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 az

Argeon Üzleti Szolgáltató Kft.
által kifejlesztetett

mySigno for PDA and Server v1.0

fejlesztő készlet fokozott biztonságú elektronikus aláíráshoz

az 1.számú mellékletben áttekintett funkcionalitással, valamint

a 2. számú melléklet biztonságos felhasználásra vonatkozó feltételek figyelembe vételével

megfelel

a 2001. évi XXXV törvényben szereplő
fokozott biztonságú elektronikus aláírás
létrehozására és ellenőrzésére alkalmazható
szabványos és biztonságos alkalmazások fejlesztéséhez.

Jelen tanúsítvány a HUNG-TJ-032-2006. számú tanúsítási jelentés alapján került kiadásra. Készült az Argeon Üzleti Szolgáltató Kft.. megbízásából.

A tanúsítvány regisztrációs száma: **HUNG-T-032-2006.**
A tanúsítás kelte: 2006. május 29.
A tanúsítvány érvényességi ideje: 2009. május 29.
Melléklet: tulajdonságok, feltételek, követelmények, egyéb jellemzők összesen 6 oldalon.

PH.

Endrődi Zsolt
Tanúsítási igazgató

dr. Szabó István
Ügyvezető igazgató

1. számú melléklet

A mySigno v1.0 legfontosabb tulajdonságainak összefoglalása

A mySigno v1.0 egy összetett rendszerbe illeszkedő, fokozott biztonságú elektronikus aláírások létrehozására és ellenőrzésére alkalmas függvénykönyvtár. Kliens és szerver oldali összetevőkkel rendelkezik.

A mySigno v1.0 egy olyan komplex informatikai rendszerbe illeszkedik, mely az elektronikus aláírások létrehozásán és ellenőrzésén kívül számos egyéb funkcionalitással is rendelkezik (kliens oldalon: összetett XML csomagok összeállítása, kézi aláírás elhelyezése, szervert oldalon: aláírt csomagok archiválása, adatbázisba szervezése, ..)

A mySigno v1.0 által kezelt szerepkörök:

- **Ügynök:** Az a szereplő, aki a csomagot a saját digitális aláírásával ellátja, integritását ezzel biztosítva.
- **Ellenőrző fél:** A szerver oldali automatikus ellenőrző folyamat tölti be ezt a szerepet.

A mySigno v1.0 hatáskörén kívüli, de a biztonságos működéssel összefüggésben lévő szerepkörök:

- **Szerver adminisztrátor:** Aki a mySigno szerver karbantartását és beállításait jogosult végezni.
- **PDA adminisztrátor:** Aki a mySigno PDA modul telepítésével, a paraméter fájlok, kulcsok biztonságos PDA-ra juttatásával kapcsolatos feladatokat végzi.

A mySigno v1.0 biztonsági funkciói programozói API-n keresztül elérhető DLL-ben megvalósított alkalmazás komponensben kerülnek megvalósításra, kliens oldali fokozott biztonságú aláíró, és ennek szerver oldali ellenőrzését lehetővé tevő funkcionalitással.

A fokozott biztonságú elektronikus aláírás az SHA-1 lenyomatoló és az RSA digitális aláíró algoritmust használja, 1024 bites kulcshosszal. Az aláírás létrehozó környezetben a magánkulcs tárolása PKCS#12 tanúsítványban történik.

A mySigno v1.0 PDA oldalon interfészt biztosít az elektronikus-aláírást létrehozó, szerver oldalon pedig az automatikus ellenőrző folyamatok számára.

2. számú melléklet

A biztonságos felhasználás feltételei

Feltételezések az mySigno v1.0 informatikai környezetére

Az alábbi (a biztonsági előirányzatban is szereplő) feltételezések az informatikai környezetre vonatkoznak:

1. A mySigno v1.0 biztonságos működéséhez szükséges kulcsokat és a mySigno v1.0 biztonsági funkcióit biztonságos módon telepítetik a PDA eszközre (A.Init_PDA).
2. A PDA eszközt elektronikus aláírás létrehozására csak feltöltött akkumulátorral használják az adatvesztés elkerülése érdekében (A.PDA_Physical_Security).
3. Feltételezzük, hogy a PDA kliens kizárólag a regisztrált ügynök felügyelete alatt marad. Az eszközt az ügynök felügyelete nélkül más személynek átadni tilos. (A.Signer_Only).
4. A mySigno PDA klienst futtató PDA közvetlenül az aláíró befolyása és a rendszert működtető szervezet felügyelete alatt áll (A.Host_PDA_Machine).
5. Az aláírás létrehozását és ellenőrzését végző informatikai környezetben a mySigno folyamatai védettek más folyamatok káros beavatkozásai ellen. A mySigno v1.0 modult csak egy hívó alkalmazás tölti be egy időben (A.Separation_and_Exclusion)
6. .A PDA modul tárolására szolgáló könyvtár tartalmát a kliens eszköz felhasználója nem módosítja (A.AccessControl).
7. A mySigno biztonsági adminisztrátora megbízható, képzett és rendelkezik a feladatai ellátáshoz szükséges hozzáférésekkel és jogosultságokkal (Trusted_Security_Administrator).
8. A biztonsági adminisztrátor vagy a mySigno v1.0-t hívó alkalmazás számára eszköz áll rendelkezésre, amellyel ellenőrizhető a mySigno szolgáltatásainak és paramétereinek a sértetlensége (A.Services_Integrity).
9. Az aláíró ügynök végig jelen van attól kezdődően, hogy kifejezte aláírási szándékát, addig, amíg megadja a magánkulcs aktiválásához szükséges hitelesítő adatát (A.Signatory_Presence).
10. Feltételezzük, hogy a PDA eszköz tartalmaz olyan külső megjelenítő alkalmazásokat, melyek képesek a csomagba foglalható formátumok (melyeket az aláírási szabályzat határoz meg) mindegyikének a megjelenítésére. Az aláírás létrehozó PDA kliens és az aláírás ellenőrző felet jelentő szerver alkalmazás IT környezete pontosan ugyanazon formátumokat ismeri és tudja megjeleníteni, illetve ezen külső alkalmazások a két oldalon egyforma konfigurációs beállításokkal működnek. Ezen külső alkalmazások kívül esnek a TOE hatáskörén (A.Packet_Viewers).
11. Az aláírás ellenőrzését végző szerver fizikailag védett a külső támadók közvetlen támadásai ellen (A.Physical_Security).
12. A mySigno v1.0 szerver oldali modult futtató gazdaszámítógép közvetlenül az ellenőrző (természetes vagy jogi személy) befolyása és felügyelete alatt áll, ami garantálja, hogy a biztonsági intézkedéseket megfelelően alkalmazzák (A.Host_Server_Machine).

13. A mySigno v1.0 szerver oldali modul hozzáféréssel rendelkezik az aláírás ellenőrzéséhez szükséges összes érvényesítő adathoz (A.Access_to_Validation_Data).

A biztonságos felhasználás egyéb feltételei

1. A mySigno v1.0 kriptográfiai modul az önkibocsátott (self issued) tanúsítványokat nem támogatja. Nem támogatja azon tanúsítványláncok ellenőrzését sem, ahol a CRL-t más tanúsítvánnyal ellenőrzik, mint a végfelhasználó tanúsítványokat. A tanúsítványlánc felépítésekor a kibocsájtó-tulajdonos egyezőséget binárisan ellenőrzi. Ezért csak olyan környezetben szabad alkalmazni, ahol önkibocsátott (self issued) tanúsítvány a tanúsítványláncba nem fordul elő, a CRL-t és a végfelhasználói tanúsítványt ugyanazzal a CA tanúsítvánnyal kell ellenőrizni, valamint a tanúsítványláncban a kibocsájtó-tulajdonos név egyezőség bináris.
2. A mySigno v1.0-át használó aláíró alkalmazás működtetési környezetében technikai és eljárásrendi intézkedéseket kell tenni annak biztosítására, hogy az aláírási folyamatba ne avatkozhassanak be olyan nem megbízható rendszer és alkalmazási folyamatok, perifériák és kommunikációs csatornák, amelyek nem szükségesek az aláírás-létrehozás alkalmazás működéséhez.
3. A mySigno v1.0 programozói könyvtár működtetési környezetében technikai és eljárásrendi intézkedéseket kell tenni az alábbiak biztosítására:
    a. vírusok ne ronthassák el az aláíró alkalmazást és az általa meghívott egyéb aláíró összetevőket, valamint
    b. az esetlegesen vírussal fertőzött aláíró összetevőket megfelelően helyre lehessen állítani.
4. Az mySigno v1.0 programozói könyvtár működtetési környezetében technikai és eljárásrendi intézkedéseket kell tenni annak biztosítására, hogy megvédjék a mySigno v1.0 programozói könyvtár funkcionális összetevőinek sértetlenségét, megakadályozva, hogy behatolók elrontsák azt.
5. A mySigno v1.0 programozói könyvtár működtetési környezetében technikai és eljárásrendi intézkedéseket kell tenni annak biztosítására, hogy az mySigno v1.0 programozói könyvtárat, valamint valamennyi az aláírás-létrehozás, aláírás-ellenőrzés folyamatokkal kölcsönhatásba lépő összetevőjét egy biztonságos területen valósítsák meg.

3. számú melléklet

Termékmegfelelőségi követelmények

Követelményeket és szabványokat tartalmazó dokumentumok

Követelmények

Az elektronikus aláírásról szóló 2001. Évi XXXV.törvény

CEN CWA 14170:2004 munkacsoport egyezmény: Security Requirements fro Signature Creation System

CEN CWA 14171:2004 munkacsoport egyezmény: General guidelines for electronic signature verification

CEN CWA 14172-4:2001 munkacsoport egyezmény: Signature-creation application and general gudelines for electronic signature verification

ETSI TS 101 733 v1.6.3 CMS Advanced Electronic Signatures (CAdES)

ETSI TS 101 862 v1.3.3 Qualified Certificate profile

ETSI SR 002 176-1 v1.2.1 Electronic Signatures and Infrastructures (ESI) Algorithms and Parameters for Secure Electronic Signatures Part 1: Hash functions and asymmetric algorithms

ETSI TS 101 903 v1.2.2 XML Advanced Electronic Signatures (XAdES)

Szabványok

RSA Rivest-Shamir-Adleman (public key cryptosystem) /ANSI X9.31/

SHA-1 Secure Hash Algorithm /FIPS PUB 180-1/

RFC3161 Time-Stamp Protocol (TSP)

RFC3275 XML Digital Signatures (XMLDSig)

RFC3280 Certificate and Certificate Revocation List (CRL) Profile

PKCS#1 RSA Cryptographic Standard /RFC2313/

PKCS #11 v2.11: Cryptographic Token Interface Standard

PKCS #12 v1.0 Personal Information Exchange Information Standard

4. számú melléklet

A tanúsítási eljárás egyéb jellemzői

A tanúsításhoz figyelembe vett, fejlesztői dokumentumok

- Kérelem a tanúsítás elvégzéséhez
- Biztonsági előirányzat v1.0
- Aláírási szabályzat v1.0
- Funkcionális specifikáció v1.0
- Magas szintű terv v1.0
- Megfeleltetés elemzések v1.0
- Tesztelési dokumentáció v1.0
- Teszt lefedettség elemzés v1.0
- Teszt mélység elemzés v1.0
- Adminisztrátori útmutató v1.0
- A konfiguráció menedzselés dokumentációja v1.0
- A fejlesztési biztonság dokumentációja v1.0
- Az útmutatók helytelen használhatóságának elemzése v1.0
- Biztonsági funkcióerősség elemzés v1.0
- Sebezhetőség elemzés v1.0

A tanúsításhoz figyelembe vett, fejlesztőktől független dokumentumok

- Értékelési jelentés az mySigno for PDA és mySigno Server elektronikus aláíró rendszerről v1.0 (Készítette HunGuard Kft.)

A követelményeknek való megfelelést ellenőrző független vizsgálat módszere

Az mySigno v1.0 értékelése az informatikai termékek technológia szempontú értékelésére szolgáló Magyar Informatikai Biztonsági és Értékelési Séma /MIBÉTS/ módszertanát követte. A MIBÉTS séma az informatikai termékek és rendszerek biztonsági értékelésére a Közös szempontrendszer (MSZ ISO/IEC 15408:2002) elveit, fogalmait és követelményrendszerét tekinti meghatározónak.

Az értékelés garanciaszintje

fokozott (EAL3)

Az értékeléshez felhasznált módszertani anyagok

- 1. számú MIBÉTS kiadvány: A MIBÉTS nemzeti séma általános modellezése /0.95 verzió, 2005 február/,
- 2. számú MIBÉTS kiadvány: Az értékelés és a tanúsítás folyamatai /0.95 verzió, 2005 február/,
- 3. számú MIBÉTS kiadvány: Az értékelés módszertana 1 - A biztonsági előirányzat értékelésének módszertana /0.95 verzió, 2005 február/,
- 3. számú MIBÉTS kiadvány: Az értékelés módszertana 3- A fokozott garanciaszint értékelésének módszertana /0.95 verzió, 2005 február/.