RENDSZER
TANÚSÍTÁSI JELENTÉS

a Mezőgazdasági és Vidékfejlesztési Hivatal által üzemeltetett, az „nShield F3 500 for netHSM” kriptográfiai hardver eszköz aktivizálásán keresztül minősített elektronikus aláírásokat létrehozó informatikai rendszerről

(2013. október 17-én aktuális verzió)

HUNG-TJ-MIBÉTS-008-2013

Verzió:	1.0	
Fájl:	Hung-TJ-MIBETS-008-2013v10.pdf	
Minősítés:	Nyilvános	
Oldalak:	16	

Változáskezelés

Verzió	Dátum	A változás leírása
v0.01	2013.10.01	A szerkezet felállítása
v0.02	2013.10.20	A tanúsítás eredményeit tartalmazó, az értékelővel egyeztetett teljes változat
v1.0	**2013.10.21**	**Végleges verzió**

A tanúsítási jelentést készítette:

Juhász Judit
HunGuard Kft
Tanúsítási divízió

Tartalomjegyzék

1 Összefoglaló

1.1 A tanúsítás jellemzői

STOE név:	a Mezőgazdasági és Vidékfejlesztési Hivatal által üzemeltetett, az „nShield F3 500 for netHSM” kriptográfiai hardver eszköz aktivizálásán keresztül minősített elektronikus aláírásokat létrehozó informatikai rendszer (MVH_BALE)
STOE verzió:	2013. október 17-én aktuális verzió (SW: v1.0.13282)
Rövid elnevezés:	**MVH_BALE v1.0**
Rendszer integrátor:	Fornax Zrt
Rendszer működtető:	Mezőgazdasági és Vidékfejlesztési Hivatal (MVH)
Rendszer üzemeltető:	Mezőgazdasági és Vidékfejlesztési Hivatal (MVH)
Értékelő szervezet:	Hunguard Kft. Értékelési Divízió.
Az értékelés módszere:	KIB 28 ajánlás szerinti Rendszerekre vonatkozó értékelési módszertan
Az értékelés garanciaszintje:	MIBÉTS fokozott (SAP-F)

1.2 STOE áttekintés

A rendszer tanúsítás tárgya a Mezőgazdasági és Vidékfejlesztési Hivatal által üzemeltetett, az „nShield F3 500 for netHSM” kriptográfiai hardver eszköz aktivizálásán keresztül minősített elektronikus aláírásokat létrehozó informatikai rendszer (a továbbiakban MVH_BALE rendszer).

Az MVH_BALE rendszer nagyszámú, elektronikus aláírás létrehozását teszi lehetővé az alábbi jellemzőkkel:

- az aláírandó pdf állományok egy külső rendszerben keletkeznek, egy fájl-kötegben kerülnek aláírásra átadásra az MVH_BALE-nek, majd az ebből a kötegből ténylegesen aláírt pdf állományokat ez a külső rendszer használja fel.
- az aláíró egy dedikált munkaállomáson áttekintheti, kihagyhatja vagy jóváhagyhatja az aláírandó állományokat, miután behelyezte titkot tartalmazó operátori kártyáját a munkaállomáson elhelyezett miniHSM olvasójába, illetve a munkaállomáson begépelte jelszavát,
- az aláírás egy aláíró szerveren hajtódik végre, egy BALE minősítésű HSM modul (netHSM) aktivizálásával, mely egyszerre több aláíró magánkulcsát tárolja és kezeli,
- a távoli hozzáférést a miniHSM és a netHSM között kiépített megbízható útvonal védi.

Az MVH_BALE rendszer által megvalósítandó folyamat magában foglalja az alábbiakat:

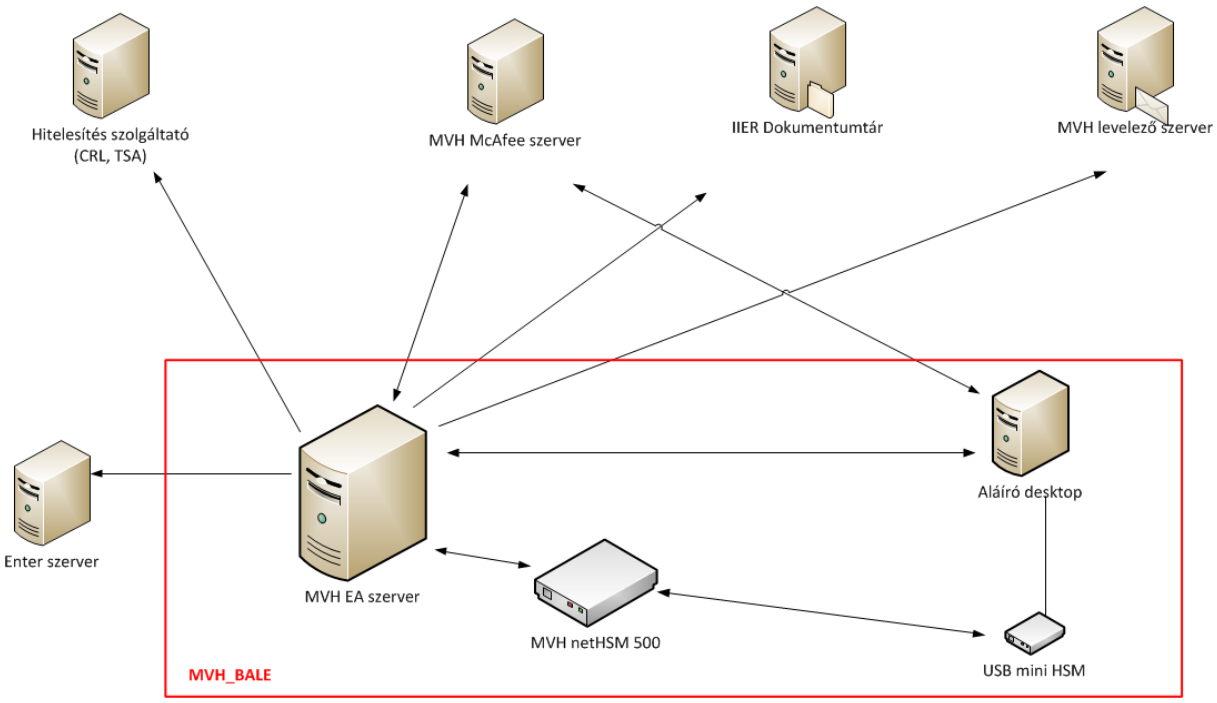
- az aláírandó dokumentumok átvétele egy külső rendszerből,
- az aláírandó dokumentumok opcionális megtekintése, esetleges kihagyása az aláírandó dokumentumok közül,
- a kiválasztott dokumentumokra egyenként minősített elektronikus aláírás létrehozása (a netHSM és az aláíró operátori kártyáján lévő információkkal elérhető magánkulcs aktivizálásával) és időbélyegzése időbélyeg-szolgáltatótól kért időbélyeggel,
- az aláírások kezdeti ellenőrzése,
- az aláírás eredményeinek opcionális lekérése.

Az MVH_BALE rendszer biztonsági funkciói magában foglalják az alábbiakat:

- a rendszerhez hozzáférő különböző szerepkörű felhasználók (aláírók, illetve az aláírói fiókok kezelésre jogosult adminisztrátorok) tanúsítvány alapú azonosítása és hitelesítése,
- hozzáférés ellenőrzés (a nyújtott szolgáltatásokat csak az arra jogosultak érik el, a megfelelő azonosítás és hitelesítés után),
- minősített elektronikus aláírás létrehozása és kezdeti ellenőrzése,
- időbélyeg kérés, és a kapott időbélyeg válasz elhelyezése az elektronikus aláíráson,
- naplózás (biztonsági naplóbejegyzések készítése a rendszer működéséről),
- rendszer és információ sértetlenség védelem (benne: rosszindulatú kódok elleni védelem, biztonsági funkcionalitás ellenőrzése, szoftver és információ sértetlenség ellenőrzés, a bemeneti információra vonatkozó korlátozások érvényesítése),
- rendszer és kommunikáció védelem,
- önvédelem (a biztonsági funkciók megkerülése vagy lerontása elleni védelem).

1.3 A tanúsítás tárgyának biztonsági környezete és határai

Az MVH_BALE egy nagyobb, az MVH teljes körű elektronikus ügyintézési folyamatát megvalósító informatikai rendszert (az Integrált Igazgatási és Ellenőrzési Rendszer, IIER) kiegészítő alrendszer. Az IIER architektúráját az 1. ábra szemlélteti, benne piros keretben szerepel a most értékelt alrendszer.



1. ábra: Az IIER architektúrája

Az IIER lényegi funkcionalitását az „Enter szerver” komponens valósítja meg.

Az aláírást megvalósító MVH_BALE (al)rendszer az „MVH EA szerver”, az „MVH netHSM 500”, az MVH Aláíró desktop és az USB mini HSM komponensekből áll.

A tényleges aláírás kiváltása távolról történik, az aláíró egy dedikált munkaállomásról („MVH Aláíró Desktop”) aktivizálja a szerver oldali aláírást, a távoli hozzáférés sértetlenségét és

bizalmasságát pedig a „USB mini HSM” biztosítja. Maga az aláírás az MVH EA szerver közvetítésével a netHSM 500-ban valósul meg.

Az aláírandó iratok körének kiválasztása és átadása, majd az aláírt dokumentumok visszatöltése az „IIER Dokumentumtár” komponensen keresztül történik.

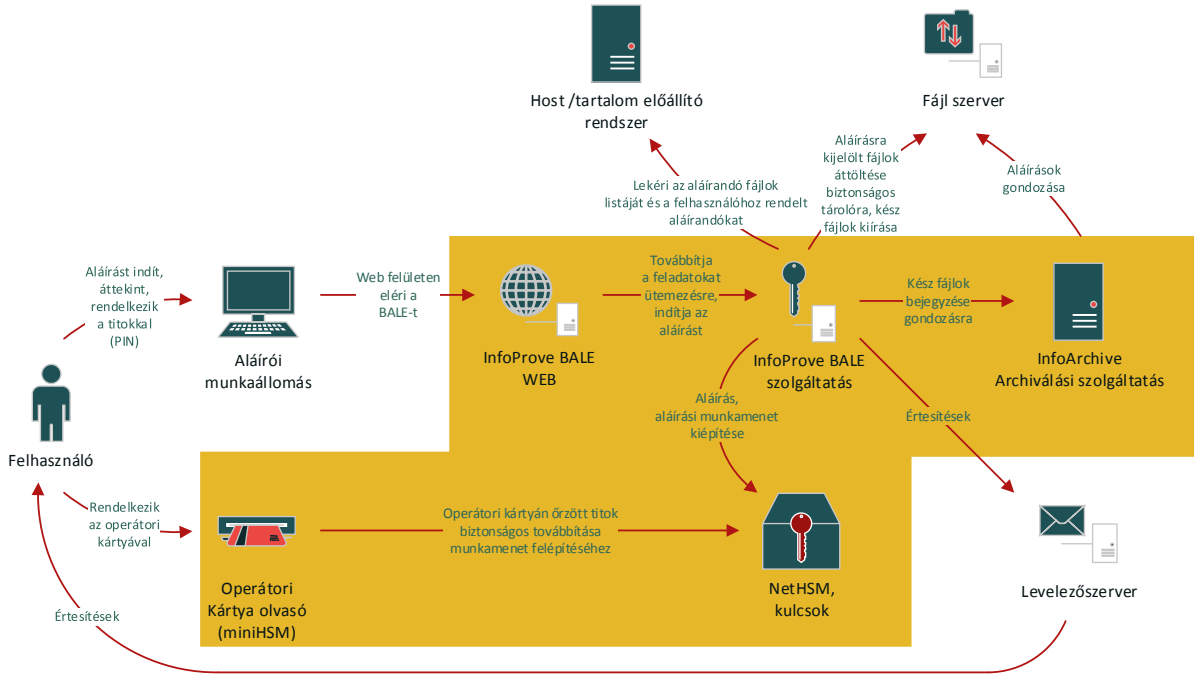
Az aláírásra kiválasztható állomány listák és az állományokhoz tartozó ellenőrző hash értékek az „Enter szerver”-ről kerülnek a rendszerbe.

Az aláíráshoz szükséges visszavonási információkat és időbélyegeket a külső „Hitelesítés szolgáltató” biztosítja.

Az „MVH levelező szerver” közvetítésével a rendszer működési hiba jelzést, biztonsági riasztást küldhet az adminisztrátornak.

Az „MVH McAfee szerver” a központi vírusellenőrző szoftverek frissítését végzi az „MVH EA szerver” és az „MVH Aláíró Desktop” komponenseken.

A 2. ábra az MVH_BALE rendszer (mint az IIER alrendszere) architektúráját részletezi:



2. ábra: Az MVH_BALE rendszer áttekintése

Az MVH_BALE rendszer az alábbi összetevőkből áll:

- aláírói munkaállomás: egy dedikált munkaállomás, ahol az aláírók áttekinthetik, kihagyhatják vagy jóváhagyhatják az aláírandó állományokat, miután behelyezték titkot tartalmazó operátori kártyájukat a munkaállomáson elhelyezett miniHSM kártya olvasójába, illetve a munkaállomáson begépelték jelszavukat,
- NetHSM: az aláírást végző BALE eszköz,
- miniHSM: az aláírói munkaállomáson telepített külön hardver eszköz, mely a NetHSM távoli hozzáféréséhez szükséges megbízható útvonalat építi ki,
- operátori kártya olvasó: az OSC miniHSM-hez kapcsolódását lehetővé tevő eszköz

- OSC (operátori kártya): az aláírói munkaállomáson az aláíró által a miniHSM kártya olvasójába illesztendő kártya, melyen az aláíróhoz rendelt egyedi magánkulcs (netHSM oldali) aktivizálásához szükséges titok egy része is elhelyezésre került.
- InfoProve BALE WEB (Frontend): felhasználói interfész a felhasználók (aláírók és az aláírói fiókokat kezelő adminisztrátorok) számára,
- InfoProve BALE szolgáltatás: a rendszer szolgáltatásait támogató alkalmazás,
- InfoArchive: az aláírt állományok archiválását végző támogató kiegészítő alkalmazás,
- InfoAuth: az aláírók hitelesítését végző kiegészítő alkalmazás (az ábrán nem szerepel).

2 A tanúsítás jellemzése

2.1 Az alkalmazott tanúsítási és értékelési módszer

Az alábbiakban az értékelés és tanúsítás során alkalmazott értékelési módszereket, technikákat és szabványokat dokumentáljuk.

MIBÉTS rendszerértékelési és tanúsítási módszertan

Az MVH_BALE rendszer műszaki szempontú értékelésére az [1]-ben és [2]-ben meghatározott, rendszerekre vonatkozó értékelési módszertant alkalmaztuk, az alábbi pontosításokkal:

- a rendszer értékelés típusa[1]: kezdeti
- a rendszer értékelés garanciaszintje[2]: MIBÉTS fokozott (SAP-F)

A rendszer értékelés keretében elvégzett fő feladat-csoportok az alábbiak voltak:

a) a rendszer biztonsági előirányzat értékelése,
b) a rendszer biztonsági architektúrájának értékelése,
c) a rendszer telepítési és üzemeltetési útmutatóinak a vizsgálata,
d) a rendszer konfiguráció vizsgálata,
e) a rendszer biztonsági tesztelése,
f) a rendszer sebezhetőség vizsgálata.

Kiegészítő értékelések

Jelen kezdeti rendszer értékelés alapvetően az nCipher Corporation Ltd. által előállított és forgalmazott nShield F3 500 for netHSM kriptográfiai hardver eszköz „3-as típusú biztonságos aláírás-létrehozó eszköz”-nek való megfelelőségét tanúsító HUNG-T-062-2013 tanúsítvány 1.-12. érvényességi feltételeinek vizsgálatára irányult. A feltételek vizsgálatára a kezdeti értékelés keretén belül, két különböző audit irányult:

- az első az MVH netHSM és miniHSM eszközök security world inicializálásának helyszíni ellenőrzése volt, mely az előkészítés szakaszára vonatkozó 1. – 8. feltételek teljesülését ellenőrizte,
- a másik pedig az aláíró szoftver oldalára vonatkozó 9. – 12 feltételek ellenőrzése, a rendszer biztonsági beállításainak helyszíni ellenőrzése során.

A tanúsítvány érvényességi feltételeinek vizsgálatán túl az értékelés kiterjedt a CWA 14170:2004 CEN munkacsoport megállapodásban (Security Requirements for Signature Creation System) meghatározott funkcionális és biztonsági követelmények teljesülésének ellenőrzésére is. Ez utóbbi vizsgálatnak a kiegészítő módszere a következő volt:
Minden követelményekre külön-külön határozat születik az alábbi lehetséges eredménnyel:

- megfelel
- nem felel meg
- nem vonatkozik rá a követelmény

Az egyes követelményekre meghozott határozatok az alábbiak alapján születhetnek:

- interjú: a fejlesztőkkel folytatott személyes konzultációk alapján,
- dokumentáció: a fejlesztők által készített írásos dokumentációk alapján,
- tapasztalat: a rendszer használata során szerzett „felhasználói” tapasztalatok alapján,
- teszt: a fejlesztők és az értékelők által végzett tesztelés eredményei alapján,

[1] A rendszer értékelés típusai: kezdeti, tervezett felülvizsgálati, rendkívüli felülvizsgálati, megismételt kezdeti.
[2] A rendszer értékelés lehetséges garanciaszintjei: MIBÉTS alap (SAP-A), MIBÉTS fokozott (SAP-F) és MIBÉTS kiemelt (SAP-K) rendszer értékelési garanciacsomag.

- forrás kód: a fejlesztők által biztosított forráskód értékelők általi elemzése alapján.

Erről a vizsgálatról egy külön megfelelés értékelési jelentés készült és ebben csak „*megfelel*” és „*nem vonatkozik rá a követelmény*” határozat született.

2.2 A tanúsításhoz felhasznált értékelési jelentések azonosítása

Rendszer értékelési jelentés:

> A Mezőgazdasági és Vidékfejlesztési Hivatal által üzemeltetett, az „nShield F3 500 for netHSM” kriptográfiai hardver eszköz aktivizálásán keresztül minősített elektronikus aláírásokat létrehozó informatikai rendszer (2013. október 17-én aktuális verziója) RENDSZER ÉRTÉKELÉSI JELENTÉS V1.0

A HUNG-T-062-2013 tanúsítvány 1.-12. érvényességi feltételeinek vizsgálatáról szóló audit jelentések:

> Audit jegyzőkönyv (az MVH netHSM és miniHSM eszközök security world inicializálásának helyszíni ellenőrzése)
>
> Audit jegyzőkönyv (az MVH netHSM BALE tanúsítvány feltételeinek és a rendszer biztonsági beállításainak helyszíni ellenőrzése)

Mértékadó követelményrendszernek való megfelelés elemzés:

> MEGFELELÉS ÉRTÉKELÉSI JELENTÉS - a Mezőgazdasági és Vidékfejlesztési Hivatal által üzemeltetett, az „nShield F3 500 for netHSM” kriptográfiai hardver eszköz aktivizálásán keresztül minősített elektronikus aláírásokat létrehozó informatikai rendszer (2013. október 17-én aktuális verziójának) megfelelése a CWA 14170:2004 követelményeinek

2.3 Az értékeléshez felhasznált fejlesztői bizonyítékok

Az értékelés, a fejlesztőkkel történt folyamatos konzultáció mellett, az alábbi fejlesztői bizonyítékok végleges verzióit használta fel:

cím	fájlnév	azonosító
Terv dokumentációk		
Rendszer biztonsági előirányzat	MVH_v1.0_rendszer_biztonsagi_eloiranyzat.doc	{1}
Rendszer architektúra áttekintés	Architektura_attekintes.doc	{2}
MVH IPR BALE - Funkcionális specifikáció	IPR BALE Funckionális specifikáció_2_7b.pdf	{3}
MVH IPR BALE - Rendszerterv	IPR BALE Rendszer Terv_1_2.pdf	{4}
Forráskód részletek	STOE_1.0.13282.131017 alkönyvtár	{5}
Útmutató dokumentációk		
Admin kézikönyv az MVH elektronikus rendszerének HSM részéhez	MVH_EA_V1_1_20130912.pdf	{11}
Adminisztrációs kézikönyv az IPR BALE rendszerhez	Adminisztrációs kézikönyv az IPR BALE szolgáltatáshoz 1.3.pdf	{12}
InfoProve BALE Felhasználói Kézikönyv	InfoProve BALE WEB - felhasznaloi kezikonyv v1.0.5	{13}
Ügyfél-tájékoztató a minősített elektronikus aláírás mezőgazdasági és vidékfejlesztési hivatal általi alkalmazásáról	Ügyféltájékoztató.docx	{14}
Az elektronikus aláírás rendszer MVHVMEA 02 szerver üzemeltetési dokumentációja	EA üzemeltetés dokumentáció.docx	{15}
Konfiguráció listák		

Konfiguráció lista – aláíró szerver SW	EA_SW.xls	{21}
Konfiguráció lista – munkaállomás SW	EDGE_SW.xls	{22}
Konfiguráció lista – 3. felek által készített SW-ek listája	Konfiglista_3party.xls	{23}
Konfiguráció lista – Inetpub és Nfast mappa tartalma	3rdparty.txt	{24}
Tesztelési dokumentációk		
Teszt jegyzőkönyv - Funkcionális tesztelés IPR BALE szolgáltatás: 1.0 (Build 13179), Frontend: 1.0 (Build 13179)	tesztjkv_20130608_SzP_20130701_2	{31}
Teszt jegyzőkönyv Az IIER interfész tesztelésének tervei Tömeges elektronikus aláírásra előkészítés	Teszt jegyzőkönyv_20130904.docx	{32}
Teszt jegyzőkönyv Az IIER interfész tesztelésének tervei Tömeges elektronikus aláírásra előkészítés	Teszt jegyzőkönyv_20130905.docx	{33}
Teszt jegyzőkönyv - Funkcionális tesztelés IPR BALE szolgáltatás: 1.0 (Build 13228), Frontend: 1.0 (Build 13252)	tesztjkv_20130608_SzP_20130909.doc	{34}
Teszt jegyzőkönyv - Funkcionális tesztelés (végleges verzió)	tesztjkv_20131011_EL.docx	{35}
Szabályzatok		
Jogosultságigénylő lap e-aláírás IIER Rendszerben	Jogosultságigénylő lap v2.0_.xls	{41}
Ügyfél-tájékoztató a minősített elektronikus aláírás MVH általi alkalmazásáról (aláírási szabályzat)	Ügyfél-tájékoztató.docx	{42}
Minta aláírt pdf	20130916_aláírt_eküldés.pdf	{43}

3 Értékelés eredményei

3.1 A rendszer biztonsági előirányzat értékelése

A *rendszer biztonsági előirányzat* (a 2.3. fejezet táblázatában az {1} egyedi azonosítóval jelzett értékelési bizonyíték) felépítése és tartalma megfelel az elvárásoknak:

A rendszer biztonsági előirányzat szakmailag helyesen, belső ellentmondásoktól mentesen levezeti a felvállalt funkcionális és biztonsági követelményeket, egyúttal magas szinten áttekinti, hogy a rendszer hogyan teljesíti ezeket.

3.2 Az értékelt rendszer biztonsági architektúrájának értékelése

A rendszer biztonsági architektúra értékelése a *terv dokumentációk* (a 2.3. fejezet táblázatában az {1}-{4} egyedi azonosítóval jelzett értékelési bizonyítékok) vizsgálatán alapult. Ezekből megállapítható, hogy az MVH_BALE rendszert úgy tervezték, hogy az az MVH nagyobb rendszerétől (IIER) a lehető legjobban elkülönüljön és funkcionalitásában a lehető legszűkebben csak a minősített elektronikus aláírást szolgálja.

A tervezési dokumentációk értékelése alapján megállapítható, hogy az MVH_BALE rendszer egy jól átgondolt, a biztonságot kitüntetett szempontként kezelt fejlesztés, illetve integrálás eredménye.

3.3 A rendszer telepítési, konfigurálási és üzemeltetési útmutatóinak a vizsgálata

Az útmutatók értékelése az *útmutató dokumentációk* (a 2.3. fejezet táblázatában a {11}-{15} egyedi azonosítóval jelzett értékelési bizonyítékok) vizsgálatán alapult.

Az útmutatók értékelésével megállapítható, hogy az MVH_BALE rendszer biztonságosan lett kialakítva és konfigurálva, valamint biztonságosan üzemeltethető.

3.4 A rendszer konfiguráció vizsgálata

A rendszer konfiguráció értékelése a *konfiguráció listák* (a 2.3. fejezet táblázatában a {21}-{24} egyedi azonosítóval jelzett értékelési bizonyítékok) vizsgálatán alapult.
A rendszer konfiguráció listája teljes, tartalmazza a rendszer valamennyi hardver és szoftver elemét, köztük a telepített programokat, a telepített szolgáltatásokat, az IIS-en futó webes alkalmazásokat, valamint a 3. felek által készített szoftver komponensek táblázatát is (ez utóbbit a fejlesztőkkel és a használt verziószámokkal).

A konfigurációs változások kezelése szabályozott:

- a netHSM és miniHSM (FIPS tanúsított termékek) verziókezelése megoldott,
- a Security World csak a tanúsító jelenlétében módosítható,
- az aláíró alkalmazásban kulcsszerepet betöltő InfoProve egy verziózott termék, amely saját hibabejelentő oldallal rendelkezik,
- az alkalmazás később feltárt hibáinak bejelentésére az InfoProve hibabejelentő oldalát használják.

3.5 A rendszer biztonsági tesztelése

A rendszer biztonsági tesztelésének értékelése a *tesztelései dokumentációk* (a 2.3. fejezet táblázatában a {31}-{35} egyedi azonosítóval jelzett értékelési bizonyítékok) vizsgálatán, valamint az értékelők által több verzióra elvégzett független tesztelés eredményein alapult.

A független tesztelés stratégiája a következő volt:

- az értékelők aktívan közreműködtek az elvégzendő tesztesetek összeállításánál,
- szimulált környezetben az összes elvégezhető tesztesetet függetlenül megismételték saját környezetükben,
- az integrátorok jelenlétében az éles rendszerben függetlenül elvégezték az összes maradék (biztonsággal és nem teljesítménnyel kapcsolatos) tesztesetet.

A rendszer tesztelése lefedettség, mélység, konzisztencia vonatkozásában megfelelő.
A biztonsági teszteléssel kapcsolatosan az alábbi állítások összegezhetők:

- Az egyes alkalmazásmodulok fejlesztői alaposan tesztelték moduljaikat.
- A rendszer integrátor tesztelte az MVH_BALE rendszer szintű működő képességét és biztonsági funkcionalitását.
- A fejlesztők és az integrátor által végzett tesztelés érintette a rendszer összes külső interfészét és összes modulját.
- Az értékelők független teszteléssel megerősítették a helyes és biztonságos működést.

3.6 A rendszer sebezhetőség vizsgálata

A sebezhetőség vizsgálat a terv dokumentációk (a 2.3. fejezet táblázatában az {1}-{5} egyedi azonosítóval jelzett értékelési bizonyítékok) vizsgálatán, a netHSM és miniHSM eszközök security world inicializálásának helyszíni ellenőrzésein, valamint a biztonsági tesztelés eredményein (2.3. fejezet táblázatában {31}-{35}) alapult.

A sebezhetőség vizsgálat kiindulópontja az volt, hogy a rendszer az MVH környezetétől leválasztásra került, kis méretű alrendszer, amely jól meghatározható interfészeken keresztül kapcsolódik a külvilághoz.

Az interfészeinek egy része szabványos, „gyári” megoldás: TSA, CRL, OCSP, vírusfrissítés. Ezeken az interfészeken keresztül tipikusan valamilyen védett adatforgalom zajlik (digitálisan aláírt üzenetek vagy védett vírus definíció), amely várhatóan még a magas szintű támadói potenciállal rendelkező támadóknak is ellenáll.

Az interfészek másik csoportja azonban az InfoProve BALE alkalmazás által implementált alkalmazási interfész. Ezeken az interfészeken mindig az InfoProve BALE alkalmazás a kezdeményező, azonban a kéréseire kapott válaszok alkalmasak lehetnek az alkalmazás hibás működésének előidézésére.

A vizsgálat során ezért alapvetően két területre fókuszáltak az értékelők. A fő terület az alkalmazás biztonsági tesztelésével összefüggésben a speciális, támadó célzattal szerkesztett interfész üzenetek bejátszása volt az alkalmazásba. A másik fő terület pedig a határvédelem és a konfiguráció helyszíni vizsgálata. A támadó üzenetek terén mind a kérés-válasz jellegű üzenetek válaszait, mind pedig a file átadó interfészen beküldött file-okat is manipuláltuk.

Az éles rendszer végleges (1.0.13282) verziójában közepes támadói potenciállal kihasználható sebezhetőséget az értékelés nem tárt fel.

3.7 Következtetések

A rendszer értékelés az alábbi fő következtetésekre jutott:

1. Az MVH_BALE rendszer teljesíti a rendszer biztonsági előirányzatában felvállalt, MIBÉTS fokozott garanciaszinthez (SAP-F) tartozó garanciális elvárásokat.

2. Az MVH_BALE rendszer kielégíti a rendszer biztonsági előirányzatában felvállalt, egyúttal a [4] CEN munkacsoport megállapodásban a minősített elektronikus aláírásokat létrehozó rendszerektől megkövetelt funkcionális és biztonsági követelményeket.

3. Az MVH_BALE rendszerben teljesülnek a netHSM-et BALE-ként elfogadott [5] tanúsítvány által az előkészítés szakaszára vonatkozó 1. – 8. feltételek.

4. Az MVH_BALE rendszerben teljesülnek a netHSM-et BALE-ként elfogadott [5] tanúsítvány által az aláíró szoftver oldalára vonatkozó 9. – 12. feltételek.

3.8 Javaslatok

Javasolt a most dokumentált kezdeti rendszer értékelés eredményeinek megerősítése, valamint a netHSM-et BALE-ként elfogadott [5] tanúsítvány által a működtetés szakaszára vonatkozó 13. – 19. feltételek teljesülésének ellenőrzése céljából egy felülvizsgálati rendszer értékelés az alábbi esetekben:

- egy év elteltével (tervezett felülvizsgálati rendszer értékeléssel),
- a rendszer architektúrájában vagy funkcionalitásában bekövetkezett változtatásokra reagálva (rendkívüli felülvizsgálati rendszer értékeléssel).

4 Javaslat a Tanúsítvány szövegezésére

4.1 Javaslat a Tanúsítvány főlapjának szövegezésére

A **HUNGUARD** Számítástechnikai-, informatikai kutató-fejlesztő és általános szolgáltató Kft. a Nemzeti Média és Hírközlési Hatóság nyilvántartásában szereplő elektronikus aláírási termékeket tanúsító szervezet és a Nemzeti Akkreditáló Testület által NAT-6-0048/2011 számon akkreditált terméktanúsító szervezet

tanúsítja,

hogy a

Mezőgazdasági és Vidékfejlesztési Hivatal (MVH).

által üzemeltetett

az „nShield F3 500 for netHSM” kriptográfiai hardver eszköz aktivizálásán keresztül minősített elektronikus aláírásokat létrehozó informatikai rendszer (MVH_BALE)

2013. október 17-én aktuális verziója (Sw: v1.0.13282)

az 1.számú mellékletben áttekintett funkcionalitással, valamint
a 2. számú melléklet feltételének figyelembe vételével
informatikai biztonsági szempontból

megfelel

a KIB 28-as Ajánlásában szereplő rendszerekre vonatkozó értékelési módszertan szerinti, MIBÉTS fokozott (SAP-F)biztonsági szintnek, valamint kielégíti a HUNG-T-62-2013 tanúsítvány 19-es feltételét.

Jelen tanúsítvány a HUNG-TJ-MIBÉTS-008-2013. számú tanúsítási jelentés alapján került kiadásra. Készült a Mezőgazdasági és Vidékfejlesztési Hivatal megbízásából.

A tanúsítvány regisztrációs száma: **HUNG-T- MIBÉTS-008-2013.**
A tanúsítás kelte: 2013. október 21.
A tanúsítvány érvényességi ideje évenkénti felülvizsgálat mellett: visszavonásig.

4.2 Javaslat a Tanúsítvány mellékleteire

Javasoljuk, hogy a Tanúsítvány mellékleteiben a következők szerepeljenek:

- Az MVH_BALE v1.0 legfontosabb tulajdonságainak összefoglalása az alábbi fejezetet alapján:

  1.2 a tanúsítás tárgya

- A tanúsítvány érvényességének feltétele az alábbi fejezet alapján

  4.8 Értékelő javaslata

- A tanúsítással és értékeléssel kapcsolatos módszertani hivatkozások az alábbi fejezet alapján:

  2.1 az alkalmazott módszertan

- A tanúsítási eljárás egyéb jellemzői
  - A tanúsításhoz figyelembe vett, fejlesztői dokumentumok
  - A tanúsításhoz figyelembe vett, fejlesztőtől független dokumentumok
  - A követelményeknek való megfelelést ellenőrzés vizsgálat garancia szintje

5 Hivatkozások

[1]: Rendszerekre vonatkozó értékelési módszertan (az „e-Közigazgatási Keretrendszer Kialakítása” projekt keretében kidolgozott dokumentum, v4 2008.09.19) http://kovetelmenytar.complex.hu (a KIB 28-as számú Ajánlás része)

[2]: Útmutató rendszer értékelőknek (az „e-Közigazgatási Keretrendszer Kialakítása” projekt keretében kidolgozott dokumentum, v3 2008.09.19) http://kovetelmenytar.complex.hu (a KIB 28-as számú Ajánlás része)

[3]: IT biztonsági műszaki követelmények a különböző biztonsági szintekre - Követelmény előírás (az „e-Közigazgatási Keretrendszer Kialakítása” projekt keretében kidolgozott dokumentum, v1.01, 2008.08.22) http://kovetelmenytar. complex.hu (a KIB 28-as számú Ajánlás része)

[4]: CWA 14170:2004: Security Requirements for Signature Creation System, May 2004

[5]: HUNG-T-062-2013 regisztrációs számú tanúsítvány (az nShield F3 500 for netHSM kriptográfiai hardver eszköz megfelelése „3-as típusú biztonságos aláírás-létrehozó eszköz”-nek)