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 a

ProfiTrade 90 Kft. és InfoScope Kft.
által kifejlesztett

TRUST&CA megbízható rendszer hitelesítés-szolgáltatáshoz v2.0

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-036-2007. számú tanúsítási jelentés alapján került kiadásra.
Készült a MÁV INFORMATIKA Kft. megbízásából.

A tanúsítvány regisztrációs száma: **HUNG-T-036-2007.**
A tanúsítás kelte: 2007. július 24.
A tanúsítvány érvényességi ideje: 2010. július 24.
Melléklet: tulajdonságok, feltételek, követelmények, egyéb jellemzők, összesen 6 oldalon.

PH
HunGuard Kft.
1123 Budapest, Kékgolyó u. 6.
Adószám: 10398221-2-43

Endrődi Zsolt
Tanúsítási igazgató

dr. Szabó István
Ügyvezető igazgató

1. számú melléklet

A TCA v2.0 legfontosabb tulajdonságainak összefoglalása

A TRUST&CA megbízható rendszer hitelesítés-szolgáltatáshoz v2.0 (a továbbiakban TCA rendszer) egy olyan speciális elektronikus aláírási termék, amely különböző hitelesítés-szolgáltatást biztosító funkciókkal rendelkezik.

A TCA rendszer az alábbi hitelesítés-szolgáltatásokat támogatja:

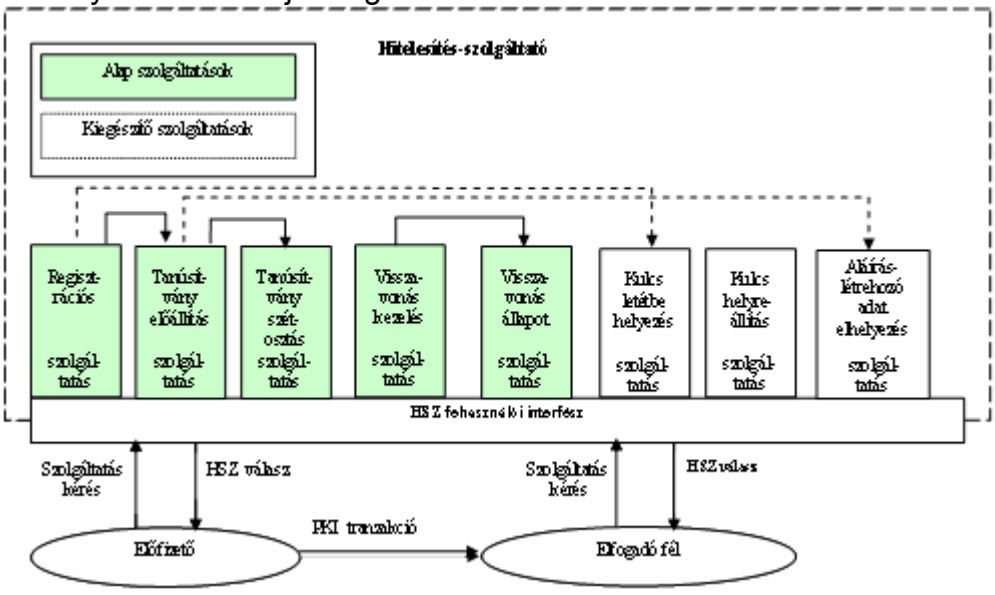
Alap (kötelező) szolgáltatások:

- regisztrációs szolgáltatás (a TCA rendszeren kívül valósul meg, eredményét a TCA rendszer használja),
- tanúsítvány előállítás szolgáltatás (funkciók: kezdeti tanúsítvány előállítás, tanúsítvány megújítás, tanúsítvány módosítás), mely szabványos X.509 formátumú tanúsítványokat állít elő,
- tanúsítvány szétosztás szolgáltatás (funkciók: tanúsítvány exportálás LDAP-ba, LDAP újraépítése adatbázisból),
- visszavonás kezelés szolgáltatás (funkciók: tanúsítvány visszavonás, tanúsítvány felfüggesztés, tanúsítvány újra érvényesítés),
- visszavonás állapot szolgáltatás (funkciók: CRL publikálása LDAP-ba, CRL exportálása állományba).

Kiegészítő (opcionális) szolgáltatások:

- aláírás-létrehozó eszközön az aláírás-létrehozó adat elhelyezése szolgáltatás (funkciók: kulcspár generáltatás, nyilvános kulcs import, tanúsítvány export).
- titkosító magánkulcs letétbe helyezése szolgáltatás (funkció: letétbe helyezés),
- titkosító magánkulcs helyreállítása szolgáltatás (funkció: helyreállítás funkció).

A TCA 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 szolgáltatást a TCA rendszer környezete valósítja meg./



1. ábra A TCA v2.0 általános felépítése

2. számú melléklet

A biztonságos felhasználás feltételei

Feltételezések a TCA v2.0 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. A TOE 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 a TOE 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 a TOE-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. A TOE 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 a 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 a TOE 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 a TOE által elvárt azon funkciókkal, melyek a biztonsági előirányzat 3.3 alfejezetében meghatározott fenyegetések kivédéséhez szükségesek. (A.Operating System)

Fizikai feltételek

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

A biztonságos felhasználás egyéb feltételei

1. A TCA rendszer éles használata kizárólag a HSM modul támogatására építő üzemmódra szorítkozhat, a szoftveres üzemmód kizárólag tesztelési célokat szolgál.
2. Az IT környezet biztosítsa és kezelje a rendszeradminisztrátor, a rendszerüzemeltető 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.
5. Az IT környezet biztosítsa a tanúsítvány helyességének garantálása céljából a gyökértanúsítvány lenyomatának ellenőrizhetőségét egy megbízható útvonalon biztosított információ megadásával.
6. A TCA rendszer használata során biztosítani kell a megfelelő tanúsítvány profilok kizárólagos használatát.
7. Elektronikus aláíró tanúsítványt kiadó megbízható rendszer esetén az aláíró tanúsítvány profilokban a kulcs letétbe helyezés funkciót tiltani kell.
8. A TCA rendszer futtatható állományainak sértetlenségét az IT környezetnek biztosítani kell.
9. Minősített elektronikus aláíró tanúsítványt kiadó megbízható rendszer esetén a TCA 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 RA és CA alrendszerek között cserélt információk bizalmasságát az IT környezet biztosítsa.
13. A megújítandó tanúsítványok érvényességét IT és nem IT eljárásokkal biztosítani kell.
14. IT és nem IT eljárásokat kell foganatosítani az alábbi CWA-14167-1 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]; [CG3.1]; [D1.1]; [D1.2]; [D2.1]; [RM1.1]; [RM1.4]; [RM1.5]; [RM2.1]; [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 Trusthworthy 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 v1.2.1 Electronic Signatures and Infrastructures (ESI) Algorithms and Parameters for Secure Electronic Signatures Part 1: Hash functions and asymmetric algorithms

Szabványok

RFC3280 Certificate and Certificate Revocation List (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

- TRUST&CA v2.0 megbízható rendszer hitelesítés-szolgáltatáshoz - Biztonsági előirányzat v1.0
- A konfiguráció menedzselés dokumentációja -Trust&CA hitelesítés-szolgáltatás szoftver v2.0 -v1.0
- Telepítési kézikönyv – Trust&CA hitelesítés-szolgáltatás szoftver v2.0 - v1.0
- TRUST&CA v2.0 megbízható rendszer hitelesítés-szolgáltatáshoz - Funkcionális specifikáció - v1.0
- TRUST&CA v2.0 megbízható rendszer hitelesítés-szolgáltatáshoz - Magas szintű terv v1.0
- TRUST&CA v2.0 megbízható rendszer hitelesítés-szolgáltatáshoz - Alacsony szintű terv v1.0
- Megfelelés elemzések - Trust&CA hitelesítés-szolgáltatás szoftver v2.0 - v1.0
- Adminisztrátori kézikönyv – Trust&CA hitelesítés-szolgáltatás szoftver v2.0 - v1.0
- RA kézikönyv – Trust&CA hitelesítés-szolgáltatás szoftver v2.0 - v1.0
- A fejlesztési biztonság dokumentációja - Trust&CA hitelesítés-szolgáltatás szoftver v2.0 - v1.0
- Az életciklust meghatározó dokumentáció –Trust&CA hitelesítés-szolgáltatás szoftver v2.0 - v1.0
- A hibajelentési eljárások –Trust&CA hitelesítés-szolgáltatás szoftver v2.0- v1.0
- A fejlesztő eszközök dokumentációja -Trust&CA hitelesítés-szolgáltatás szoftver v2.0 - v1.0
- Tesztelési dokumentáció – Trust&CA teszt jegyzőkönyv_fin.doc és Trust&CA teszt jegyzőkönyv_fin_nshield.doc
- Teszt lefedettség elemzés -Trust&CA hitelesítés-szolgáltatás szoftver v2.0 - v1.0
- Teszt mélység elemzés -Trust&CA hitelesítés-szolgáltatás szoftver v2.0 - v1.0
- Az útmutatók elemzése –Trust&CA hitelesítés-szolgáltatás szoftver v2.0 - v1.0
- Biztonsági funkcióerősség elemzés – Trust&CA hitelesítés-szolgáltatás szoftver v2.0 - v1.0
- Sebezhetőség elemzés – Trust&CA hitelesítés-szolgáltatás szoftver v2.0 - v1.0

A tanúsításhoz figyelembe vett, fejlesztőktől független dokumentumok

Értékelési jelentés - TRUST&CA v2.0 megbízható rendszer hitelesítés-szolgáltatáshoz v1.0 (Készítette HunGuard Kft.)

A követelményeknek való megfelelést ellenőrző független vizsgálat módszere

A TCA v2.0 rendszer a CEM (Common Evaluation Methodology) v2.3 módszertana szerint került független értékelésre és tanúsításra.

Az értékelés garanciaszintje

EAL4

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