TANÚSÍTVÁNY

A **HUNGUARD** Számítástechnikai-, informatikai kutató-fejlesztő és általános szolgáltató Kft. a 9/2005. (VII. 21.) IHM rendelet alapján, mint a Magyar Köztársaság Informatikai és Hírközlési Miniszter 002/2006 számú kijelölési okiratával kijelölt tanúsító szervezet

tanúsítja,

hogy a

Utimaco Safeware AG

által előállított és forgalmazott

CryptoServer 2000

hardver verzió: 1.0.2.0, förmver verzió:1.0.0.2

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-035-2006. számú értékelési jelentés alapján került kiadásra.
A tanúsítványt a Safesoft Kft. kérésére állítottuk ki.

A tanúsítvány regisztrációs száma: **HUNG-T-035-2006.**
A tanúsítás kelte: 2006. december 7.
A tanúsítvány érvényességi ideje évenkénti felülvizsgálati eljárás mellett: 2009. december 7.
Mellékletek: feltételrendszer, követelmények, dokumentumok, összesen: 7 oldalon.

PH.

Endrődi Zsolt
Tanúsítási igazgató

dr. Szabó István
Ügyvezető igazgató

1. számú melléklet

A tanúsítvány érvényességi feltételei

A Utimaco CryptoServer 2000 modul 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 140-2-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 Utimaco CryptoServer 2000 modult 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 Utimaco CryptoServer 2000 kriptográfiai modul szolgáltatásait igénybe vevő különböző munkaköröket (Kriptográfiai felhasználó, Adminisztrátor) betöltő személyek:
   - kompetensek, jól képzettek és megbízhatóak, valamint
   - betartják a különböző útmutatók (CryptoServer 2000 - Administrator's Guide for CryptoServer in FIPS-Mode) által leírt, kötelező tevékenységeket.

II. A FIPS 140-2 megfelelőségből fakadó érvényességi feltételek

Az alábbi feltételek ahhoz elengedhetetlenek, hogy a Utimaco CryptoServer 2000 modul megfeleljen a FIPS 140-2 3-as biztonsági szintjének.

A CryptoServer 2000 beállításánál és első perszonalizációjánál el kell végezni a következő szolgáltatásokat, melyekről részletesen a CryptoServer 2000 Administrator's Guide for CryptoServer in FIPS-Mode című dokumentumban lehet olvasni.

2. Teljesülnie kell az előfeltételeknek.

A CryptoServernek perszonalizációs módban és inicializált állapotban kell lennie.

Minden FIPS módhoz kötelező förmver modulnak rendelkezésre kell állnia és megfelelően aláírással kell rendelkeznie, melyet az inicializációs kulccsal készítettek. A kötelező förmver modulok a következők:

- SMOS: fájl 'smos.mtc', 1.0.3.7-es verzió
- CMDS: fájl 'cmds.mtc', 1.0.5.0-ás verzió
- UTIL: fájl 'util.mtc', 1.0.6.0-ás verzió
- ADM: fájl 'adm.mtc', 1.0.2.0-ás verzió
- DB: fájl 'db.mtc', 1.0.1.1-es verzió
- VDES: fájl 'vdes.mtc', 1.0.0.3-as verzió
- VRSA: fájl 'vrsa.mtc', 1.0.3.3-as verzió
- AES: fájl 'aes.mtc', 1.0.0.0-ás verzió
- HASH: fájl 'hash.mtc', 1.0.1.0-ás verzió
- LNA: fájl 'lna.mtc', 1.0.3.0-ás verzió
- ASN1: fájl 'asn1.mtc', 1.0.1.1-es verzió
- CSI: fájl 'csi.mtc', 1.0.0.3-as verzió
- FIPS140: fájl 'fips140.mtc' 1.0.0.2-es verzió

A inicializációs kulcsot tartalmazó intelligens kártyának rendelkezésre kell állnia.

3. A CryptoServer adminisztrációjának alapvető feltétele az, hogy a vásárló specifikus inicializációs kulcs be legyen töltve a modulba.

4. Végre kell hajtani a GetState parancsot a mellékelt menedzsmentszoftverben. Ennek az *inicializált* állapotot kell mutatnia, a riasztási állapotot pedig nem jelezhet.

5. További perszonalizációs lépésekhez szükség van az inicializációs kulcs magánkulcsára, ami tipikusan egy intelligens kártyán van.

6. A BLSetRTC paranccsal be kell állítani a modul belső óráját.

7. Az alapvető FIPS módhoz szükséges förmver modulokat (SMOS, CMDS, ADM, UTIL) be kell tölteni a BLLoadFile paranccsal.

8. El kell indítani a modulokat a StartOS paranccsal.

9. A GetState paranccsal meg kell győződni, hogy a modul működési állapotban van-e.

10. A LoadFile paranccsal be kell tölteni a többi, FIPS módhoz szükséges modult is.

11. A GetState parancs kiadásával meg kell győződni arról, hogy a modul FIPS módban van (FIPS mode = ON).

III. A minősített hitelesítés-szolgáltatáshoz történő használhatóság kiegészítő feltételei

Egy minősített hitelesítés-szolgáltatónak a Utimaco CryptoServer 2000 felhasználása során az alábbi kiegészítő feltételeket is be kell tartania:

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

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

14. Digitálisan aláírni csak 8-cal osztható bithoszzúságú blokkot lehet

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

16. 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 a Utimaco CryptoServer 2000 nem támogat), 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 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.

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

18. Amennyiben az aláírás-létrehozó eszközön az aláírás-létrehozó adat elhelyezése szolgáltatás keretén belül az előfizetői (aláírói) kulcspár generálása az aláírás-létrehozó eszközön kívül (a Utimaco CryptoServer 2000 kriptográfiai modulban) történik, biztosítani kell, hogy az elektronikus aláírásra szolgáló aláírói kulcsok különbözzenek minden más funkcióra szolgáló kulcstól, mint például a titkosításra szolgálóktól.

19. Amennyiben az aláírás-létrehozó eszközön az aláírás-létrehozó adat elhelyezése szolgáltatás keretén belül az előfizetői (aláírói) kulcspár generálása az aláírás-létrehozó eszközön kívül (a Utimaco CryptoServer 2000 kriptográfiai modulban) történik, biztosítani kell, hogy a Utimaco CryptoServer 2000 kriptográfiai modulban és az aláírás létrehozó eszköz között biztonságos útvonal legyen. Ennek az útvonalnak forráshitelesítést, sérthetetlenséget és bizalmasságot kell biztosítania megfelelő kriptográfiai mechanizmusok használatával.

20. A Tanúsítvány csak a jelenlegi hardver és förmver verzióra érvényes /hardver verzió: 1.0.2.0, förmver verzió: 1.0.0.2/. 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 az NHH biztonságos elektronikus aláírási termék nyilvántartásába.

21. Az MD5 lenyomatképző algoritmus sérülékenysége miatt a hitelesítés-szolgáltatás során az algoritmus nem használható.

IV. Egyéb, az érvényességet befolyásoló megjegyzések

22. 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.

23. 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

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

FIPS 140-2: Security Requirements for Cryptographic Modules

Derived Test Requirements for FIPS 140-2

ETSI TS 101 456 v1.3.1 Policy Requirements for Certification Authorities Issuing Qualified Certificates

ETSI TS 102 176-1 V1.2.1 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/

Kérdőív a tanúsítás kérelmezéséhez

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 140-2 Validation Certificate No. 543 /Utimaco CryptoServer 2000/

CryptoServer Security Policy /Version 1.1.4, Doc. No.: 2004-0007, 9th May 2005/

CryptoServer 2000 Administrator's Guide for CryptoServer in FIPS-Mode /Version 1.0.2, Doc. No.: 2004-0002, 26th January 2005/