TANÚSÍTVÁNY

A **HUNGUARD** Számítástechnikai-, informatikai kutató-fejlesztő és általános szolgáltató Kft. a 15/2001.(VIII. 27.) MeHVM rendelet alapján, mint a Magyar Köztársaság Informatikai és Hírközlési Miniszter 002/2004 számú kijelölési okiratával kijelölt terméktanúsító szervezet

tanúsítja,

hogy az
Axelero Rt.
által kifejlesztett és forgalmazott

Marketline Integrált Aláíró Modul

2.0-ás verzió

elektronikus aláírási 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
fokozott biztonságú elektronikus aláírás

létrehozásában és ellenőrzésében történő felhasználásra

Jelen tanúsítvány a HUNG-TJ-026-2004. számú tanúsítási jelentés alapján került kiadásra.
Készült az Axelero Rt. megbízásából.

A tanúsítvány regisztrációs száma: **HUNG-T-026/2004.**
A tanúsítás kelte: 2004. november 30.
A tanúsítvány érvényességi ideje: 2007. november 30.
Mellékletek: tulajdonságok, feltételek, követelmények, egyéb jellemzők, összesen 6 oldalon.

PH.

Endrődi Zsolt
tanúsítási igazgató

dr. Szabó István
ügyvezető igazgató

1. számú melléklet

A Marketline Integrált Aláíró Modul v2.0 legfontosabb tulajdonságainak összefoglalása

1.1 Architektúra

A MIAM v2.0 Java nyelven készített automata aláírást létrehozó és aláírást ellenőrző alkalmazás.

Az elektronikus aláíró és aláírás ellenőrzési funkciókat a MultiSigno Developer Professional (2.1 verzió) függvénykészlete felhasználásával valósítja meg, amit Java illesztő felületen keresztül ér el.

A MultiSigno Developer Professional fejlesztő készlet DLL elemei a Microsoft Crypto API függvényeit hívják meg. Az aláírandó/ellenőrizendő XML struktúrára az MS Crypto API-n keresztül történik az aláírás létrehozásának és ellenőrzésének aktivizálása.

A MIAM v2.0 futtatási környezete Windows 2000 server.

Az aláírások létrehozása és ellenőrzése automatizált folyamatként emberi beavatkozás nélkül történik.

Az aláírás-létrehozó adat (magánkulcs) az operációs rendszer tanúsítványtárában található.

Az aláíró tanúsítványát a Matáv hitelesítés-szolgáltató hitelesíti.

Az aláírások ellenőrzéséhez a Matáv hitelesítés-szolgáltató biztosít CRL-t, legalább 24 óránkénti frissítéssel.

1.2 A tranzakciós környezet

A tranzakciós környezetben az OTP és beszállítói között elektronikus megrendelések és azokra küldött visszaigazolások, valamint ajánlatkérések és ajánlatok kétirányú kommunikációja zajlik a Marketline közvetítésével.

Az aláírásra és ellenőrzésre kerülő tranzakciók (dokumentumok) iDOC XML formátumúak.

Egy iDOC XML tranzakcióhoz tetszőleges formátumú csatolt dokumentum is kapcsolódhat, melyek a tranzakció részeként, azzal együtt szintén aláírásra kerülnek.

Az OTP oldali rendszerből a beszállítók felé a következő típusú tranzakciók indulnak (mely tranzakciókat a MIAM v2.0 elektronikus aláírással lát el):

- ajánlatkérés,
- megrendelés
- megrendelés módosítása és törlése.

A beszállítók oldaláról az OTP rendszerébe a következő típusú tranzakciók érkeznek (mely tranzakciók elektronikus aláírásait a MIAM v2.0 ellenőrzi):

- ajánlat,
- megrendelés visszaigazolása,
- számla.

A Marketline rendszere a tranzakciókat csak továbbítja, archiválja és naplózza, azokon nem módosít. A tranzakciókon az aláírás kapcsán formátum változtatás történik, mely a tartalmat nem befolyásolja.

1.3 Tulajdonságok

A MIAM v2.0 nem használ külső eszközt az aláírások létrehozására.

A MIAM v2.0 által létrehozott, és fogadáskor ellenőrzött aláírások formátuma az XML-Signature (RFC 3275, XML-Signature Syntax and Processing) szabványnak felel meg.

A rendszer többszörös aláírásokat nem kezel.

Az aláírások aláírt aláírási jellemzőként tartalmazzák az alábbiakat:
- aláírási szabályzat azonosító,
- az aláíráshoz felhasznált végfelhasználói tanúsítvány,

Az aláírások nem aláírt aláírási jellemzőként tartalmazzák az alábbiakat:
- időbélyegző,
- az aláírás létrehozásának időpontjában érvényes visszavonási lista,
- a visszavonási lista aláírásához használt szolgáltatói tanúsítvány.

A MIAM v2.0 eArchiv funkciója az archiválandó dokumentumokat rendszeresen ellenőrzi, és megpróbálja kicserélni az aláíró tanúsítványhoz tartozó visszavonási listát egy az aláírás ideje (az időbélyegzőben szereplő időpont) utáni kibocsátásúra. Ha ez az aláírás ideje után 48 órával sem sikerül, az adott dokumentumra hibát jelez, az archiválás sikertelen.

A MIAM v2.0 tanúsítványtárnak az operációs rendszer tanúsítványtárát használja.

A MIAM v2.0 mind a sikeres, mind a sikertelen aláírásokról naplóbejegyzést készít.

1.4 Az értékelés tárgya és hatóköre

Jelen tanúsítás (és az alapját képező biztonsági értékelés) tárgya a MIAM v2.0, mely egyéb programokkal együttműködve valósítja meg az aláíró alkalmazásoktól elvárt funkcionalitást. /A MIAM v2.0 program a MultiSigno Developer Professional (Pack.dll) fejlesztő készlet elemeit hívja meg az aláírás létrehozásának és ellenőrzésének folyamatában. A MultiSigno Developer Professional teljes mértékben a Windows operációs rendszer erőforrásaira, eszközeire támaszkodik. A Crypto API függvényeit használja, amely a Windows CSP-jét használja./

Az értékelés feltételezte, hogy a MIAM v2.0 alapját képező alábbi funkciók és platformok biztonságosan és helyesen működnek:
- a MultiSigno Developer Professional (Pack.dll) aláíró alkalmazás fejlesztő készlet DLL elemei (ennek biztonságos és helyes működését a HUNG-T-010-2003 számú tanúsítás is alátámasztja),
- a Microsoft Crypto API függvényei,
- a Windows CSP.

2. számú melléklet

A biztonságos felhasználás feltételei

Az alábbiakban összefoglaljuk azokat a kötelezően betartandó, a tanúsítvány érvényességére kiható feltételeket, melyek hozzájárulnak a MIAM v2.0 által kezelt aláírások fokozott biztonságához.

1. számú feltétel
A MIAM v2.0 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.

2. számú feltétel
A MIAM v2.0 működtetési környezetében technikai és eljárásrendi intézkedéseket kell tenni az alábbiak biztosítására:

- vírusok ne ronthassák el az aláíró alkalmazást és az általa meghívott egyéb aláíró összetevőket, valamint
- az esetlegesen vírussal fertőzött aláíró összetevőket megfelelően helyre lehessen állítani.

3. számú feltétel
A MIAM v2.0 működtetési környezetében technikai és eljárásrendi intézkedéseket kell tenni annak biztosítására, hogy megvédjék a MIAM v2.0 funkcionális összetevőinek sértetlenségét, megakadályozva, hogy behatolók elrontsák ezt.

4. számú feltétel
A MIAM v2.0 működtetési környezetében technikai és eljárásrendi intézkedéseket kell tenni annak biztosítására, hogy a MIAM v2.0 alkalmazást, valamint valamennyi az aláírás-létrehozás, aláírás-ellenőrzés folyamatokkal kölcsönhatásba lépő összetevőjét egy biztonságos területen valósítsák meg.

5. számú feltétel
A magánkulcsok és tanúsítványok számítógépre táplálásakor (a Windows 2000 operációs rendszer védett tárába, illetve tanúsítványtárába) az OTP ISzR Kulcskezelési szabályzat (V2.0) 5.2 (Magánkulcs és tanúsítvány betáplálása), 6.1 (Magánkulcs biztonsági mentése) és 6.2 (Aktiválási adat biztonsági mentése) pontjaiban meghatározott szabályokat be kell tartani. A működtetés során folyamatosan biztosítani kell azt is, hogy illetéktelen módon a magánkulcsokat és tanúsítványokat ne cseréljék ki, a tárakat pedig más magánkulccsal, tanúsítvánnyal illetéktelenül ne egészítsék ki.

3. számú melléklet

TERMÉKMEGFELELŐSÉGI KÖVETELMÉNYEK

Követelményeket és szabványokat tartalmazó dokumentumok

Követelmények

Az elektronikus aláírásról szóló 2001. évi XXXV. törvény

CEN/ISSS/E-Sign; CWA 14170:2004; Security requirements for signature creation applications

CEN/ISSS/E-Sign; CWA 14171:2004; General guidelines for electronic signature verification

Szabványok

RFC 3161	Internet X.509 PKI - Time-Stamp Protocol
RFC 3275	XML-Signature Syntax and Processing
RFC 3280	Internet X.509 PKI - Certificate and Certificate Revocation List (CRL) Profile

4. számú melléklet

A tanúsítási eljárás egyéb jellemzői

A tanúsításhoz figyelembe vett fejlesztői dokumentumok

- Kérdőív a tanúsítás kérelmezéséhez
- Koncepcionális Terv - OTP - Marketline elektronikus számlafogadás megvalósítása (2003. december 23.)
- Bevezetési Terv - OTP - Marketline elektronikus számlafogadás megvalósítása (2004. február 27.)
- PKI koncepció az OTP – Marketline e-szla projekthez (2004. február 27.)
- Elektronikus Számla Interface - Specifikáció - Verzió 1.0 - Document Rev. 1.0. (2004. január 21.)
- Elektronikus Számla válasz (INVOICERESPONSE) specifikáció - Verzió 1.0) (2004. január 26.)
- Üzemeltetési Leírás /az OTP R/3 rendszerét és a Marketline Integrált Szállítói Rendszert összekötő és digitálisan aláíró rendszerkomponensek üzemeltetésére (elektronikus számlával kiegészült verzió)/ (2004. október 18.)
- Fejlesztési környezet - OTP - Marketline Szállítói rendszer - elektronikus aláírás projekt - Aláírási modul (2004. február 2.)
- Marketline ISzR Aláírási szabályzat - Verzió 4.0 (2004 október 20.)
- OTP ISzR Kulcskezelési szabályzat - Verzió 2.0 (2003 március 31.)

A tanúsításhoz figyelembe vett, fejlesztőktől független dokumentumok

- Értékelési jelentés az „OTP elektronikus számlafogadás megvalósítása" projekt keretében az OTP oldalán megvalósított Marketline Integrált Aláíró Modulról (verzió: 2.0) /2004. 11.08/

A követelményeknek való megfelelést ellenőrző független vizsgálat garancia szintje

A követelményeknek való megfelelést ellenőrző független vizsgálat garancia szintje az MSZ ISO/IEC 15408:2002 /Közös szempontok, Common Criteria/ EAL 2-es szintjéhez hasonló volt:

1. Az ellenőrző vizsgálat a MIAM v2.0 biztonsági viselkedésének megértése érdekében elemezte a biztonsági funkciókat, ehhez felhasználta a fejlesztői dokumentációkat.
2. Az értékelés kitért az aláírást és aláírás ellenőrzést végző modul fejlesztési környezetének, valamint a fejlesztők által a konfigurációkezelésre és verziókezelésre alkalmazott eljárások vizsgálatára is.
3. Az értékelés kitért az aláírást és aláírás ellenőrzést végző modulra, illetve az ennek működtetési környezetére vonatkozó szabályzatok vizsgálatára is. Ennek az értékelési feladatnak annak megállapítása volt a célja, hogy az értékelés tárgya megfelel-e a szabályzatokban leírtaknak, illetve biztosítja-e a szabályzatban leírtak támogatását.
4. Az értékelők a fejlesztőktől független tesztelést végeztek.