasználó kezdeti PIN kódját,
 - (a PIN kód átadásával) engedélyezve az aláírói kulcspár generálását.
2. A Token felhasználó azonnal lecseréli saját PIN kódját.
3. A Token felhasználó haladéktalanul legenerálja saját (aláírói) kulcspárját.
4. A Token kriptográfiai tisztviselő (vagy az érintett Token felhasználó) exportálja a legenerált nyilvános kulcsot.
5. A Token kriptográfiai tisztviselő (vagy az érintett Token felhasználó) a felhasználói tokenre tölti a nyilvános kulcsra (a hitelesítés-szolgáltatótól kapott) tanúsítványt.

A fenti folyamat után minősített aláírások létrehozására csak a helyi Token felhasználó (illetve a nevében eljáró program) képes, ha sikeresen hitelesítette magát PIN kódja megadásával.

Távoli felhasználók hálózatról való bejelentkezéssel és távoli hitelesítéssel nem aktivizálhatják a CSA8000 adapteren lévő magánkulcsukat.

A CSA8000 párhuzamosan több tokent támogat, mindegyiken egy-egy Token felhasználónak biztosítva hozzáférést, összességében tehát több különböző Token felhasználónak nyújtva (aláírói) szolgáltatást.

A fenti 5 lépéses eljárás minden Token felhasználóval külön-külön elvégzendő.



15. Egy BALE-ként használt CSA8000 kriptográfia modulra biztosítani kell az alábbiakat:
1. Azt követően, hogy egy Token felhasználó minősített aláírások létrehozására használható kulcspárt generált rajta, **a token nem vehető ki slot-jából** (az erre speciális jogosultsággal felhatalmazott Adminisztrátor kivételével). /A CSA8000 adaptert úgy kell beállítani, hogy nullázza védett memória tartalmát, ha jogosulatlanul kiemelik a gazdagép PCI slot-jából, akár annak kikapcsolt állapotában is./
 2. A CSA8000 bekapcsolt, működő gazdagépének **közvetlen környezete** olyan **fizikai védelem alatt álljon**, mely megakadályozza a PCI slot-jában elhelyezett CSA8000 speciális eszközökkel való manipulálását, fizikai támadását.
16. Az aláíró csak megbízható aláírás-létrehozó alkalmazást használhat.
17. A megbízható csatornák kialakításában közreműködő kulcsokat (HIMK) a host oldalon is védeni kell. A CSA8000 adapter és az alkalmazások közötti megbízható csatorna egy közös titok ismeretén alapul. Ezt a titkot (HIMK) a gazdagép oldalán is kellő biztonsággal meg kell védeni az illetéktelen felfedés ellen.
18. a) A CSA8000 adaptert felhívó aláíró alkalmazásoknak meg kell teremteni az aláírók számára annak lehetőségét, hogy egy sikeres hitelesítést követő aláírás(ok) után deaktivizálhassa az eszközt, azaz saját tokenén a magánkulcsát újra hitelesítés nélkül aktivizálhatatlan állapotba hozhassa.
- b) Az aláíró (Token felhasználó) kötelessége deaktivizálni a CSA8000 által védett saját magánkulcsát, amikor aláírási szándéka megszűnik, illetve amikor az eszköz feletti személyes kontroll felvállalását szünetelni kívánja.
19. Egy 3-as típusú BALE-ként használt CSA8000 adapter eszköz nem használható hitelesítés-szolgáltató hardver kriptográfiai moduljaként.
20. A Tanúsítvány csak a jelenlegi hardver és firmware verzióra érvényes /hardver verzió: G revízió, Cprov firmware verzió:1.10/. Új firmware verzió upgradje csak az alábbi követelmények együttes teljesülése esetén lehetséges:
- az új firmware verziót a fejlesztő-gyártó cég digitális aláírása hitelesíti,
 - az új firmware verziót értékelte egy FIPS 140 értékeléssel meghatalmazott (akkreditált) laboratórium, s erről egy új FIPS tanúsítvány is készül,
 - az új firmware verzió BALE-ként való felhasználhatóságát egy erre kijelölt hazai tanúsító szervezet megfelelőségi tanúsítványba foglalja, s mint ilyen, az új verzió is bekerül a HIF biztonságos elektronikus aláírási termék nyilvántartásába.



2. számú melléklet

TERMÉKMEGFELELŐSÉGI KÖVETELMÉNYEK

A követelményeket tartalmazó dokumentumok

Az elektronikus aláírásról szóló 2001. évi XXXV. törvény

2/2002. (IV. 26.) MeHVM irányelv a minősített elektronikus aláírással kapcsolatos szolgáltatásokra és ezek szolgáltatóira vonatkozó biztonsági követelményekről

CEN/ISSS ESign Workshop – Expert Group F: Protection Profile – Secure Signature-Creation Device Type 3, version: 1.05, EAL4+

FIPS 140-1: Security Requirements for Cryptographic Modules

Derived Test Requirements for FIPS 140-1



3. számú melléklet

A tanúsításhoz figyelembe vett egyéb dokumentumok

Kérelem /a tanúsítás elvégzésére/

Kérdőív a tanúsítás kérelmezéséhez

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/