TANÚSÍTVÁNY

A **HUNGUARD** Számítástechnikai-, informatikai kutató-fejlesztő és általános szolgáltató Kft. a 9/2005. (VII.21.) IHM rendelet alapján, mint a Nemzeti Fejlesztési Minisztérium IKF/19519-2/2012-NFM számú Kijelölési okiratával kijelölt tanúsító szervezet és mint a NAT által NAT-6-0048/2011 számon akkreditált terméktanúsító szervezet

tanúsítja,

hogy a

SafeNet Inc.

által előállított és forgalmazott

ProtectServer Gold

Hardver verzió B4 Förmver verziók 2.07.00, 2,08.00 és 3.00.03

Hardver verziók B2 és B3 Förmver verzió 2.08.00 és

Hardver verzió C / PSG-01-0101 Förmver verzió 2.08.00

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-061-2013. számú tanúsítási jelentés alapján került kiadásra.
Készült a NetLock Informatikai és Hálózatbiztonsági Szolgáltató Kft. megbízásából.
A tanúsítvány regisztrációs száma: **HUNG-T-061-2013.**
A tanúsítás kelte: 2013. szeptember 2.
A tanúsítvány érvényességi ideje évenkénti felülvizsgálati eljárás mellett: 2016. szeptember 7.
Mellékletek: feltételrendszer, követelmények, dokumentumok, összesen: 6 oldalon.

PH.

Endrődi Zsolt
Tanúsítási igazgató:

Lengyel Csaba
Ügyvezető igazgató

1. számú melléklet

A tanúsítvány érvényességi feltételei

A ProtectServer Gold (PSG) 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 ProtectServer Gold 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 ProtectServer Gold kriptográfiai modul szolgáltatásait igénybe vevő különböző munkaköröket (Kriptográfiai felhasználó, Adminisztrátor) betöltő személyek:
   - kompetensek, jól képzettek és megbízhatóak, valamint
   - betartják a különböző útmutatók által leírt, kötelező tevékenységeket.

II. A FIPS 140-2 megfelelőségből fakadó érvényességi feltételek

2 A FIPS üzemmódnak való megfelelés érdekében a ProtectServer Gold-ot biztonságos módon kell konfigurálni. Ez magába foglalja a következőket:
   - Csak FIPS-jóváhagyott algoritmusokkal való működés;
   - Kulcsok nyílt formában történő exportálásának tiltása;
   - A biztonsági üzemmód blokkolása az üzemmód beállításba való beavatkozás megakadályozása érdekében;
   - PIN nyílt formában történő használatának megakadályozása;
   - Annak megakadályozása, hogy a PSG förmvert az összes védett kulcs és kritikus biztonsági paraméter előzetes törlése nélkül módosítani lehessen;
   - Hitelesítés és session kezelés biztonságának megvalósítása.

Egy operátor „FIPS-módba” állíthatja a ProtectServer Gold-ot azzal, hogy lefuttatja a `CTCONF -fF` parancsot távoli menedzsment segítségével. A parancs végrehajtás után a PSG visszautasít minden nem FIPS algoritmusra vagy konfigurációra vonatkozó kérést.

Egy operátor megnézheti az aktuális PSG üzemmódot a `CTCONF -v` parancs futtatásával. A parancs végrehajtásának eredményeként a PSG visszaadja a részletes adapter konfiguráció információkat. A konfigurációs részletek tartalmazzák a betöltött förmver információkat és az adapter biztonsági mód flagek listáját, melyek egyike azt mutatja, hogy a modul FIPS üzemmódban van.

III. A minősített hitelesítés-szolgáltatáshoz történő használhatóság kiegészítő feltételei

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

3. RSA aláírási algoritmus használata esetén a minimális modulus hosszúság (`MinModLen`): 2048 bit legyen.

4. DSA aláírási algoritmus használata esetén a minimális p prímhosszúság (`pMinLen`) 2048 bit, a minimális q prímhosszúság (`qMinLen`) 224 bit legyen.

5. Az ECDSA aláírási algoritmus használata esetén a következő paraméter feltételek teljesítése szükséges: `qMinLEN=256` SHA256 használata mellett, továbbá `r0Min` nagyobb mint 10^4 és `MinClass` legalább `200`, ahol a paraméterek jelölése megfelel az ETSI TS 102 176-1 v 2.1.1 –ben leírtaknak.

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

7. SHA-1 vagy annál gyengébb lenyomatoló algoritmus használata tilos.

8. A minősített tanúsítvány aláírására használt kulcsot csak a minősített tanúsítványok, illetve esetlegesen a rájuk vonatkozó visszavonási információk, illetve ezek kibocsátásához szükséges tanúsítványok aláírására szabad felhasználni.

9. 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, 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 vagy AES 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.

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

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

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

13. A Tanúsítvány csak a megadott hardver és förmver verzióra érvényes. 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 készült,
    - 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 NMHH biztonságos elektronikus aláírási termék nyilvántartásába.

IV. Egyéb, az érvényességet befolyásoló megjegyzések

14. 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.

15. 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 140-2: Security Requirements for Cryptographic Modules

Derived Test Requirements for FIPS 140-2

ETSI TS 102 176-1 v2.1.1 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/

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 Generation Services – Protection Profile (CMCKG-PP, HSM-PP)

FIPS 140-2 Validation Certificate No. 1137 /ProtectServer Gold/

Level3 Security Policy for ProtectServer Gold (PSG) /Revision: 31; Document Number: CR-2505/