TANÚSÍTVÁNY

A **HUNGUARD** Számítástechnikai-, informatikai kutató-fejlesztő és általános szolgáltató Kft. a 9/2005. (VII.21.) IHM rendelet alapján, mint a Magyar Köztársaság Gazdasági és Közlekedési Miniszterének 113/2007 számú kijelölési okiratával kijelölt tanúsító szervezet

tanúsítja,

hogy az

InfoScope Kft.
által kifejlesztett

InfoCA megbízható rendszer hitelesítés-szolgáltatáshoz v2.5

megnevezésű termék az 1.számú mellékletben áttekintett funkcionalitással, valamint

a 2. számú melléklet biztonságos felhasználásra vonatkozó feltételeinek figyelembe vételével

megfelel

a 2001. évi XXXV. törvényben szereplő minősített hitelesítés-szolgáltató és nem minősített hitelesítés szolgáltató megbízható rendszerében működő alkalmazáshoz.

Jelen tanúsítvány a HUNG-TJ-048-2009. számú tanúsítási jelentés alapján került kiadásra.
Készült a MÁV INFORMATIKA Zrt. megbízásából.

A tanúsítvány regisztrációs száma: **HUNG-T-048-2009.**
A tanúsítás kelte: 2009. augusztus 19.
A tanúsítvány érvényességi ideje: 2012. augusztus 19.
Melléklet: tulajdonságok, feltételek, követelmények, egyéb jellemzők, összesen 7 oldalon.

PH.

Endrődi Zsolt
Tanúsítási igazgató

dr. Szabó István
Ügyvezető igazgató

1. számú melléklet

Az InfoCA v2.5 legfontosabb tulajdonságainak összefoglalása

Az InfoCA megbízható rendszer hitelesítés-szolgáltatáshoz v2.5 (a továbbiakban InfoCA rendszer) egy olyan speciális elektronikus aláírási termék, amely különböző hitelesítés-szolgáltatást biztosító funkciókkal rendelkezik.

Az InfoCA rendszer az alábbi hitelesítés-szolgáltatásokat támogatja:

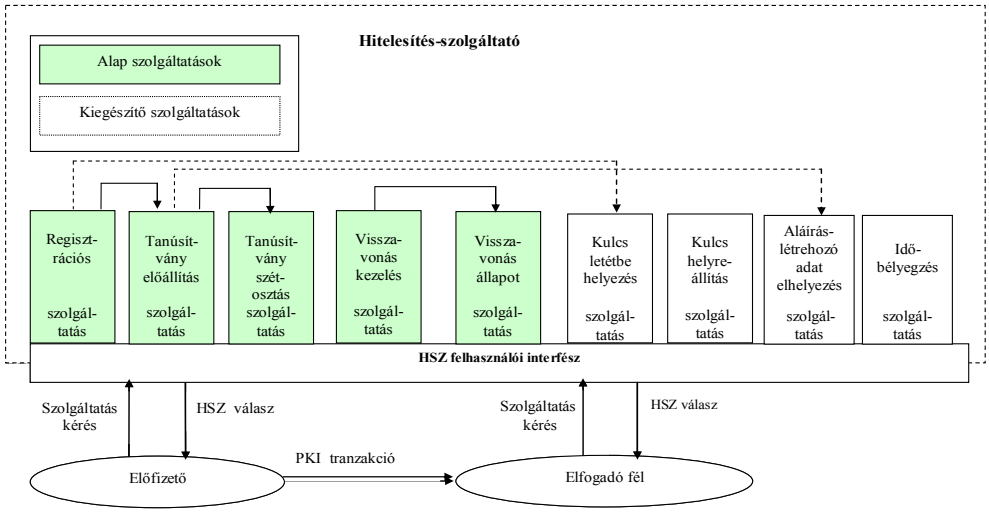
Alap (kötelező) szolgáltatások:

- Regisztrációs szolgáltatás (az InfoCA rendszeren kívül valósul meg, de eredményét az InfoCA rendszer használja)
- Tanúsítvány előállítás szolgáltatás,
- Tanúsítvány szétosztás szolgáltatás,
- Visszavonás kezelés szolgáltatás,
- Visszavonás állapot szolgáltatás (CRL, OCSP).

Kiegészítő (opcionális) szolgáltatások:

- titkosító magánkulcs letétbe helyezése szolgáltatás,
- titkosító magánkulcs helyreállítása szolgáltatás,
- aláírás-létrehozó eszközön az aláírás-létrehozó adat elhelyezése szolgáltatás (az InfoCA rendszeren kívül valósul meg),
- időbélyegzés szolgáltatás.

Az InfoCA rendszer alapvetően egy hitesítés-szolgáltató megbízható rendszerének lett tervezve, mely a hitesítés-szolgáltató által nyújtott (alap és kiegészítő) szolgáltatásokat valósítja meg, vagy nyújt a megvalósításhoz műszaki támogatást, ahogyan azt az 1. ábra szemlélteti. /Az ábrán jelzett regisztrációs, valamint aláírás-létrehozó eszközön az aláírás-létrehozó adat elhelyezése szolgáltatást az InfoCA rendszer környezete valósítja meg./



1. ábra Az InfoCA v2.5 általános felépítése

2. számú melléklet

A biztonságos felhasználás feltételei

Feltételezések az InfoCA v2.5 informatikai környezetére

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

Személyi feltételek

1. A biztonság-kritikus eseményekről naplóbejegyzés készül, s ezeket a rendszervizsgáló átvizsgálja. (A.Auditors Review Audit Logs)
2. Az InfoCA működési környezetében érvényben van egy olyan hitelesítési adat (jelszó és PIN kód) kezelésre vonatkozó szabályzat, melynek betartásával a felhasználók hitelesítési adataikat megfelelő időközönként, és megfelelő értékekre (azaz megfelelő hosszúsággal, előtörténettel, változatossággal stb. rendelkező értékekre) változtatják. (A.Authentication Data Management)
3. Szakértő rendszeradminisztrátorok, rendszerüzemeltetők, tisztviselők és rendszervizsgálók vannak kijelölve az InfoCA és az általa tartalmazott információk biztonságának kezelésére. (A.Competent Administrators, Operators, Officers and Auditors)
4. Minden rendszeradminisztrátor, rendszerüzemeltető, tisztviselő és rendszervizsgáló jól ismeri azt a hitelesítési rendet (CP) és szolgáltatási szabályzatot (CPS), mely alatt az InfoCA-t működtetik. (A.CPS)
5. A hitelesítési adatokat és az ezekhez tartozó jogosultságokat eltávolítják, miután a hozzáférési jogosultság megszűnt (pl. munkahely vagy munkakör változás következtében). (A.Disposal of Authentication Data)
6. Az InfoCA számára küldött rosszindulatú futtatható kódot nem írja alá egy megbízható entitás. (A.Malicious Code Not Signed)
7. A rendszeradminisztrátoroknak, a rendszerüzemeltetőknek, a tisztviselőknek, a rendszervizsgálóknak és az egyéb felhasználóknak értesíteniük kell a megfelelő vezetőket az InfoCA rendszert érintő bármely biztonsági eseményről, a további adatvesztés vagy kompromittálódás lehetőségének minimalizálása érdekében. (A.Notify Authorities of Security Issues)
8. Az általános felhasználók, a rendszeradminisztrátorok, a rendszerüzemeltetők, a tisztviselők és a rendszervizsgálók képzettek a "social engineering" típusú támadások megakadályozási technikáiban. (A.Social Engineering Training)
9. A felhasználóknak néhány olyan feladatot vagy feladatcsoportot is végre kell hajtani, amelyek biztonságos IT környezetet igényelnek. A felhasználóknak az InfoCA által kezelt információk közül legalább néhányhoz hozzá kell férniük, egyúttal feltételezzük, hogy a felhasználók együttműködő módon tevékenykednek. (A.Cooperative Users)

Kapcsolódási feltételek

10. Az operációs rendszer úgy kerül kiválasztásra, hogy az rendelkezik az InfoCA által elvárt azon funkciókkal, melyek a biztonsági előirányzat 3.3 alfejezetében meghatározott fenyegetések kivédéséhez szükségesek. (A.Operating System)

Fizikai feltételek

11. Az InfoCA rendszer megfelelő fizikai védelemmel van ellátva a kommunikáció elvesztésével, azaz a kommunikáció rendelkezésre állásának elvesztésével szemben. (A.Communication Protection)
12. Az InfoCA azon hardver, szoftver és förmver elemei, amelyek létfontosságúak a TOE (Target of Evaluation, az értékelés tárgya) biztonsági politikája (TSP, TOE Security Policy) érvényre juttatásához, védve vannak a jogosulatlan fizikai módosításokkal szemben. (A.Physical Protection)

A biztonságos felhasználás egyéb feltételei

1. Az InfoCA rendszer éles használata kizárólag a HSM modul támogatására építő üzemmódra szorítkozhat, a szoftveres üzemmód csak tesztelési célokat szolgál.
2. Az IT környezet biztosítsa és kezelje a rendszeradminisztrátor (SSO, SO), a rendszerüzemeltető (RO) és rendszervizsgáló szerepköröket.
3. Az IT környezet (operációs rendszer) biztosítsa a saját és külső felhasználóknak kinyomtatott PIN kódok, mint érzékeny maradvány információk védelmét.
4. Az IT környezet biztosítsa a megfelelő HSM modul használatát, illetve a HSM modul tanúsításakor meghatározott felhasználási feltételek betartását.
5. Az IT környezet biztosítsa a tanúsítvány helyességének garantálása céljából a gyökértanúsítvány lenyomatának ellenőrizhetőségét egy megbízható útvonalon biztosított információ megadásával.
6. Az InfoCA rendszer használata során biztosítani kell a megfelelő tanúsítvány profilok kizárólagos használatát.
7. Elektronikus aláíró tanúsítványt kiadó megbízható rendszer esetén az aláíró tanúsítvány profilokban a kulcsletétbe helyezés funkciót tiltani kell.
8. Az IT környezet biztosítsa az InfoCA rendszer futtatható állományainak sértetlenségét.
9. Minősített elektronikus aláíró tanúsítványt kiadó megbízható rendszer esetén az InfoCA rendszert az ExitConfig.dll (noreq) verziójával kell telepíteni.
10. A naplózás tárolási hibája miatt végzett tevékenységek naplózása érdekében IT és nem IT eljárásokat kell foganatosítani.
11. A napló események digitális aláírásának az ellenőrzését (vagyis a napló sértetlenségének igazolását) az IT környezetnek kell biztosítania.
12. Az IT környezet biztosítsa az RA és CA alrendszerek között cserélt információk bizalmasságát.
13. A megújítandó tanúsítványok érvényességét IT és nem IT eljárásokkal biztosítani kell.
14. Az IT környezet biztosítson az OCSP alrendszer és a CA alrendszer között megbízható csatornát és garantálja, hogy az OCSP alrendszer az adott tanúsítvány aktuális állapotával válaszol.
15. Időszakonként az InfoCA rendszerben alkalmazott algoritmusokról ellenőrizni kell, hogy azok megfelelnek-e a "Biztonságos algoritmusok[1]" című dokumentumban meghatározott követelményeknek.

[1] Lásd 3. mellékletet: ETSI SR 002 176-1 v2.0.0

16. IT és nem IT eljárásokat kell foganatosítani az alábbi követelmények teljesüléséhez:
[M1.4] QCA ;[SO2.1]; [SO2.2]; [SO2.3] ;[SO3.1] QCA; [SO3.1] NQCA; [IA2.2] QCA; [SA1.2]; [KM1.2]; [KM1.3]; [KM1.4]; [KM1.7]; [KM2.4]; [KM2.6]; [KM3.1]; [KM3.2] QCA; [KM4.1]; [KM4.2]; [KM5.1; [KM5.2]; [KM5.3]; [KM5.4]; [KM6.1]; [KM6.2]; [KM6.3]; [KM6.4]; [KM6.5]; [KM6.6]; [AA2.1]; [AA2.2]; [AA4.1]; [AA4.2]; [AA5.1]; [AA6.1]; [AA8.1]; [AR1.1]; [AR1.2]; [AR1.3]; [AR1.4]; [AR2.1]; [AR3.1]; [BK1.1]; [BK1.2]; [BK1.3]; [BK2.1] NQCA; [BK2.1] QCA; [BK2.2]; [BK3.1]; [BK3.2]; [R1.1]; [R1.2]; [R1.3] QCA; [R1.4]; [R1.5] QCA; [R1.6]; [R2.1]; [R3.1]; [CG1.2]; [CG1.3]; [CG2.1]; [CG2.2]; [CG2.3]; [CG2.4]; [CG3.1]; [D1.1]; [D1.2]; [D2.1]; [RM1.1]; [RM1.4]; [RM1.5]; [RM2.1]; [RS2.2], [TS1.1], [TS2.1], [TS2.2], [TS4.2], [TS4.3], [TS4.4], [TS4.6], [TS6.1], [SP1.1]; [SP1.3]; [SP1.4]; [SP1.5]; [SP1.6]; [SP1.7]; [SP2.1]; [SP3.1]; [SP3.2]

3. számú melléklet

Termékmegfelelőségi követelmények

Követelményeket és szabványokat tartalmazó dokumentumok

Követelmények

Az elektronikus aláírásról szóló 2001. évi XXXV.törvény

CEN CWA 14167-1:2003 – Security Requirements for Trustworthy Systems Managing Certificates for Electronic Signatures - Part 1: System Security Requirements

MSZ CWA 14167-1:2006 - Elektronikus aláírások tanúsítványait kezelő megbízható rendszerek biztonsági követelményei - 1. rész: Rendszerbiztonsági követelmények

ETSI TS 101 862 v1.3.3 Qualified Certificate profile

ETSI SR 002 176-1 v2.0.0 Electronic Signatures and Infrastructures (ESI) Algorithms and Parameters for Secure Electronic Signatures Part 1: Hash functions and asymmetric algorithms

Szabványok

RFC 2560: X.509 Internet Public Key Infrastructure - Online Certificate Status Protocol

RFC 3161 X.509 Internet Public Key Infrastructure - Time-Stamp Protocol

RFC 5280: X.509 Internet Public Key Infrastructure - Certificate and CRL Profile

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

- InfoCA v2.5 megbízható rendszer hitelesítés-szolgáltatáshoz - Biztonsági előirányzat-v1.1
- Telepítési kézikönyv v1.8 – InfoCA hitelesítés-szolgáltatás szoftver, v2.5
- Adminisztrátori kézikönyv v1.11– InfoCA hitelesítés-szolgáltatás szoftver, v2.5
- RA kézikönyv v1.0 – Trust&CA hitelesítés-szolgáltatás szoftver v2.0 (nem változott az előző értékeléshez képest)
- InfoCA v2.5 megbízható rendszer hitelesítés-szolgáltatáshoz - Funkcionális specifikáció-v1.1
- InfoCA v2.5 megbízható rendszer hitelesítés-szolgáltatáshoz - Magas szintű terv-v1.1
- InfoCA v2.5 megbízható rendszer hitelesítés-szolgáltatáshoz - Alacsony szintű terv-v1.1
- InfoCA v2.5 megbízható rendszer hitelesítés-szolgáltatáshoz - Megfelelés elemzés-v1.1
- InfoCA v2.5 megbízható rendszer hitelesítés-szolgáltatáshoz - Biztonsági szabályzat modell-v1.1
- InfoCA v2.5 megbízható rendszer hitelesítés-szolgáltatáshoz – A konfiguráció menedzselés dokumentációja -v1.2
- InfoCA v2.5 megbízható rendszer hitelesítés-szolgáltatáshoz - A fejlesztési biztonság dokumentációja-v1.1
- InfoCA v2.5 megbízható rendszer hitelesítés-szolgáltatáshoz - A fejlesztő eszközök dokumentációja-v1.1
- InfoCA v2.5 megbízható rendszer hitelesítés-szolgáltatáshoz - Az életciklust meghatározó dokumentáció-v1.1
- InfoCA v2.5 megbízható rendszer hitelesítés-szolgáltatáshoz - A hibajelentési eljárások -v1.1
- Tesztelési dokumentáció (tesztelési jegyzőkönyvek): TJ_090511_OCSP.rtf (OCSP, szoftveres); TJ_090609_OCSP.rtf (OCSP, Luna HSM-mel); TJ_090710_OCSP.rtf (OCSP, nShield HSM-mel); TJ_090511_TSS.rtf (TimeStamp, szoftveres); TJ_090526_TSS.rtf (TimeStamp, Luna HSM-mel); TJ_090710_TSS.rtf (TimeStamp, nShield HSM-mel)-
- InfoCA v2.5 megbízható rendszer hitelesítés-szolgáltatáshoz - Teszt lefedettség elemzés-v1.1
- InfoCA v2.5 megbízható rendszer hitelesítés-szolgáltatáshoz - Teszt mélység elemzés-v1.1
- InfoCA v2.5 megbízható rendszer hitelesítés-szolgáltatáshoz - Az útmutatók elemzése -v1.1
- InfoCA v2.5 megbízható rendszer hitelesítés-szolgáltatáshoz - Sebezhetőség elemzés -v1.1
- Biztonsági funkcióerősség elemzés-v1.0 – Trust&CA hitelesítés-szolgáltatás szoftver v2.0 (nem változott az előző értékeléshez képest)

A tanúsításhoz figyelembe vett, fejlesztőktől független dokumentumok

Értékelési jelentés - InfoCA v2.5 megbízható rendszer hitelesítés-szolgáltatáshoz v1.1 (Készítette Hunguard Kft.)

A követelményeknek való megfelelést ellenőrző független vizsgálat módszere

Az InfoCA v2.5 rendszer a CEM (Common Evaluation Methodology) v2.3 módszertana szerint került független értékelésre és tanúsításra.

Az értékelés garanciaszintje

EAL4+ (ALC_FLR.2 hibajelentési eljárásokkal kibővítve)

Az értékeléshez felhasznált módszertani anyagok

- MSZ/ISO/IEC 15408:2003 Informatika – Biztonságtechnika - Az informatikai biztonságértékelés közös szempontjai
- Common Criteria for Information Technology Security Evaluation (CC) Part 1: Introduction and general model - Version 2.3, August 2005
- Common Criteria for Information Technology Security Evaluation (CC) Part 2: Security functional requirements - Version 2.3, August 2005
- Common Criteria for Information Technology Security Evaluation (CC) Part 3: Security assurance requirements - Version 2.3, August 2005
- Common Methodology for Information Security Evaluation (CEM), Version 2.3, August 2005