



# 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 006/2002 számú kijelölési okiratával kijelölt termék tanúsító szervezet

**tanúsítja,**  
hogy az  
**Axelero Rt.**  
által kifejlesztett és forgalmazott

**Marketline**  
**integrált aláíró alkalmazás**  
1.0-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-015-2004. számú tanúsítási jelentés alapján került kiadásra.  
Készült az Axelero Rt. megbízásából.

A tanúsítvány regisztrációs száma: **HUNG-T-015/2004.**

A tanúsítás kelte: 2004. február 12.

A tanúsítvány érvényességi ideje: 2006. február 12.

Mellékletek: tulajdonságok, feltételek, követelmények, egyéb jellemzők, összesen 6 oldalon.

PH.

Tanúsítási igazgató:

Ügyvezető igazgató



## 1. számú melléklet

### A Marketline integrált aláíró alkalmazás v1.0 legfontosabb tulajdonságainak összefoglalása

#### 1.1 Architektúra

A Marketline integrált PKI modul egy Java nyelven készített automata aláírást létrehozó és aláírást ellenőrző alkalmazás.

Az elektronikus aláíró és aláírás ellenőrzési funkciókat a MultiSigno Developer (1.3 verzió) függvény készletének felhasználásával valósítja meg, amit Java illesztő felületen keresztül ér el.

A MultiSigno Developer 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.

Futtatási környezet: 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, 24 óránkénti frissítéssel.

#### 1.2 Tulajdonságok

A Marketline integrált PKI modul szerveren tárolt tanúsítványokat használ az aláírások létrehozására.

Az aláírandó adat formátuma mindig iDOC XML.

A csatolt dokumentumok formátuma (az aláírás szabályzatban meghatározottaknak megfelelően) az alábbi lehet:

- iDOC XML,
- Microsoft Word dokumentum (DOC),
- Microsoft Excel táblázat (XLS),
- Adobe Acrobat dokumentum (PDF),
- Microsoft PowerPoint prezentáció (PPT),
- Zip tömörített állomány (ZIP),
- Rar tömörített állomány (RAR),
- egyszerű szövegállomány (TXT),
- Rtf dokumentum (RTF),
- Web oldal (HTML),
- GIF formátumú kép,
- TIF formátumú kép és
- JPG formátumú kép.



Az aláírás formátuma: XML-Signature.

Aláírt aláírási tulajdonságként az aláíró által állított aláírási dátum kerül az aláírásba.

Nem aláírt aláírási tulajdonságként az aláíró tanúsítványa, valamint az aláíráskor aktuális CRL kerül az aláírásba.

A rendszer időbélyegző alkalmazását nem követeli meg.

Az aláírás dátuma a rendszer dátuma, ami negyedóránál nagyobb mértékben nem térhet el a központi szerver órájától.

A Marketline integrált PKI modul tanúsítványtárnak az operációs rendszer tanúsítványtárát használja.

A Marketline integrált PKI modul mind a sikeres, mind a sikertelen aláírásokról naplóbejegyzést készít.

Az aláírás kötelezettségvállalást jelent, miszerint az aláíró (aki a Marketline integrált PKI modul alkalmazást elindító, a cég nevében eljáró személy) az aláírásával elismeri, hogy az aláírt iDOC XML dokumentumot és a csatolásokat ő készítette, hagyta jóvá és küldte el az aláírásban jelölt időpontban.

### **1.3 Az értékelés tárgya és hatóköre**

Jelen tanúsítási jelentés tárgya maga a Marketline integrált PKI modul, mint aláíró alkalmazás.

A tanúsítás során feltételeztük, hogy az alábbi, a Marketline integrált PKI modul aláíró alkalmazás alapját képező funkciók és platformok biztonságosan és helyesen működnek:

- a MultiSigno Developer fejlesztő készlet DLL elemei (ennek biztonságos és helyes működését a HUNG-T-003-2003 számú tanúsítás is alátámasztja),
- a Microsoft Crypto API függvényei.



## 2. számú melléklet

### A biztonságos felhasználás feltételei

Az alábbiakban összefoglaljuk azokat a kötelezően betartandó, a tanúsítvány érvényességére kiható feltételeket, melyek hozzájárulnak a Marketline integrált aláíró alkalmazás által kezelt aláírások fokozott biztonságához.

#### **1. számú feltétel**

A magánkulcsok és tanúsítványok számítógépre táplálásakor (a Windows 2000 operációs rendszer védett tárába, illetve tanúsítványtárába) az ISZR Kulcskezelési szabályzat (V2.0) 5.2 és 6.3 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 tárokat pedig más magánkulccsal, tanúsítvánnyal illetéktelenül ne egészítsék ki.

#### **2. számú feltétel**

A Marketline integrált aláíró alkalmazás működtetési környezetében technikai és eljárásrendi intézkedéseket kell tenni annak biztosítására, hogy az aláírási folyamatba ne avatkozassanak be olyan nem megbízható rendszer és alkalmazási folyamatok, perifériák és kommunikációs csatornák, amelyek nem szükségesek az aláírás-létrehozás alkalmazás működéséhez.

#### **3. számú feltétel**

A Marketline integrált aláíró alkalmazás működtetési környezetében technikai és eljárásrendi intézkedéseket kell tenni az alábbiak biztosítására:

- vírusok ne ronghassák el a Marketline integrált aláíró alkalmazást és az általa meghívott egyéb aláíró összetevőket (DLL, CSP), valamint
- az esetlegesen vírussal fertőzött aláíró összetevőket megfelelően helyre lehessen állítani.

#### **4. számú feltétel**

A Marketline integrált aláíró alkalmazás működtetési környezetében technikai és eljárásrendi intézkedéseket kell tenni annak biztosítására, hogy megvédjék az aláíró alkalmazás funkcionális összetevőinek sértetlenségét, megakadályozva, hogy behatolók elrontsák ezt.

#### **5. számú feltétel**

A Marketline integrált aláíró alkalmazás működtetési környezetében technikai és eljárásrendi intézkedéseket kell tenni annak biztosítására, hogy az aláíró alkalmazást, 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/ISSS/E-Sign; Area G1, 14170 munkacsoport egyezmény: Security Requirements for Signature Creation Systems

CEN/ISSS/E-Sign; Area G2, 14171 munkacsoport egyezmény: Procedures for Electronic Signature Verification

CEN/ISSS/E-Sign; Area V, 14172-4 munkacsoport egyezmény: Signature Creation Application and Procedures for Electronic Signature Verification



## 4. számú melléklet

### A tanúsítási eljárás egyéb jellemzői

#### **A tanúsításhoz figyelembe vett egyéb fejlesztői dokumentumok**

Kérelem a tanúsítás elvégzésére

Kérdőív a tanúsítás kérelmezéséhez

#### **A tanúsításhoz figyelembe vett, fejlesztőktől független dokumentumok**

Értékelési jelentés a „PKI Projekt” keretében fejlesztett, csatolt dokumentumok kezelésével kiegészített, központi oldali elektronikus aláírási alkalmazás összetevőre /2003. 06.24/

Értékelési jelentés kiegészítés a „PKI Projekt” keretében fejlesztett, csatolt dokumentumok kezelésével kiegészített, /hitelesítés-szolgáltató váltás miatt módosított/ központi oldali elektronikus aláírási alkalmazás összetevőre /2004.01.12/

**A követelményeknek való megfelelést ellenőrző független vizsgálat garancia szintje  
az ISO 14508 /Common Criteria/ EAL 2-es szintjéhez hasonló volt**

**A Marketline integrált aláíró alkalmazás v 1.0 biztonsági funkciók értékelt erőssége  
közepes szintű**