



TANÚSÍTVÁNY

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.

Melléklet: tulajdonságok, feltételek, követelmények, egyéb jellemzők összesen 5 oldalon.

PH.

Endrődi Zsolt
Tanúsítási igazgató

Lengyel Csaba
Ügyvezető igazgató



1. számú melléklet

Az MVH_BALE v1.0 legfontosabb tulajdonságainak összefoglalása

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 hajtodik 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 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).



2. számú melléklet

A tanúsítvány érvényességének feltétele

A jelen dokumentumban tanúsított kezdeti rendszer értékelés eredményeinek megerősítése, a tanúsítvány érvényességének megtartása, valamint a netHSM-et BALE-ként elfogadó [5] tanúsítvány által a működtetés szakaszára vonatkozó 13. – 19. feltételek teljesülésének ellenőrzése céljából egy felülvizsgálati rendszer értékelést kell végrehajtani az alábbi esetekben:

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



3. számú melléklet

A tanúsítással és értékeléssel kapcsolatos módszertani 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)



4. számú melléklet

A tanúsítási eljárás egyéb jellemzői

A tanúsításhoz figyelembe vett, fejlesztői dokumentumok

Terv dokumentációk

- Rendszer biztonsági előirányzat
- Rendszer architektúra áttekintés
- MVH IPR BALE - Funkcionális specifikáció
- MVH IPR BALE - Rendszerterv
- Forráskód részletek

Útmutató dokumentációk

- Admin kézikönyv az MVH elektronikus rendszerének HSM részéhez
- Adminisztrációs kézikönyv az IPR BALE rendszerhez
- InfoProve BALE Felhasználói Kézikönyv
- Ügyfél-tájékoztató a minősített elektronikus aláírás mezőgazdasági és vidékfejlesztési hivatal általi alkalmazásáról
- Az elektronikus aláírás rendszer MVHVMEA 02 szerver üzemeltetési dokumentációja

Konfiguráció listák

- Konfiguráció lista – aláíró szerver SW
- Konfiguráció lista – munkaállomás SW
- Konfiguráció lista – 3. felek által készített SW-ek listája

Tesztelési dokumentációk

- Teszt jegyzőkönyv - Funkcionális tesztelés IPR BALE szolgáltatás: 1.0 (Build 13179), Frontend: 1.0 (Build 13179)
- Teszt jegyzőkönyv Az IIER interfész tesztelésének tervei Tömeges elektronikus aláírásra előkészítés
- Teszt jegyzőkönyv Az IIER interfész tesztelésének tervei Tömeges elektronikus aláírásra előkészítés
- Teszt jegyzőkönyv - Funkcionális tesztelés IPR BALE szolgáltatás: 1.0 (Build 13228), Frontend: 1.0 (Build 13252)
- Teszt jegyzőkönyv - Funkcionális tesztelés (végleges verzió)

Szabályzatok

- Jogosultságigénylő lap e-aláírás IIER Rendszerben
- Ügyfél-tájékoztató a minősített elektronikus aláírás MVH általi alkalmazásáról (aláírási szabályzat)
- Minta aláírt pdf

A tanúsításhoz figyelembe vett, fejlesztőktől független dokumentumok

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

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)

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

A követelményeknek való megfelelést ellenőrző független vizsgálat módszere

KIB 28 ajánlás szerinti Rendszerekre vonatkozó értékelési módszertan

Az értékelés garanciaszintje

MIBÉTS fokozott (SAP-F)