Tanúsítási jelentés

Hung-TJ-062-2013

nShield F3 500 for netHSM
biztonságos aláírás-létrehozó eszköz

/Hardware Version: nC4033P-500N, Firmware Version: 2.33.60-3

/ nCipher Corporation Ltd. /

Verzió:	1.0
Fájl:	Hung-TJ-062-2013_v10.pdf
Minősítés:	Nyilvános
Oldalak:	22

Változáskezelés

Verzió	Dátum	A változás leírása
v0.1	2013.04.03.	A szerkezet felállítása
v0.81	2013.08.28.	Egyeztetésre kiadott változat
v0.9	2013.09.04.	Megrendelőnek egyeztetésre kiadott változat
v1.0	**2013.09.23**	**Végleges verzió**

A tanúsítási jelentést készítette:

Juhász Judit
HunGuard Kft
Tanúsítási divízió

Tartalom

1. Bevezetés

1.1. A tanúsítási jelentés tárgya

Jelen tanúsítási jelentés tárgya a nShield F3 500 for netHSM megnevezésű kriptográfiai hardver eszköz/Hardware Version: nC4033P-500N, Firmware Version: 2.33.60-3/, (a későbbiekben erre a termékre „nShield F3 500 for netHSM**”**-ként vagy „netHSM”-ként hivatkozunk), s melyet minősített aláírás létrehozásához kívánnak felhasználni, mint biztonságos aláírás-létrehozó eszköz (BALE).

A biztonságos aláírás-létrehozó eszközre vonatkozó követelményeket az elektronikus aláírásról szóló 2001. évi XXXV. törvény [1] igen általánosan az alábbi módon fogalmazza meg 1. sz. mellékletében:

1. *A biztonságos aláírás-létrehozó eszköznek megfelelő technikai és eljárási eszközökkel biztosítaniuk kell legalább a következőket:*
   a) *az aláírás készítéséhez használt aláírás-létrehozó adat aláírónként biztosan mindig különbözik, s titkossága kellően biztosított,*
   b) *az aktuálisan elérhető technológiával kellő bizonyossággal garantálható, hogy az aláírás készítéséhez használt aláírás-létrehozó adat nem rekonstruálható, megvalósítható annak a jogosulatlan felhasználókkal szembeni védelme, illetve az aláírás nem hamisítható.*
2. *A biztonságos aláírás-létrehozó eszköznek nem szabad az aláírandó elektronikus dokumentumot az aláírás elhelyezéséhez szükséges mértéken felül módosítaniuk, illetőleg nem akadályozhatják meg azt, hogy az aláíró a dokumentumot az aláírási eljárás előtt megjelenítse.*

A fenti követelmények lényegében (kisebb fordítási különbséggel) megegyeznek az Európai Parlament és Tanács elektronikus aláírásokra vonatkozó 1999/93/EK számú Irányelvének [2] III. mellékletében foglaltaknak:

1. *A biztonságos aláírás-létrehozó eszköznek megfelelő műszaki és eljárási módok segítségével garantálnia kell legalább azt, hogy:*
   a) *az aláírás létrehozásához használt aláírás-létrehozó adat gyakorlatilag csak egyszer jöhessen létre, és titkossága ésszerű mértékig biztosított legyen;*
   b) *az aláírás létrehozásához használt aláírás-létrehozó adat kikövetkeztethetősége, ésszerű mértékig kizárt legyen, az aláírás pedig a jelenleg rendelkezésre álló technológiát alkalmazó hamisítás ellen védett legyen;*
   c) *az aláírás létrehozásához használt aláírás-létrehozó adatot a jogszerűen aláíró személy megbízhatóan védeni tudja a mások általi felhasználással szemben.*
2. *A biztonságos aláírás-létrehozó eszköz nem módosíthatja az aláírással ellátandó adatokat, és nem akadályozhatja meg, hogy az adatokat az aláíró az aláírási eljárás előtt megtekintse.*

A [2] Irányelv fenti követelményeinek szakmai lebontásaként egy CEN Munkacsoport egyezmény [3] született, mely a Közös szempontok (CC, ISO/IEC 15408) által definiált védelmi profilok formájában határozta meg a biztonságos aláírás-létrehozó

eszközökre vonatkozó részletes funkcionális és garanciális biztonsági követelményeket.
[3] a funkcionalitás szempontjából három különböző BALE típust definiál:

- 1-es típus: csak az aláírás-létrehozó/aláírás-ellenőrző adatpárok generálását támogatja, de nem állít elő elektronikus aláírást az általa előállított aláírás-létrehozó adattal,
- 2-es típus: biztosítja az elektronikus aláírás előállítását egy olyan aláírás-létrehozó adat felhasználásával, amelyet egy 1-es típusú BALE-től importál,
- 3-as típus: biztosítja mind az aláírás-létrehozó/aláírás-ellenőrző adatpárok generálását, mind az elektronikus aláírás előállítását az aláírás-létrehozó adattal.

Végül [4] útmutatót nyújt a BALE-k különböző platformokon történő megvalósításához.

1.2. A tanúsítási jelentés feladata

Jelen tanúsítási jelentés fő feladatai:

- az nShield F3 500 for netHSM kriptográfiai hardver eszközre vonatkozó meglévő (FIPS 140-2 level 3) tanúsítási eredmény alapján ki lehet-e mutatni, hogy a kriptográfiai hardver eszköz megfelel a 3-as típusú BALE-kra kidolgozott védelmi profil követelményeinek is, s ezáltal alkalmas-e minősített aláírás-létrehozáshoz való felhasználásra,
- a netHSM kriptográfiai hardver eszközre vonatkozó meglévő tanúsítvány érvényességi feltételei, illetve a többi kielégítendő funkcionális és biztonsági követelmény teljesülése milyen korlátozásokat, feltételeket támaszt a kriptográfiai hardver eszköz (3-as típusú BALE-ként való) felhasználására.

1.3. A tanúsítási jelentés hatóköre

Jelen tanúsítási jelentés hatóköre csak a biztonságos aláírás-létrehozó eszközként való felhasználhatóságra és ennek feltétel-rendszerének meghatározására szorítkozik.

Nem terjed ki a nShield F3 500 for netHSM egyéb tulajdonságaira (pl. titkosításra való felhasználhatóságára).

1.4. A tanúsítási jelentés szerkezete

A tanúsítási jelentés további szerkezete a következő:

- A 2. fejezet az nShield F3 500 for netHSM legfontosabb tulajdonságait, valamint az ezeket igazoló FIPS 140-2 szerinti tanúsítás eredményeit tekinti át.
- A 3. fejezet a tanúsításnál alkalmazott módszert tekinti át.
- A 4. fejezet az értékelés eredményeit tartalmazza.
- Az 5. fejezet az értékelés és tanúsítás következtetéseit írja le: a minősített aláírás-létrehozáshoz való alkalmasság megállapításával, valamint az alkalmazás feltételeinek és korlátainak a meghatározásával.
- A 6. fejezet az alkalmazott rövidítések jegyzéke.
- Végül a 7. fejezet megnevezi az értékelésnél figyelembe vett egyéb dokumentumokat.

2. A tanúsítás tárgyának leírása

2.1. Korábbi tanúsítási eredmények

Az nShield F3 500 for netHSM kriptográfiai hardver eszköz nem rendelkezik a 3-as típusú BALE-kra kidolgozott védelmi profiloknak való megfelelőséget igazoló CC tanúsítvánnyal. Ugyanakkor rendelkezik az alábbi, nemzetközileg elismert tanúsítási eredménnyel:

- FIPS 140-2 szerinti, Level 3 szintű tanúsítvány (lásd 3.5. fejezet /1/ fejlesztői bizonyíték)

Bár a két értékelési/tanúsítási séma (FIPS 140-2 és CC) követelményrendszere teljesen nem feleltethető meg egymásnak, jelentős átfedések, párhuzamosságok vannak köztük.

2.2. Az igazolt tulajdonságok áttekintése

A FIPS 140-2 szerinti, Level 3 szintű tanúsítvány a Biztonsági szabályzatában részletezett alábbi tulajdonságcsoportokkal kapcsolatos biztonsági megfelelést igazolja:

- modul portok és interfészek
- szerepkörök
- az egyes szerepkörök által elérhető szolgáltatások (Command / Service)
- kulcsok
- szabályok
- fizikai biztonság
- funkció erősség
- támogatott algoritmusok

A Biztonsági szabályzat szerint a HSM-et három üzemmódban lehet inicializálni:

- non-FIPS mode
- FIPS level 2 mode
- FIPS level 3 mode

A jelen tanúsítás a FIPS level 3 mode üzemmódra irányul.

Az nShield F3 500 for netHSM dokumentációjában szereplő Műszaki architektúra leírás 6. fejezetében leírja a biztonság réteges szerkezetét, mely az alábbi elemekből áll össze:

- FIPS boundary (FIPS tanúsított HSM: core az összes kriptográfiai művelet számára)
- Platform boundary (zárt fizikai berendezés a maradék rendszerkomponensek számára)
- Transport boundary (hálózati kapcsolat a kliensek és a netHSM között)
- Client boundary (a kliens oldalon megvalósított biztonsági tulajdonságok)

3. A tanúsítás jellemzése

Az alábbiak az értékelés és tanúsítás során alkalmazott értékelési módszert dokumentálják.

3.1. A teljesítendő követelmények és feltételek meghatározása

A 3-as típusú BALE-ra vonatkozó követelményeket az [5] védelmi profil (SSCD PP) határozza meg (vezeti le), az alábbi megközelítéssel:

1. Néhány feltételezés (3.1 Assumptions) mellett meghatározza a kivédendő fenyegetéseket (3.2 Threats to Security) és az érvényre juttatandó szervezeti biztonsági szabályokat (3.3 Organisational Security Policies).
2. Külön-külön meghatározza a TOE-ra (4.1 Security Objectives for the TOE) és annak környezetére (4.2 Security Objectives for the Environment) vonatkozó biztonsági célokat, melyek teljesülése esetén a fenyegetéseket kivédik, a szervezeti biztonsági szabályok pedig érvényre jutnak.
3. Meghatározza, pontosabban a TOE-ra vonatkozó biztonsági célokból levezeti a funkcionális (5.1 TOE Security Functional Requirements) és garanciális biztonsági követelményeket (5.2 TOE Security Assurance Requirements), melyek kielégítése esetén teljesülnek a TOE-ra vonatkozó biztonsági célok.

A fentiekből következik, hogy az nShield F3 500 for netHSM akkor használható (BALE-ként) minősített elektronikus aláírásra, ha:

- az nShield F3 500 for netHSM eszközre teljesülnek az [5] védelmi profilban meghatározott funkcionális biztonsági követelmények (5.1),
- az nShield F3 500 for netHSM eszközre teljesülnek az [5] védelmi profilban meghatározott garanciális biztonsági követelmények (5.2),
- az elektronikus aláírás létrehozási környezetének (ami egyben az nShield F3 500 for netHSM környezete is) teljesülnek az [5] védelmi profilban a környezetre meghatározott biztonsági célok (4.2).

További követelmények és feltételek származhatnak abból a tényből, hogy az [5] védelmi profil indirekt módon smart card, mobile phone, PDA vagy PC platformon képzelte el a BALE megvalósítását, HSM platformon nem (ez egyértelműen látszik [4] 8.-11. fejezeteiből).

A HSM platformnak a fenti megoldásokhoz képest több sajátossága is van:

- a HSM (mint BALE) több különböző felhasználó aláíró magánkulcsát is tárolhatja,
- az aláíró tipikusan nincs a HSM (mint BALE) közelében, amikor aláír,
- a HSM által tárolt magánkulcsok mentése és visszaállítása egy HSM esetén tipikusan támogatott (elvárt) funkcionalitás, BALE esetén viszont szigorúan tilos.

3.2. A követelmények teljesülésének vizsgálata

A funkcionális és garanciális biztonsági követelmények teljesülésének tételes vizsgálata, valamint a fejlesztési bizonyítékokban megadott FIPS 140-2 level 3 szerinti tanúsítási eredmény alapján az alábbi lehetséges határozatok hozhatók minden követelményre:

- az adott követelmény **teljesül**
- az adott követelmény **feltétellel teljesül** (a netHSM működtetésére vonatkozó feltétel(ek) teljesítése esetén)
- az adott követelmény **nem teljesül** (azt a netHSM működési környezetében egy vagy több – reálisan megvalósítható - ellenintézkedéssel kell teljesíteni).

A követelmények teljesülésének tételes vizsgálata kizárólag a netHSM „FIPS level 3 mode" üzemmódjára irányul, alapfeltevés tehát, hogy az eszköz így legyen inicializálva.

3.3. A működtető környezetben (rendszer szinten) vizsgálandó feltételek meghatározása

Az elektronikus aláírás létrehozás (egyúttal a netHSM) működési környezetében egy későbbi, rendszer szintű értékelés keretében ellenőrizendő feltételek az alábbi módon határozhatók meg:

- a „FIPS level 3 mode" üzemmódból adódó feltételek,
- a védelmi profilban a környezetre meghatározott biztonsági célok,
- a „feltétellel teljesül" és „nem teljesül" határozatoknál meghatározott, a működési környezetben megvalósítandó ellenintézkedések,
- a netHSM üzemmódja (lokális vagy távoli),
- a „HSM platform" specifikus problémák megoldása érdekében megvalósítandó ellenintézkedések.

A netHSM elektronikus aláírás létrehozásra két jelentősen eltérő működési környezetben is alkalmazható:

- lokális üzemmódban (amikor a helyi aláíró közvetlenül a netHSM kártyaolvasójába helyezi operátori kártyáját), és
- távoli üzemmódban (amikor a távoli aláíró távolról, egy miniHSM kártyaolvasójába helyezi operátori kártyáját).

3.4. A tanúsításhoz felhasznált értékelési jelentések azonosítása

Értékelési jelentés:

> nShield F3 500 for netHSM biztonságos aláírás-létrehozó eszköz /Hardware Version: nC4033P-500N, Firmware Version: 2.33.60-3/ ÉRTÉKELÉSI JELENTÉS v1.0 /netHSM_SSCD_ETR_v1.0.doc/

3.5. Az értékeléshez felhasznált fejlesztői bizonyítékok

Az értékelés az alábbi bizonyítékokat használta fel:

Fejlesztői bizonyíték	Cím	Verzió
/1/ NIST – CSEC FIPS 140-2 szerinti Level 3 szintű Tanúsítvány	FIPS 140-2 Validation Certificate – nShield F3 500, nShield F3 500 for NetHSM and nShield F3 10 PCI by nCipher Corporation Ltd. (When operated in FIPS mode)	Certificate No. 966
/2/ Biztonsági szabályzat	nShield Security Policy nShield F3 500, nShield F3 500 for NetHSM and nShield F3 10 PCI in FIPS 140-2 level 3 mode	Version: 2.2.3 3 June 2008
/3/ Útmutató	nCipher Security Officer's Guide	-
/4/ Útmutató	Technical Reference Manual	-
/5/ Műszaki architektúra leírás	nCipher netHSM Technical Architecture – White Paper	-
/6/ Felhasználói útmutató	nShield – User Guide for Windows	7.1

4. Az értékelés eredményei

Ez a fejezet az értékelés eredményeit foglalja össze:

- 4.1 az [5] védelmi profil (funkcionális és garanciális) biztonsági követelményeinek teljesülésére vonatkozó határozatokat tartalmazza,
- 4.2 a működtető környezetben vizsgálandó feltételeket határozza meg.

4.1 Az SSCD PP biztonsági követelményeinek teljesülése

4.1.1. Az SSCD PP funkcionális biztonsági követelményeinek teljesülése

Az alábbi táblázat áttekinti az eredményeket.

SSCD SFR azonosítója	SSCD PP SFR elnevezése	határozat	feltétel (lásd 4.2.3)
FCS	**Kriptográfiai támogatás**		
FCS_CKM.1	A kriptográfiai kulcsok előállítása	teljesül	-
FCS_CKM.4	A kriptográfiai kulcsok megsemmisítése	teljesül	-
FCS_COP.1	Kriptográfiai műveletek		
/Correspond	SCD/SVD megfelelés ellenőrzés	teljesül	-
/Signing	Aláírás-létrehozás	teljesül	-
FDP	**A felhasználói adatok védelme**		
FDP_ACC.1	Részleges hozzáférés ellenőrzés		
/Initialisation	Inicializáláskor	teljesül	-
/Personalisation	Megszemélyesítéskor	teljesül	-
/SVD Transfer	Nyilvános kulcs exportáláskor	teljesül	-
/Sign-creation	Aláírás-létrehozáskor	feltétellel teljesül	6., 7.
FDP_ACF.1	Biztonsági tulajdonság alapú hozzáférés ellenőrzés		
/Initialisation	Inicializáláskor	feltétellel teljesül	5.
/Personalisation	Megszemélyesítéskor	teljesül	-
/SVD Transfer	Nyilvános kulcs exportáláskor	teljesül	-
/Sign-creation	Aláírás-létrehozáskor	teljesül	-
FDP_ETC.1	Felhasználói adatok exportálása biztonsági tulajdonságok nélkül	teljesül	-
FDP_ITC.1	Felhasználói adatok importálása biztonsági tulajdonságok nélkül	teljesül	-
FDP_RIP.1	Részleges maradvány információ védelem	teljesül	-
FDP_SDI.2	A tárolt adatok sértetlenségének figyelése és beavatkozás		
/Persistent	folyamatosan tárolt adatokra	teljesül	-
/DTBS	átmenetileg tárolt adatokra	teljesül	-
FDP_UIT.1	A tárolt adatok sértetlenségének figyelése és beavatkozás		
/SVD Transfer	nyilvános kulcs exportálásánál/fogadásakor	feltétellel teljesül	4.
/TOE DTBS	DTBS fogadásakor	teljesül	-
FIA	**Azonosítás és hitelesítés**		
FIA_AFL.1	Hitelesítési hibák kezelése	nem teljesül	10.
FIA_ATD.1	Felhasználói tulajdonságok megadása	teljesül	-
FIA_UAU.1	A hitelesítés időzítése	feltétellel teljesül	1., 2., 3.

SSCD SFR azonosítója	SSCD PP SFR elnevezése	határozat	feltétel (lásd 4.2.3)
FIA_UID.1	Az azonosítás időzítése	teljesül	-
FMT	**Biztonsági menedzsment**		
FMT_MOF.1	A biztonsági funkciók viselkedésének kezelése	teljesül	-
FMT_MSA.1 /Adminitrator /Signatory	Biztonsági tulajdonságok kezelése Adminisztrátor esetén Aláíró esetén	 teljesül teljesül	 - -
FMT_MSA.2	Biztonságos biztonsági tulajdonságok	teljesül	-
FMT_MSA.3	Statikus tulajdonságok kezdeti értékadása	teljesül	-
FMT_MTD.1	TSF adatok kezelése	feltétellel teljesül	2., 3.
FMT_SMR.1	Biztonsági szerepkörök	teljesül	-
FPT	**A TOE biztonsági funkciók védelme**		
FPT_AMT.1	Az alapot jelentő absztrakt gép tesztelése	teljesül	-
FPT_EMSEC.1	A TOE kisugárzása	feltétellel teljesül	8.
FPT_FLS.1	Hiba esetén biztonságos állapot megőrzése	teljesül	-
FPT_PHP.1	A fizikai támadás passzív észlelése	feltétellel teljesül	9.
FPT_PHP.3	A fizikai támadásokkal szembeni ellenálló képesség	teljesül	
FPT_TST.1	A TSF tesztelése	teljesül	-
FTP	**Megbízható útvonal/csatornák**		
FTP_ITC.1 /SVD Transfer /DTBS Import	TSF-ek közötti megbízható csatorna A nyilvános kulcs CGA felé exportálásakor A DTBS fogadása SCA-tól aláírásra	 feltétellel teljesül teljesül	 4. -
FTP_TRP.1	Megbízható útvonal	teljesül	-

4.1.2. Az SSCD PP garanciális biztonsági követelményeinek teljesülése

Az nShield F3 500 for netHSM rendelkezik FIPS 140-2 szerinti, Level 3-as szintű tanúsítvánnyal (lásd 3.5 fejezet /1/ fejlesztői bizonyíték).

A garanciális elvárások tekintetében a FIPS 140-2 (a FIPS 140-1 továbbfejlesztése után) már közvetlenül összehasonlítható a CC-vel. Az alábbi táblázat a garancia osztályok megfelelését adja meg (az SSCD PP-nek megfelelő v2.1-es CC verzióval):

CC v2.1 garanciaosztályai	FIPS 140-2 megfelelője
10. ASE: Security Target evaluation	Appendix C: Cryptographic Module Security Policy
13 ACM: Configuration management	4.10 Design Assurance 4.10.1 Configuration Management
14 ADO: Delivery and operation	4.10 Design Assurance 4.10.2 Delivery and Operation
15 ADV: Development	4.10 Design Assurance 4.10.3 Development
16 AGD: Guidance documents	4.10 Design Assurance 4.10.4 Guidance Documents
17 ALC: Life cycle support	Ennek a garanciaosztálynak nincs közvetlen megfelelője
18 ATE: Tests	4.9 Self-Tests
19 AVA: Vulnerability assessment	4.5: Physical Security 4.7: Cryptographic Key Management 4.8: Electromagnetic Interference/Compatibility (EMI/EMC) 4.11: Mitigation of Other Attacks

A fentieken kívül számos mértékadó dokumentum, köztük az alábbiak is:

- ETSI TS 101 456: Policy Requirements for Certification Authorities Issuing Qualified Certificates
- CEN 14167-1 munkacsoport egyezmény: Security Requirements for Trustworthy Systems Managing Certificates for Electronic Signatures
- 2/2002. (IV. 26.) MeHVM irányelv a minősített elektronikus aláírással kapcsolatos szolgáltatásokra és ezek szolgáltatóira vonatkozó biztonsági követelményekről

az alábbi megfeleltetéseket teszi a FIPS 140 és a CC garancia szintjei között:

FIPS 140	CC (ISO/IEC 15408)
Level 1	EAL 2
Level 2	EAL 3
Level 3	**EAL 4**

A fenti táblázat utolsó sorából következik az nShield F3 500 for netHSM lényegi megfelelése az SSCD védelmi profil garanciális biztonsági követelményeinek.

Az SSCD PP EAL 4+ garanciaszintet vár el: a megemelt követelmények a sebezhetőséggel szembeni ellenállásra vonatkoznak (AVA_MSU.2 helyett AVA_MSU.3, AVA_VLA.2 helyett AVA_VLA.4 az elvárás). Ez azt jelenti, hogy az SSCD PP alacsony helyett magas támadó képességű támadó ellen is védelmet igényel.

A magas támadó képességű támadó elleni védelmet a FIPS Level 3 nem várja el. Ugyanakkor (ellentétben a felhasználók személyes felügyelete alatt álló BALE-kkel) egy HSM modult védett fizikai környezetben működtetik, ezért ez elfogadható.

4.2. A működtető környezetben (rendszer szinten) vizsgálandó feltételek

4.2.1. A „FIPS level 3 mode" üzemmódból adódó feltételek

FIPS 140-2 level 3 megfelelés
A Security World létrehozásakor biztosítani kell a FIPS 140-2 level 3 megfelelőséget.

A modul ellenőrzése
A fizikai biztonság érdekében rendszeresen ellenőrizni kell a netHSM készüléken vagy a miniHSM-en elhelyezett „tamper-detecting" jelzés sértetlenségét.

4.2.2. Az SSCD PP környezetre meghatározott biztonsági céljai

OE.CGA_QCert Minősített tanúsítványok generálása
A CGA minősített tanúsítványokat generál, amelyek tartalmazzák többek között

a) a TOE-t használó aláíró nevét,
b) az aláíró kizárólagos befolyása alatt álló TOE által tartalmazott SCD-hez tartozó SVD-t,
c) a CSP fokozott biztonságú aláírását.

OE.SVD_Auth_CGA A CGA ellenőrzi az SVD hitelességét
A CA ellenőrzi, hogy az SCD-e a kapott SVD küldője, valamint ellenőrzi a kapott SVD sértetlenségét. A CA ellenőrzi az aláíró BALE-jében lévő SCD és a minősített tanúsítványban szereplő SVD közötti összetartozást.

OE.HI_VAD A VAD védelme
Ha külső eszköz gondoskodik a humán interfészről a felhasználói hitelesítés során, akkor ennek az eszköznek biztosítania kell a VAD bizalmasságát és sértetlenségét, ahogyan azt az alkalmazott hitelesítési módszer megkívánja.

OE.SCA_Data_Intend Az aláírni kívánt adat
Az SCA

a) elkészíti a DTBS-ként bemutatott adat DTBS-reprezentációját, amit az aláíró alá akar írni, a TOE által aláírásra alkalmas formában;
b) továbbítja a DTBS-reprezentációt a TOE felé, és lehetővé teszi, hogy a TOE ellenőrizni tudja a DTBS-reprezentáció sértetlenségét;
c) hozzácsatolja a TOE által előállított aláírást az adathoz, vagy különállóan szolgáltatja azt.

4.2.3. Az SSCD PP feltétellel teljesített követelményeiből adódó kiegészítő elvárások

1. Létre kell hozni egy FIPS 140-2 level 3-nak megfelelő Security World-t, benne egy ACS-t és a szükséges számú OCS-t.

2. Az ACS kártya készlet két, az OCS kártya készletek pedig egy elemből álljanak.

3. Minden felhasználónak használnia kelljen egy pass phrase-t.

4. Az aláíró kulcspárokat a netHSM-mel oly módon kell generáltatni, mely a nyilvános kulcsokat aláírással védi. A Generate Key Pair parancs kiadásakor használni kell azt az opcionális lehetőségét, hogy a netHSM aláíró kulcsával (module signing key) aláírja mindkét kulcsot, és e két generált tanúsítványt is exportálja. /Ehhez arra is szükség lesz, hogy a modul aláíró magánkulcs nyilvános felét a Get Module Long Term Key parancs segítségével exportálják, a generált tanúsítványok validálhatósága érdekében./
Az aláíró kulcspárokat az aláírók generálják.
A QCA felé az aláíró személyének és a nyilvános kulcsnak az összetartozását még külön igazolni kell (vagy az aláíró viszi be személyesen a nyilvános kulcsát, vagy egy RO személyesen felügyeli a nyilvános kulcs exportálását).

5. Az aláíró kulcspárt ne az NSO generálja, hanem maguk az aláírók. Ehhez a későbbi aláírók számára az NSO (egy erre a célra kibocsájtott tanúsítvánnyal) engedélyezze az RSA aláíró kulcspár generálást.

6.Az aláíró a következő paraméterekkel generálja az RSA kulcspárt:
- cél: aláírás,
- aktivizáló: kizárólag saját maga,
- algoritmus: RSA,
- kulcsméret: minimum 2048

7. A Security World-t OCS replacement opció nélkül kell létrehozni.

8. Az nShield F3 500 for netHSM környezete olyan fizikai védelem alatt álljon, mely megakadályozza a bekapcsolt, működő nShield F3 500 for netHSM speciális eszközökkel való manipulálását, fizikai támadását.
Amennyiben az nShield F3 500 for netHSM (pl lopás miatt) kikerül ebből a védett környezetből, valamennyi általa generált magánkulcsához tartozó aláíró tanúsítványt haladéktalanul vissza kell vonatni.

9. Az nShield F3 500 for netHSM működtetési környezetében rendszeresen ellenőrizni kell az alábbiakat:
- Meg kell vizsgálni az epoxy gyanta bevonatot, hogy van–e rajta valamilyen látható sérülés.
- Az intelligens kártya olvasó kábele közvetlenül a modulba csatlakozik, és sehol sincs megbontva. Ahol a modul egy eszköz, ott a csatlakozás biztonságát védhetik pecsétek vagy más bontásvédelmi megoldások.

10. Az nShield F3 500 for netHSM-et meghívó (a környezet részét képező) aláíró szoftver kezelje le az nShield F3 500 for netHSM által visszajelzett sikertelen hitelesítési kísérleteket, és kényszerítse ki az alábbiakat:

- az első sikertelen kísérlet után iktasson be egy t (t konfigurálható vagy fix 1 sec értékű) késleltetést a következő kísérlet felkínálásáig,
- minden későbbi sikertelen kísérlet után növelje kétszeresére ezt a késleltetést,
- sikeres hitelesítés után állítsa vissza t alapértékét.

11. A környezet részét képező aláíró szerver kényszerítse ki, hogy a jelmondat legalább 8 karakterből álljon, valamint betűt és számot is tartalmazzon. (Az SSCD PP közvetlenül nem tartalmaz elvárást a jelszó metrikájára nézve (FIA_SOS.1 nincs), de az EAL4 garanciális szint közvetve elvárja, hogy ne lehessen alacsony támadó képességgel áthatolni a hitelesítésen.

4.2.4. A „HSM platform" specifikus problémákból adódó kiegészítő ellenintézkedések

A következő problémákat kell átgondolni:

1. A HSM több aláíró magánkulcsát is kezeli, ezeket egymás elől is védeni kell.
   Csak aláíró tud aláírni (FDP_ACF.1/ Sign-creation)
   Aláírni csak sikeres hitelesítés után lehet (FIA_UAU.1), melynek keretében bizonyítani kell (birtok és tudás alapján) a magánkulcs feletti rendelkezést.
   Következésképp egy hitelesített aláíró csak a saját maga által aktivizálható magánkulcsokkal tud aláírást létrehozni.

2. A magánkulcsok aktivizálását védeni kell az adminisztrátoroktól.
   Csak aláíró tud aláírni (FDP_ACF.1/ Sign-creation)
   Csak aláíró írhat alá, NSO nem.

3. Ki kell zárni annak lehetőségét, hogy egy adminisztrátor mentsen, duplikáljon, klónozzon magánkulcsot, és ezen keresztül egy másik felhasználót aláíró jogosultsággal ruházzon fel.
   OCS replacement opció nélkül kell a Security World-t létrehozni. Ez önmagában kizárja, hogy egy NSO mentsen, duplikáljon, klónozzon magánkulcsot.

4. A HSM nem tárolja a magánkulcsokat, hanem titkosítja és exportálja, majd a felhasználás előtt importálja, dekódolja és integritását ellenőrzi. Átgondolandó a HSM-en kívüli magánkulcs tárolás biztonsága.
   A key blob-ok AES256-tal titkosítva vannak tárolva a netHSM-en kívül.
   Ez megfelelő biztonságot ad arra, hogy senki sem képes ebből visszaállítani a magánkulcsot.
   Amennyiben egy key blob megsérül vagy megsemmisül, új magánkulcsot kell generálni (tehát vigyázni kell ezekre, javasolt mentésük is), de visszaélésre a mentésen keresztül sincs mód (az AES titkosítás kellő védelmet nyújt a magánkulcs megismerése ellen) .

5. A Tanúsítási jelentés eredménye és érvényességi feltételei

5.1. Következtetések

5.1.1. Az értékelés összefoglaló eredménye

Az értékelés fő következtetései az alábbiak:

Az nShield F3 500 for netHSM (Hardware Version: nC4033P-500N, Firmware Version: 2.33.60-3, a továbbiakban netHSM) kriptográfiai hardver eszközre vonatkozó meglévő FIPS 140-2 level 3 szerinti tanúsítási eredményekből közvetlenül nem vezethető le teljesen, hogy az eszköz megfelel 3-as típusú BALE-kra kidolgozott védelmi profil követelményeinek.

Az nShield F3 500 for netHSM installálására, konfigurálására, informatikai rendszerbe integrálására és működtetésére ugyanakkor meghatározhatók olyan korlátozások és feltételek, melyek teljesítése esetén az eszköz megfelel az [1] törvény és a [2] irányelv BALE-kre vonatkozó követelményeinek, felhasználásával több aláíró is létrehozhat minősített elektronikus aláírásokat.

A meghatározott korlátozások és feltételek teljesülését az nShield F3 500 for netHSM-t működtető informatikai rendszer biztonsági értékelésével lehet és kell ellenőrizni, igazolni.

5.2. A Tanúsítási jelentés eredménye

Az nShield F3 500 for netHSM
kriptográfiai hardver eszköz
/nCipher Corporation Ltd./

tanúsítás tárgyát képező verziója

Hardware Version: nC4033P-500N, Firmware Version: 2.33.60-3

a tanúsítás érvényességi feltételeinek együttes teljesülése esetén

ALKALMAS

minősített aláírások létrehozására

mint

3-as típusú biztonságos aláírás-létrehozó eszköz.

5.2.1. Feltételek

A tanúsítás fenti következtetései az alábbi, az üzemeltetési környezetre vonatkozó feltételezések teljesülésén múlnak.

Feltételek az előkészítés szakaszában:

1. Inicializálás során az alábbi lépéseket kell elvégezni:
   a) Gyári alapállapotba hozás (Initialise)
   b) Firmware verzió ellenőrzése (New Enquiry, elvárt verziószám 2.33.60)
   c) Hosszú távú kulcs generálása (Generate KLF).
   d) Hosszú távú kulcs nyilvános felének exportálása (GetLongTermKey)

2. A Security World létrehozása során az alábbi opciókat kell beállítani:

• Cipher suite: AES	key blobok titkosítása AES-sel
• Key recovery: No	nincs kulcs helyreállítás
• ACS (K and N): (N=K=2)	titokmegosztás van a 2 NSO (adminisztrátor) között
• pass phrases: YES	az adminisztrátor hitelesítéséhez jelmondat is kell
• FIPS 140-2 level 3 compliance: YES	FIPS 140-2 level 3 üzemmód
• FTO: NO	csak nCipher kártya használható
• Remote Operator: YES	az aláírónak távolról is hozzá kell férnie a netHSM-hez
• OCS replacement: NO	NSO ne tudjon magánkulcsot menteni, klónozni, átruházni
• Pass phrase replacement: NO	NSO ne tudjon jelmondatot visszaállítani
• Nonvolatile memory (NVRAM) options: NO	a key-blob tárolható a kriptográfiai hardver eszközön kívül
• Security World SEE options: NO	az SEE (nCipher Secure Execution Engine) használatának tiltása
• Real-time clock (RTC) options: NO	az RTC (Real-time clock) használatának tiltása
• Security World replacement options: NO	NSO ne tudjon Security World-öt-t klónozni

3. Az Operator Card Set-ek (OCS) létrehozása a kártyatulajdonosok (operátorok, aláírók) jelenlétében az alábbi beállításokkal történjen:

• OCS (K and N): (N=K=1)	nincs titokmegosztás az aláíróknál
• pass phrases: YES	hitelesítéshez jelmondat is kell
• formal FIPS 140-2 level 3 compliance: YES	FIPS 140-2 level 3 üzemmód
• OCS persistent: YES	csak olvasóba helyezett kártya mellett lehet aláírást kezdeményezni
• remotely-readable: YES vagy NO	YES esetén a kártya távolról is olvasható
• Time-outs: nincs feltétel	
• pass phrase replacement: NO	az NSO ne állíthassa vissza az aláíró jelmondatát
• felhatalmazás kulcspár generálására	NSO tanúsítvánnyal engedélyt ad

4. Amennyiben az OCS létrehozása során engedélyezésre került a távoli kártya olvasás (remotely-readable: YES) akkor miniHSM alkalmazása szükséges az aláírói végponton. Az alkalmazott miniHSM-re teljesülniük kell az alábbiaknak:

- érvényes FIPS 140-2 level 3 szerinti tanúsítvánnyal rendelkezzen,
- a jelen tanúsítvány tárgyát képező HSM verzióval (nShield F3 500 for netHSM, hardver verzió: nC4033P-500N, förmver verzió: 2.33.60-3) kliens üzemmódban együttműködésre képes szoftver/förmver verzióval legyen ellátva.

5. A létrehozott operátorok (aláírók) kulcspár generálása az alább lépésekből álljon:

a) Kulcspár generálás /cél: aláírás, aktivizáló: kizárólag saját maga, algoritmus: RSA, kulcsméret: minimum 2048, key recovery: nem/,
b) Nyilvános kulcs exportálása,
c) QCA-hoz továbbítás /vagy az aláíró viszi be személyesen a nyilvános kulcsát, vagy egy RO személyesen felügyeli a nyilvános kulcs exportálását/,
d) A QCA ellenőrzi a nyilvános kulcs hitelességét /azaz a nyilvános kulcs sértetlen, az aláíró rendelkezik a nyilvános kulcshoz tartozó, megfelelő magánkulccsal, a kulcspárt egy BALE generálta /,
e) A QCA minősített tanúsítványt generál /amely tartalmazza többek között az aláíró nevét, a nyilvános kulcsot, a QCA fokozott biztonságú aláírását/,
f) A generált minősített tanúsítvány visszajuttatása az aláíró szoftverhez.

6. A 2-es feltételben szereplő ACS titokmegosztás (ACS (K and N): N=K=2) érvényesítése az alábbi módon történjen:

- az egyik NSO kártyája és jelmondata az üzemeltetőknél marad,
- a másik NSO kártyája és leírt, borítékba zárt jelmondata egy közjegyzőhöz kerül, a szükséges OCS-ek létrehozását és legenerálását követően haladéktalanul, az auditor jelenlétében.

7. Amennyiben a jövőben új aláírói végpont (miniHSM) telepítésére lesz szükség, a titokmegosztás érvényesítése az alábbi módon történhet:
   - az auditor jelenlétében felveszik a közjegyzőtől a második NSO kártyát és a hozzá tartozó jelmondatot tartalmazó borítékot,
   - az auditor jelenlétében és a két NSO közreműködésével megtörténik az új aláírói végpont létrehozása,
   - a második NSO kártyája és leírt, borítékba zárt jelmondata haladéktalanul visszakerül a közjegyzőhöz, az auditor jelenlétében.

8. Az nShield F3 500 for netHSM készüléken, illetve az alkalmazott miniHSM-en az auditor (ld. 19. feltétel) helyezzen el az eszköz felnyitását egyértelműen bizonyító, egyedi azonosítóval rendelkező „tamper-detecting" jelzést.

Feltételek az aláíró szoftver oldalán:

9. Az nShield F3 500 for netHSM-et meghívó (a környezet részét képező) aláíró szoftver kezelje le az nShield F3 500 for netHSM által visszajelzett sikertelen hitelesítési kísérleteket, és kényszerítse ki az alábbiakat:
   - az első sikertelen kísérlet után iktasson be egy *t* (*t* konfigurálható vagy fix, legalább 1 sec értékű) késleltetést a következő kísérlet felkínálásáig,
   - minden későbbi sikertelen kísérlet után növelje kétszeresére ezt a késleltetést,
   - sikeres hitelesítés után állítsa vissza *t* alapértékét.

10. A környezet részét képező aláíró szoftver kényszerítse ki, hogy a jelmondat legalább 8 karakterből álljon, valamint betűt és számot is tartalmazzon.

11. A környezet részét képező aláíró szoftver:
   - ellenőrizze, hogy a gyártó által szállított PKCS#11 vagy egyéb (Microsoft CSP, Java) driver-rel kommunikál,
   - készítse el az aláírandó adatként bemutatott adat DTBS-reprezentációját (legalább SHA256 vagy SHA512 hash képét) a netHSM által aláírásra alkalmas formában,
   - továbbítsa a DTBS-reprezentációt a netHSM felé,
   - csatolja a netHSM által előállított aláírást az adathoz.

12. A környezet részét képező aláíró szoftver:
   - minden aláírandó dokumentum csomag indítása esetén kötelezően kérje be az OCS jelszót, és authentikálja az OCS-t (ezen keresztül az aláírót), és ha az OCS nincs jelen, ne induljon el (azaz minden csomag indítása előtt kötelezően új munkamenetet építsen fel),
   - az aláírások elkészültét követően azonnal szakítsa meg a munkamenetet a netHSM-mel.

Feltételek a működtetés szakaszában:

13. Az nShield F3 500 for netHSM környezete olyan fizikai védelem alatt álljon, mely megakadályozza a bekapcsolt, működő nShield F3 500 for netHSM speciális eszközökkel való manipulálását, fizikai támadását.
Amennyiben a netHSM (például lopás miatt) kikerül ebből a védett környezetből, valamennyi a rendszerben generált magánkulcshoz tartozó aláíró tanúsítványt haladéktalanul vissza kell vonatni, a netHSM-et pedig újra kell inicializálni.

14. A netHSM készüléken vagy a miniHSM-en az auditor által elhelyezett „tamper-detecting" jelzés sértetlenségét rendszeresen ellenőrizni kell. Amennyiben a jelzés sérült, a rendszer által kezelt aláíró kulcsokhoz tartozó tanúsítványokat vissza kell vonni, és magát az eszközt újra kell inicializálni.

15. Az aláíró vigyázzon a hitelesítéséhez szükséges eszközére (nCipher smart card), kizárólag a miniHSM-hez vagy az nShield F3 500 for netHSM-hez való hozzáféréskor használja azt, védett környezetben. Az aláírások jóváhagyását, az aláírások megkezdését követően haladéktalanul vegye ki az olvasóból, és tartsa személyes felügyelete alatt. Amennyiben a hitelesítéshez szükséges eszköz kikerül az aláíró ellenőrzése alól, az általa generált magánkulcshoz tartozó tanúsítványt haladéktalanul vissza kell vonatnia.

16. Az aláíró vigyázzon a hitelesítéséhez szükséges tudására (pass phrase), értékét senkinek se fedje fel, illetve a OCS-t biztonságos helyen őrizze.

17. Az aláíró magánkulcsok key blob-ok formájában, AES256-tal titkosítva vannak tárolva az nShield F3 500 for netHSM-en kívül. Amennyiben egy ilyen key blob helyreállíthatatlanul megsemmisül, új magánkulcsot kell generálni, a megsemmisült kulcshoz tartozó tanúsítványt pedig vissza kell vonatni.

18. A minősített aláírások létrehozására használt magánkulccsal kizárólag minősített elektronikus aláírást szabad létrehozni.

19. Az nShield F3 500 for netHSM eszközzel csak olyan rendszerben lehet minősített elektronikus aláírást előállítani, amely rendszer jelen tanúsítványban lévő 1.-12. feltételeknek való megfelelését az informatika biztonsági szakterület jogszabályban rögzített vagy nemzetközi mértékadó követelményen alapuló technológiai értékelési követelményrendszere alapján

- akkreditált értékelő szervezet a megfelelő akkreditált eljárásrendben értékelte, és
- ennek alapján akkreditált tanúsító szervezet a megfelelő akkreditált eljárásrendben tanúsította.

6. Rövidítések és szakkifejezések

6.1. Rövidítések

Az alábbiakban meghatározzuk a jelen értékelési jelentésben használt betűszavak jelentését.

ACS (Administrator Card Set)	adminisztrátori kártya készlet
CA (Certification Authority)	hitelesítés-szolgáltató
CC (Common Criteria)	Közös szempontok
CGA (Certification-generation application)	tanúsítvány-létrehozó alkalmazás
CEN (Comité Européen de Normalisation)	Európai Szabványügyi Bizottság
CSEC	Communications Security Establishment Canada
CSP (Critical security parameter)	Kritikus biztonsági paraméter
CWA (CEN Workshop Agreement)	CEN munkacsoportmegállapodás
DTBS (Data to be signed)	aláírandó adat
EAL (Evaluation Assurance Level)	értékelési garanciaszint
ETR (Evaluation Technical Report)	értékelési jelentés
ETSI (European Telecommunication Standards Institute)	Európai Telekommunikációs Szabványok Intézete
FIPS	Federal Information Processing Standard
HSM (Hardware Security Module)	kriptográfiai hardver eszköz
NIST	National Institute of Standards and Technology
OCS (Operator Card Set)	operátori kártya készlet
QCA (Qualified Certification Authority)	minősített hitelesítés-szolgáltató
RSA (Rivest-Shamir-Adleman)	RSA-eljárás
SCA (Signature-creation application)	aláírás-létrehozó alkalmazás
SCD (Signature-creation data)	aláírás-létrehozó adat (magánkulcs)
SFR (Security Functional Requirement)	funkcionális biztonsági követelmény
SHA (Secure Hash Algorithm)	biztonságos hash algoritmus
SSCD (Secure signature-creation device)	BALE (biztonságos aláírás-létrehozó eszköz)
SVD (Signature verification data)	aláírás-ellenőrző adat (nyilvános kulcs)
TOE (Target of Evaluation)	értékelés tárgya
TSF (TOE Security Functionality)	a TOE biztonsági funkcionalitása
TSP (TOE Security Policy)	a TOE biztonsági szabályzata
VAD (Verification authentication data)	hitelesítő adat

7. A tanústáshoz figyelembe vett egyéb dokumentumok

[1]: 2001. évi XXXV törvény az elektronikus aláírásról

[2]: Az Európai Parlament és Tanács 1999/93/EK Irányelv (1999. december 13.) az elektronikus aláírásra vonatkozó közösségi keretfeltételekről.

[3]: CWA 14169, Secure signature-creation devices “EAL 4+”, March 2004

[4]: CWA 14355, Guidelines for the implementation of Secure Signature-Creation Devices, March 2004

[5]: Protection Profile — Secure Signature-Creation Device - Type 3, March 2004 (Prepared By: ESIGN Workshop - Expert Group F)