



# 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 terméktanúsító szervezet

**tanúsítja,**

hogy a

**polysys®**

által kifejlesztett és forgalmazott

**"A2-Polysys CryptoSigno Interop JAVA API**

**minősített elektronikus aláíráshoz"**

**aláíró alkalmazás fejlesztő készlet**

2.0.0-ás verzió

elektronikus aláírási termék

*az 1.számú mellékletben áttekintett funkcionalitással, valamint*

*a 2. számú mellékletben meghatározott,*

*informatikai környezetre és biztonságos használatra vonatkozó feltételeinek figyelembe vételével*

**megfelel**

a 2001. évi XXXV. törvényben szereplő

**minősített elektronikus aláírás**

**létrehozása és ellenőrzése céljából történő**

**szabványos és biztonságos alkalmazások fejlesztéséhez.**

Jelen tanúsítvány a HUNG-TJ-29-2006. számú tanúsítási jelentés alapján került kiadásra.

Készült a Polysys Kft. megbízásából.

A tanúsítvány regisztrációs száma: **HUNG-T-29/2006.**

A tanúsítás kelte: 2006. február 23.

A tanúsítvány érvényességi ideje: 2009. február 23.

Mellékletek: tulajdonságok, feltételek, követelmények, egyéb jellemzők, összesen 11 oldalon.

PH.

Endrődi Zsolt  
tanúsítási igazgató

dr. Szabó István  
ügyvezető igazgató



## 1. számú melléklet

### Az A2-Polysys CryptoSigno Interop JAVA API minősített elektronikus aláíráshoz v2.0.0 legfontosabb tulajdonságainak összefoglalása

Az A2-Polysys CryptoSigno Interop JAVA API minősített elektronikus aláíráshoz v2.0.0 (a továbbiakban A2-API) egy platform független fejlesztő készlet (könyvtár), mely a ráépülő, Java technológiával készülő alkalmazások számára támogatást nyújt az alábbiakhoz:

- minősített vagy fokozott biztonságú elektronikus aláírás létrehozása és ellenőrzése,
- titkosítás és dekódolás,
- tanúsítási útvonal felépítése és érvényesítése,
- tanúsítvány visszavonási listák ellenőrzése,
- azonosítás, hitelesítés és jogosultság ellenőrzés

annak érdekében, hogy az alkalmazások hatékony és szabványos PKI szolgáltatásokat legyenek képesek biztosítani.

Az A2-API-nak két üzemmódja különböztethető meg:

- szigorú üzemmód, mely minősített elektronikus aláírás létrehozására alkalmas,
- normál üzemmód, mely fokozott biztonságú elektronikus aláírás létrehozására alkalmas,

Mindkét üzemmód szoftver konfigurációs követelményei az alábbiak:

- Operációs rendszer: Linux, Solaris, Unix, Java Desktop System, Windows,
- JRE 1.5 Java futtató környezet, vagy JRE1.4.2 és (BALE vagy ALE használata esetén) egy PKCS#11 kriptográfiai szolgáltató modul,
- PKCS#11 driver.

Mindkét üzemmód hardver konfigurációs követelményei az alábbiak:

- CPU: 400 MHz vagy magasabb,
- RAM: 256 Mbyte vagy több,
- Diszk hely: 20 Mbyte vagy több,
- PKCS#11 token.



Az A2-API a már korábban (Hung-T-25/2004 regisztrációs számon) tanúsított „A1-Polysys CryptoSigno JAVA API minősített elektronikus aláíráshoz v1.1.0” aláíró alkalmazás fejlesztő készlet (a továbbiakban A1-API) továbbfejlesztett és kibővített változata.

Az A2-API felülről kompatibilis az A1-API-val, amely azt jelenti, hogy képes az annak megfelelő aláírások létrehozására és ellenőrzésére.

A továbbfejlesztés és bővítés eredményeként az A2-API:

- a szabványos XAdES formátumok teljes skáláját felölelő (XAdES-BES, EPES, T, C, X, X-L, A), egyúttal interoperabilitást is biztosító (az „Az Informatikai és Hírközlési Minisztérium ajánlása a közigazgatásban alkalmazható elektronikus aláírás formátumok műszaki specifikációjára (2005. november 22.)” ajánlásnak megfelelően) aláírás létrehozó és ellenőrző funkciókat valósít meg,
- az aláírás létrehozása és ellenőrzése során az RFC 3161 (TSP, X.509 Internet Public Key Infrastructure Time-Stamp Protocol) szerint kér és ellenőriz időbélyegeket,
- az aláírás létrehozása és ellenőrzése során képes az RFC 2560 (OCSP, X.509 Internet Public Key Infrastructure Online Certificate Status Protocol) szerinti OCSP kérésre és az OCSP válasz ellenőrzésére.



## 2. számú melléklet

### A biztonságos felhasználás feltételei

Az alábbiakban összefoglaljuk azokat a feltételeket, melyek betartása hozzájárul az A2-API segítségével fejlesztett aláíró alkalmazások biztonságához.

Ezek a feltételek a fejlesztésekkel szembeni általános minőségbiztonsági (tervezési, tesztelési, dokumentálási stb.) követelményeken túlmutatóan az aláírás-specifikus elemek ellenőrzött védelmi szintjét szándékoznak garantálni.

#### A fejlesztők által kötelezően betartandó szabályok

Az alábbi feltétel az A2-API felhasználásával aláíró alkalmazásokat fejlesztők számára fogalmaz meg kötelező elvárást (feltételt), hogy hogyan használják ezt a terméket saját fejlesztésükhöz.

1. Az A2-API-t CD-n vagy PenDrive-on juttatják el a felhasználókhöz, vagy Java WebStart technológia alkalmazásával on-line módon lehet azt letölteni. Használatba vétele előtt kötelező másolatot készíteni róla, hogy az eredetit mesterpéldányként lehessen felhasználni.

Az A2-API elsődleges felhasználója a fejlesztő készletet felhasználó alkalmazások fejlesztője. Ugyanakkor az A2-API szolgáltatása alapvetően a vele fejlesztett alkalmazásokban fog érvényre jutni. Ezért az A2-API másodlagos felhasználójaként a ráépülő alkalmazások használói (akik valószínűleg felhasználói és adminisztrátori szerepkörökbe lesznek szétválasztva) is megjelennek majd.

A fentiekhez hasonlóan Az A2-API informatikai környezete egyrészt a fejlesztő készletet felhasználó alkalmazások fejlesztői környezete, másrészt az így készült alkalmazásokat működtető környezet.

Az alábbi feltételezések a felhasználó és az informatikai környezet fogalmát a fenti kettős értelemben értik.

#### Feltételezések az A2-API informatikai környezetére

1. A jogosult felhasználók megbízhatóak a számukra kijelölt funkciók végrehajtására.
2. Az A2-API helyesen van telepítve és konfigurálva.
3. Az A2-API normál üzemmódjához (fokozott biztonságú aláírás létrehozásához) az informatikai környezet tartalmaz egy vagy több kriptográfiai modult, amely(ek) megfelel(nek) a FIPS 140 legalább 1-es szintjének, és a következő műveletek végrehajtására alkalmas(ak): RSA kulcspár generálása (legalább 1024 bit kulcsmérettel), 256 bites AES kulcs generálása, digitális aláírás létrehozása és ellenőrzése (RSA algoritmussal), titkosítás és dekódolás (AES algoritmussal), biztonságos lenyomat készítés (SHA-1 algoritmussal), véletlenszám generálás.



4. Az A2-API szigorú üzemmódjához (minősített aláírás létrehozásához) az informatikai környezet tartalmaz:
  - egy az NHH által nyilvántartásba vett, tanúsított, PKCS#11 interfészt támogató BALE eszközt, mely a következő műveletek végrehajtására alkalmas: RSA kulcspár generálása (legalább 1024 bit kulcsmérettel), digitális aláírás létrehozása (RSA algoritmussal), RSA-val titkosított AES kulcs kulcs dekódolása,
  - egy vagy több olyan kriptográfiai modul, amely(ek) megfelel(nek) a FIPS 140 legalább 1-es szintjének, és a következő műveletek végrehajtására alkalmas(ak): digitális aláírás ellenőrzése (RSA algoritmussal), 256 bites AES kulcs generálása, a generált AES kulcs (legalább 1024 bit kulcsméretű) RSA-val történő titkosítása, titkosítás és dekódolás (AES algoritmussal), biztonságos lenyomat képzés (SHA-1 algoritmussal).
5. Az A2-API-vel szembeni támadási potenciált alacsonynak tételezzük fel.
6. Az informatikai környezet gondoskodik a fizikai védelemről, így az A2-API szoftver elemei jogosulatlan fizikai hozzáférés ellen védettek.
7. Az A2-API fejlesztő készletet meghívó alkalmazás biztosítja a fejlesztő készlet számára a tanúsítvány és tanúsítvány visszavonási lista információkat.
8. Az informatikai környezet gondoskodik a megfelelő pontosságú rendszeridőről.
9. A hardver konfigurációra vonatkozóan az alábbi (kiegészítő) elvárások vannak:
  - CPU: 400 MHz vagy magasabb,
  - RAM: 256 Mbyte vagy több,
  - Diszk hely: 20 Mbyte vagy több.
10. Az operációs rendszerhez (Linux, Solaris, Unix, Java Desktop System, Windows) a Sun Java JRE 1.5 Java futtató környezet rendelkezésre áll, és az operációs rendszer képes azt futtatni. Ha az adott platformon még nem áll rendelkezésre a JRE 1.5 verzió, akkor az helyettesíthető JRE 1.4.2 + PKCS#11 kriptográfiai szolgáltató modul együttesével.
11. Szigorú üzemmód esetén (minősített aláírás létrehozásához), ha a környezet nem tekinthető biztonságosnak, az A2-API fejlesztő készlettel készített aláíró alkalmazáshoz olyan PKCS#11 driver-t, vagy egyéb hardver-szoftver összetevők vannak alkalmazva, amelyek képesek egy megbízható útvonalat kiépíteni a BALE-vel, s ezzel biztosítani a BALE-nek továbbított, aláíró hitelesítő adat (PIN kód) bizalmasságát, illetve az aláírandó adatból képzett lenyomat és valamennyi protokoll adat sértetlenségét.
12. Az informatikai környezetben olyan BALE /ALE kezelő szoftvert van alkalmazva, amely képes biztosítani a tudáson alapuló hitelesítő adatok (PIN kód) lecserélhetőségét és a lecserélésnél az új PIN kód kétszeri bekérését, vagy ezt a funkcionalitást az A2-API fejlesztő készlettel készített alkalmazásnak kell megvalósítania.



### **Feltételezések az A2-API biztonságos használatára**

Az alábbi feltételek (felhasználói felelősségek) a biztonságos használatra vonatkoznak:

1. A felhasználónak biztosítania kell a rendszeridő megfelelő pontosságát. A rendszeridőt pontosan be kell állítani, majd a rendszeridő pontosságának időszakonkénti ellenőrzéséről és szinkronizálásáról is gondoskodni kell.
2. Szigorú üzemmódban a felhasználónak gondoskodnia kell a BALE fizikai védelméről. A felhasználónak mindent el kell követnie ahhoz, hogy a BALE-t ne tulajdoníthassák el, fizikailag ne sérüljön meg, a BALE a PIN kód többszöri helytelen megadása következtében ne kerüljön zárolt állapotba.
3. Szigorú üzemmódban a felhasználónak titokban kell tartania a BALE hozzáféréséhez szükséges hitelesítő adatát (PIN kódját, jelszavát vagy jelmondatát). Ezt a hitelesítő adatot tilos papírra vagy elektronikusan olyan módon feljegyezni, hogy az mások számára hozzáférhetővé válhasson.
4. Normál üzemmódban a felhasználónak gondoskodnia kell az ALE vagy PKCS#12 kulcstároló (pl. fájl, PEN drive, stb) fizikai védelméről. A felhasználónak mindent el kell követnie ahhoz, hogy az ALE-t ne tulajdoníthassák el, az ALE a PIN kód többszöri helytelen megadása következtében ne kerüljön zárolt állapotba, a PKCS#12 kulcstároló tartalmát ne másolják le.
5. Normál üzemmódban a felhasználónak titokban kell tartania az ALE vagy PKCS#12 kulcstároló hozzáféréséhez szükséges hitelesítő adatát (PIN kódját, jelszavát vagy jelmondatát). Ezt a hitelesítő adatot tilos papírra vagy elektronikusan olyan módon feljegyezni, hogy az mások számára hozzáférhetővé válhasson.

### **Feltételezések az A2-API segítségével fejlesztett alkalmazásokra**

Az alábbi feltételeket az alkalmazás fejlesztőjének azért erősen javasolt figyelembe vennie, hogy az alkalmazás is kellően biztonságos legyen:

1. Az alkalmazás adminisztrátori útmutatójában a jelen mellékletben a „Feltételezések az A2-API informatikai környezetére” címszó alatt meghatározottak is szerepeljenek.
2. Az alkalmazás útmutató dokumentumaiban a jelen melléklet „Feltételezések az A2-API biztonságos használatára” címszó alatt meghatározottak is szerepeljenek.
3. Az alkalmazásoknak célszerű szétválasztani a felhasználói és adminisztrátori szerepköröket. Ebben az esetben csak az adminisztrátori szerepkört betöltő személy vagy folyamat végezhesse az alábbiakat:
  - megbízható legfelső szintű hitelesítő tanúsítványok menedzsmentje,
  - a CRL a kibocsátást követő hány napig aktuális biztonsági jellemző beállítása,
  - a CRL a következő kibocsátási dátumot követő hány napig aktuális biztonsági jellemző beállítása,
  - időbélyeg szolgáltatás elérhetősége biztonsági jellemző beállítása,
  - OCSP szolgáltatás elérhetősége biztonsági jellemző beállítása,
  - OCSP szolgáltatás támogatása esetén az alábbi biztonsági jellemző beállítása:
    - az OCSP válasz az előállítást követő hány percig aktuális,
    - az OCSP válasz a kibocsátást követő hány percig aktuális,
    - az OCSP válasz a következő kibocsátást követő hány percig aktuális,
    - OCSP válasz frissesség ellenőrzés engedélyezése
  - szervezeti aláírási szabályzat biztonsági jellemző beállítása
  - a biztonságot érintő jellemzők alapállapota.



4. Az alkalmazás telepítési eljárását úgy kell kialakítani, hogy az magában foglalja az A2-API megfelelő telepítését is.
5. Az A2-API működését befolyásoló biztonsági jellemzőket az alkalmazás felhasználójának tudtával és szándékával megegyezően kell beállítani. Az alkalmazást úgy kell kialakítani, hogy rendelkezzen olyan megfelelő GUI felületekkel, amelyeken az alkalmazás felhasználója a biztonsági jellemzőket beállíthatja. A GUI felületeken a felhasználót a biztonsági jellemző beállítani kívánt értékével kapcsolatban fellépő sebezhetőségről tájékoztatni kell. A biztonsági jellemzők beállítása nem történhet az alkalmazás felhasználó számára rejtett módon (programozottan).
6. Az alkalmazás a következő biztonsági jellemzőkre egy adott futásnál beállított értékeket ne tárolja perzisztens módon (vagy azt a következő futásnál ne vegye figyelembe):
  - CRL frissesség ellenőrzés engedélyezése,
  - visszavonás ellenőrzés kihagyásának engedélyezése.A javasolt megoldás az, hogy az alkalmazás programozottan ne állítson be a felsorolt biztonsági jellemzőknek értéket, hanem a felhasználó, a megfelelő GUI felületen, minden egyes futásnál, tudatosan és felelősséggel kezdeményezze a beállítást.
7. Az alkalmazás használata során a visszavonás ellenőrzése legyen bekapcsolva (lásd A2ApiControl osztály, serviceSetBypassRevocationCheckEnabled metódus). A visszavonás ellenőrzése csak indokolt esetben, az alkalmazás felhasználójának tudtával és szándékával megegyezően kapcsolható ki. Az alkalmazás felhasználói útmutatójában figyelmeztetni kell a felhasználót arra, hogy amint lehet, ismétlje meg az aláírás ellenőrzését a visszavonás ellenőrzés bekapcsolt állapotával.
8. Az alkalmazás használata során a visszavonási lista (CRL) frissesség ellenőrzése legyen bekapcsolva (lásd A2ApiControl osztály, serviceSetCRLFreshnessCheckEnabled metódus). A frissesség ellenőrzése csak indokolt esetben, az alkalmazás felhasználójának tudtával és szándékával megegyezően kapcsolható ki. Az alkalmazás felhasználói útmutatójában figyelmeztetni kell a felhasználót arra, hogy amint lehet, ismétlje meg az aláírás ellenőrzését a CRL frissesség ellenőrzés bekapcsolt állapotával.
9. Az alkalmazás használata során, ha az lehetséges, a pontos időt nem a lokális informatikai környezet rendszer órájából, hanem megbízható időszervertől kérve kell megállapítani (lásd A2ApiControl osztály, setTimeServers metódus).
10. Az alkalmazás használata során a CRLAfterThisUpdateLimit és CRLAfterNextUpdateLimit biztonsági jellemzők értékét lehetőség szerint a lehető legkisebb (1 nap, illetve 0 nap) értékre kell állítani. A nagyobb értékre történő beállítás azt eredményezheti, hogy a régi CRL alapján, egy már időközben visszavont tanúsítvány elfogadásra kerülhet (lásd A2ApiControl osztály, serviceSetCRLAfterThisUpdateLimit és serviceSetCRLAfterNextUpdateLimit metódusok).
11. Az alkalmazás futása során, az azonosítás/hitelesítés-hez tartozó tanúsítványhoz a tanúsítási útvonal felépítését és érvényesítését (lásd A2ApiControl osztály, serviceCheckIAACertificate metódus) a lehető leghamarabb el kell végezni.





### Feltételek az A2-API biztonságos használatára

1. Az A2-Polysys CryptoSigno Interop JAVA API fejlesztő készlettel létrehozott aláíró alkalmazáshoz olyan PKCS#11 driver-t kell alkalmazni, amely képes megőrizni az aláírandó adat reprezentáns (DTBSR) és valamennyi protokoll adat sértetlenségét.
2. Az A2-Polysys CryptoSigno Interop JAVA API fejlesztő készlettel létrehozott aláíró alkalmazáshoz olyan PKCS#11 driver-t kell alkalmazni, amely képes megőrizni az aláíró hitelesítő adatok bizalmasságát.
3. Az A2-Polysys CryptoSigno Interop JAVA API fejlesztő készletet 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 aláírási létrehozás alkalmazás működéséhez.
4. Az A2-Polysys CryptoSigno Interop JAVA API fejlesztő készletet használó aláíró alkalmazáshoz:
  - a. vagy olyan PKCS#11 kezelőt kell alkalmazni, amely képes egy időkorlátot megadni arra az időtartamra, ami az aláíró hitelesítő adatok megadásától az aláírási kiváltásáig eltelhet,
  - b. vagy az alkalmazásnak kell biztosítania az elvárást azáltal, hogy az aláírási kiváltása után kéri be a hitelesítő adatot.
5. Az A2-Polysys CryptoSigno Interop JAVA API fejlesztő készletet használó aláíró alkalmazáshoz:
  - a. vagy olyan PKCS#11 kezelőt kell alkalmazni, amely képes egy időkorlát letelte után az aláírási folyamatot félbeszakítani és az aláíró hitelesítő adatok új megadását megkövetelve, kezdi újra a folyamatot, és az újraindítás szükségességéről tájékoztatja az aláíró,
  - b. vagy az alkalmazásnak kell biztosítania az elvárást azáltal, hogy az aláírási kiváltása után kéri be a hitelesítő adatot.
6. Az A2-Polysys CryptoSigno Interop JAVA API fejlesztő készlet használó aláíró alkalmazáshoz telepíteni kell a BALE eszköz kezelő szoftverét, amely biztosítja a tudáson alapuló hitelesítő adatok lecserélhetőségét.
7. Az A2-Polysys CryptoSigno Interop JAVA API fejlesztő készlet használó aláíró alkalmazáshoz telepített BALE eszköz kezelő szoftverének biztosítani kell PIN kód lecserélésénél az új PIN kód kétszeri megadását, a helytelen adatbevitel elkerülése érdekében.
8. Az A2-Polysys CryptoSigno Interop JAVA API 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.





9. Az A2-Polysys CryptoSigno Interop JAVA API programozói könyvtár működtetési környezetében technikai és eljárásrendi intézkedéseket kell tenni annak biztosítására, hogy megvédjék Az A2-Polysys CryptoSigno Interop JAVA API programozói könyvtár funkcionális összetevőinek sértetlenségét megakadályozva, hogy behatolók elrontsák ezt.
10. Az A2-Polysys CryptoSigno Interop JAVA API programozói könyvtár működtetési környezetében technikai és eljárásrendi intézkedéseket kell tenni annak biztosítására, hogy az A2-Polysys CryptoSigno Interop JAVA API 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/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

ETSI TS 101 733 v1.5.1 (2003-12) Electronic Signature Formats

ETSI TS 101 903 v1.2.2 (2004-04) XML Advanced Electronic Signatures (XAdES)

PKE PP (Public Key-Enabled Application Family of Protection Profiles) with < Certification Path Validation (CPV) – Basic, PKI Signature Generation, PKI Signature Verification, PKI Encryption using Key Transfer Algorithms, PKI Decryption using Key Transfer Algorithms, Certificate Revocation List (CRL) Validation Online Certificate Status Protocol Client > at EAL <3> with augmentation /Version: 2.5, 31.10.2002/

#### Szabványok

PKCS #1 RSA Cryptography Standard /RFC 2313/

PKCS#11 Cryptographic Token Interface Standard

PKCS#12 Personal Information Exchange Information Standard

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

RFC 2560 OCSP, X.509 Internet Public Key Infrastructure Online Certificate Status Protocol

RFC 3280 Internet X.509 PKI Certificate and Certificate Revocation List (CRL) Profile

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

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



## 4. számú melléklet

### A tanúsítási eljárás egyéb jellemzői

#### A tanúsításhoz figyelembe vett fejlesztői dokumentumok

- Kérelem a tanúsítás elvégzésére
- Kérdőív a tanúsítás kérelmezéséhez
- Védelmi profil: PKE PP /Public Key-Enabled Application Family of Protection Profiles) with < Certification Path Validation (CPV) – Basic, PKI Signature Generation, PKI Signature Verification, PKI Encryption using Key Transfer Algorithms, PKI Decryption using Key Transfer Algorithms, Certificate Revocation List (CRL) Validation > at EAL <3> with augmentation - Version 2.5 - 31.10.2002/
- Biztonsági előirányzat v2.0
- Funkcionális specifikáció v2.0
- Magas szintű terv v2.0
- Teszt lefedettség és mélység elemzés v2.0
- Tesztelési dokumentáció v2.0
- Konfigurációkezelés dokumentáció v2.0
- Módosítás menedzsment v2.0
- A kiszállítási eljárásai v2.0
- Támogató dokumentáció v2.0
- Fejlesztői útmutató v2.0 /a2-api-DOC-2\_0\_0.jar/
- Sebezhetőség elemzés v2.0
- Melléklet v1.0

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

- Értékelési jelentés az A2-Polysys CryptoSigno Interop JAVA API minősített elektronikus aláíráshoz használható fejlesztő készletről (készítette a Hunguard Kft. értékelési divíziója)

#### A követelményeknek való megfelelést ellenőrző független vizsgálat módszere

Az A2-API 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 /0.95verzió, 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/.