Tanúsítási jelentés

Hung-TJ-025-2004

az
A1-Polysys CryptoSigno JAVA API
minősített elektronikus aláíráshoz v1.1.0
aláíró alkalmazás fejlesztő készletről

/Polysys Kft./

Tartalomjegyzék

1. Összefoglaló

1.1 Az értékelés jellemzői

Az értékelt termék neve:	**A1-Polysys CryptoSigno JAVA API (minősített elektronikus aláíráshoz)**
Verzió szám:	**1.1.0**
Rövid elnevezés:	**A1-API v1.1.0.**
Az értékelt termék típusa:	fejlesztő készlet (könyvtár)
Védelmi profilnak való megfelelés:	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 Verzió: 2.5, Dátum: 2002.10.31.
Értékelés befejezése:	2004. október 28.
Az értékelés módszere:	a MIBÉTS séma értékelési módszertana[1]
Az értékelés garanciaszintje:	fokozott (EAL3+)
Az értékelt termék funkcionalitása:	A fejlesztő készlet (könyvtár) 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.
Konfigurációs követelmények:	Szoftver konfiguráció: • Operációs rendszer: Linux, Solaris, Unix, Java Desktop System, Windows • JRE 1.5 Java futtató környezet, vagy JRE1.4.2 + (ALE/BALE használata esetén) PKCS#11 kriptográfiai szolgáltató modul • PKCS#11 driver (ALE/BALE használata esetén). Hardver konfiguráció: • CPU: 400 MHz vagy magasabb, • RAM: 256 Mbyte vagy több, • Diszk hely: 20 Mbyte vagy több, • PKCS#11 token (ALE/BALE használata esetén).

[1] Az értékelés az alábbi dokumentumokban leírt módszertant és eljárásrendet követte:

- 1. számú MIBÉTS kiadvány: **A MIBÉTS nemzeti séma általános modellezése** /0.9 verzió, 2003 augusztus/,
- 2. számú MIBÉTS kiadvány: **Az értékelés és a tanúsítás folyamatai** /0.9 verzió, 2003 szeptember/,
- 3. számú MIBÉTS kiadvány: Az értékelés módszertana 1 - **A biztonsági előirányzat értékelésének módszertana** /0.9 verzió, 2003 október/,
- 3. számú MIBÉTS kiadvány: Az értékelés módszertana 3 - A fokozott garanciaszint értékelésének módszertana /0.9 verzió, 2003 október/

1.2 Az A1-API v1.1.0 biztonsági előirányzatának jellemzői

1.2.1 A TOE (A1-API v1.1.0) által kivédett fenyegetések

1.2.1.1 (Kivédett) általános fenyegetések

T.Attack	A TOE értékek észrevétlen kompromittálódása következhet be egy (külső vagy belső) támadó jogosulatlan tevékenység végzésének kísérlete miatt.
T.Bypass	Jogosulatlan egyed vagy felhasználó meghamisíthatja a biztonsági tulajdonságokat vagy más adatokat a TOE biztonsági funkcióinak kikerülése és a TOE értékekhez való jogosulatlan hozzáférés megszerzése érdekében.
T.Imperson	Jogosulatlan egyed megszemélyesíthet egy jogosult TOE felhasználót, és ezáltal hozzáféréshez jut a TOE adatokhoz, kulcsokhoz és műveletekhez.
T. Modify	Egy támadó módosíthatja a TSF-et vagy más adatokat, például a tárolt biztonsági beállításokat vagy kulcsokat, hogy hozzáférést szerezzen a TOE-hoz és annak adataihoz.
T.Object_Init	Egy támadó hozzáférhet jogosulatlanul egy objektumhoz annak létrehozása során, ha a biztonsági tulajdonságokat nem állítják be vagy bárki megadhatja azokat az objektum létrehozás során.
T.Private_key	Egy támadó egy felhasználónak adja ki magát a felhasználó magánkulcsának generálása vagy használata által.
T.Role	Egy felhasználó magasabb szintű jogosultságú szerepben jelenhet meg, mint amekkora neki megengedett, és ezt az emelt szintű jogosultságot használhatja fel jogosulatlan tevékenységekhez.
T.Secure_attributes	Egy felhasználó módosíthatja egy objektum biztonsági tulajdonságait, ami által jogosulatlanul hozzáfér az objektumhoz.
T.Shoulder_Surf	Egy jogosulatlan felhasználó a jogosult felhasználó válla fölötti kémleléssel megismeri a hitelesítési információkat a hitelesítési folyamat során.
T.Tries	Egy jogosulatlan egyed próbálgatás és hiba következtében kitalálhatja a hitelesítési információt.

1.2.1.2 A tanúsítási útvonal érvényesítésére irányuló (kivédett) fenyegetések

T.Certificate_Modi	Egy jogosulatlan felhasználó módosíthat egy tanúsítványt, és ezáltal rossz nyilvános kulcs kerül felhasználásra.
T.DOS_CPV_Basic	A visszavonási információk vagy a hozzájuk való hozzáférés lehetősége elvész, így sérül a rendszer rendelkezésre állása.
T.Expired_Certificate	Lejárt (és feltehetően visszavont) tanúsítványt aláírás ellenőrzésre használnak.
T.Masquarade	Nem megbízható egyed (CA) kibocsáthat tanúsítványokat álegyedeknek, miáltal ezek kiadhatják magukat más jogosult felhasználónak.
T.No_Crypto	A felhasználó nyilvános kulcsa és a kapcsolódó információk nem állnak rendelkezésre a kriptográfiai funkció elvégzéséhez.
T.Path_Not_Found	Egy érvényes tanúsítási útvonal nem található valamely rendszerfunkció hiánya miatt.
T.Revoked_Certificate	Egy visszavont tanúsítvány érvényesként való használata a biztonság megsértését vonja maga után.
T.User_CA	Egy felhasználó CA-ként lép fel, és jogosulatlan tanúsítványokat bocsát ki.

1.2.1.3 Az aláírás létrehozására irányuló (kivédett) fenyegetés

T.Clueless_PKI_Sig	A felhasználó jelzés hiányában csak helytelen tanúsítványokat próbál ki az aláírás során.

1.2.1.4 Az aláírás ellenőrzésére irányuló (kivédett) fenyegetések

T.Assumed_Identity_PKI_Ver	Egy felhasználó az aláíró személyére mást feltételezhet egy PKI aláírás ellenőrzése során.
T.Clueless_PKI_Ver	A felhasználó jelzés hiányában csak helytelen tanúsítványokkal próbál ellenőrizni.

1.2.1.5 A titkosításra irányuló (kivédett) fenyegetések

T.Assumed_Identity_WO_En	Egy felhasználó a címzett személyére mást feltételezhet egy kulcs átviteli algoritmussal végrehajtott titkosítás során.
T.Clueless_WO_En	A felhasználó jelzés hiányában csak helytelen tanúsítványokkal próbál titkosítani, kulcs átviteli algoritmust használva.

1.2.1.6 A dekódolásra irányuló (kivédett) fenyegetés

T.Garble_WO_De	A felhasználó nem a megfelelő kulcs átviteli algoritmust vagy nem a megfelelő magánkulcsot alkalmazza, ami az adatok összezagyválását eredményezi.

1.2.1.7 A tanúsítvány visszavonási lista ellenőrzésére irányuló (kivédett) fenyegetések

T.DOS_CRL	A CRL vagy a CRL-hez való hozzáférés nem áll rendelkezésre, így a rendszer rendelkezésre állása sérül.
T.Replay_Revoc_Info_CRL	A felhasználó elfogadhat egy régi CRL-t, mely következtében már visszavont tanúsítványt érvényesnek fogadnak el.
T.Wrong_Revoc_Info_CRL	A felhasználó elfogadhat egy visszavont tanúsítványt, vagy elutasíthat egy érvényeset, rossz CRL miatt.

1.2.2 Feltételezések a TOE (A1-API v1.1.0) informatikai környezetére

Az informatikai környezet biztonságos használatára vonatkozó feltételezések az alábbiak:

AE.Authorized_Users	Az engedéllyel rendelkező felhasználók megbízhatóak a tekintetben, hogy a számukra kijelölt funkciókat megfelelően hajtják végre.
AE.Configuration	A TOE-t megfelelően telepítik és konfigurálják.
AE.Crypto_Module_Normal	A TOE környezetről feltételezés, hogy tartalmaz egy vagy több a FIPS 140 legalább 1-es szintjének megfelelő kriptográfiai modult, mely modul vagy modulok a következő műveletek közül hajtanak végre egyet vagy többet: kulcspár generálás, digitális aláírás létrehozása és ellenőrzése, titkosítás, dekódolás, biztonságos lenyomat képzés, véletlenszám generálás, HMAC és/vagy más szükséges kriptográfiai funkció. Összegezve, a TOE-ben minden kriptográfiai modulnak a FIPS 140 legalább 1-es szintjének megfelelőnek kell lennie.
AE.Crypto_Module_Rigid	A TOE környezetről feltételezés, hogy tartalmaz legalább két kriptográfiai modult, mely közül az egyik egy NHH által, a tanúsított BALE-k nyilvántartásába felvett eszköz, a másik (illetve a többi) pedig a FIPS 140 legalább 1-es szintjének megfelelő. A BALE kriptográfiai modul hajtja végre a következő műveleteket: kulcspár generálás, digitális aláírás létrehozása, dekódolás, biztonságos lenyomat képzés, véletlenszám generálás. A FIPS 140 legalább 1-es szintjének megfelelő kriptográfiai modul (vagy modulok) hajtja (hajtják) végre a következő műveleteket: digitális aláírás ellenőrzése, titkosítás, biztonságos lenyomat képzés, véletlenszám generálás, HMAC és/vagy más szükséges kriptográfiai funkció.
AE.Low	A TOE-val szembeni támadási potenciált alacsonynak tételezzük fel.
AE.Physical_Protection	A környezetről feltételezzük, hogy fizikailag véd. A TOE hardverről és szoftverről feltételezzük, hogy védett a jogosulatlan fizikai hozzáféréssel szemben.
AE.PKI_Info	A tanúsítvány és tanúsítvány visszavonási információk a TOE rendelkezésére állnak.
AE.Time	A környezetről feltételezzük, hogy GMT formában és a megkívánt pontossággal gondoskodik a pontos rendszeridőről.

2. Azonosítás

Az értékelt termék neve:	**A1-Polysys CryptoSigno JAVA API minősített elektronikus aláíráshoz**
Verzió szám:	**1.1.0**
Az értékelt termék alkotó elemei (a felhasználókhoz, vagyis a fejlesztő készlet felhasználásával alkalmazást fejlesztőkhöz kiszállított tételek):	**1. a1-api-BIN-1_1_0.jar** (a fejlesztéshez szükséges A1-API fájlok) **2. a1-api-DOC-1_1_0.jar** (az A1-API v1.1.0 JavaDoc dokumentációja) **3. A1-Polysys_SG_Support_Guide.pdf** (támogató dokumentáció, mely bemutatja az A1-API v1.1.0 fejlesztő készletet, tartalmazza az adminisztrátori és felhasználói útmutatást, leírja az A1-API v1.1.0 telepítését megelőzően elvégzendő teendőket, a telepítés menetét, illetve a fejlesztőknek szóló útmutatást)

3. Biztonsági szabályzat

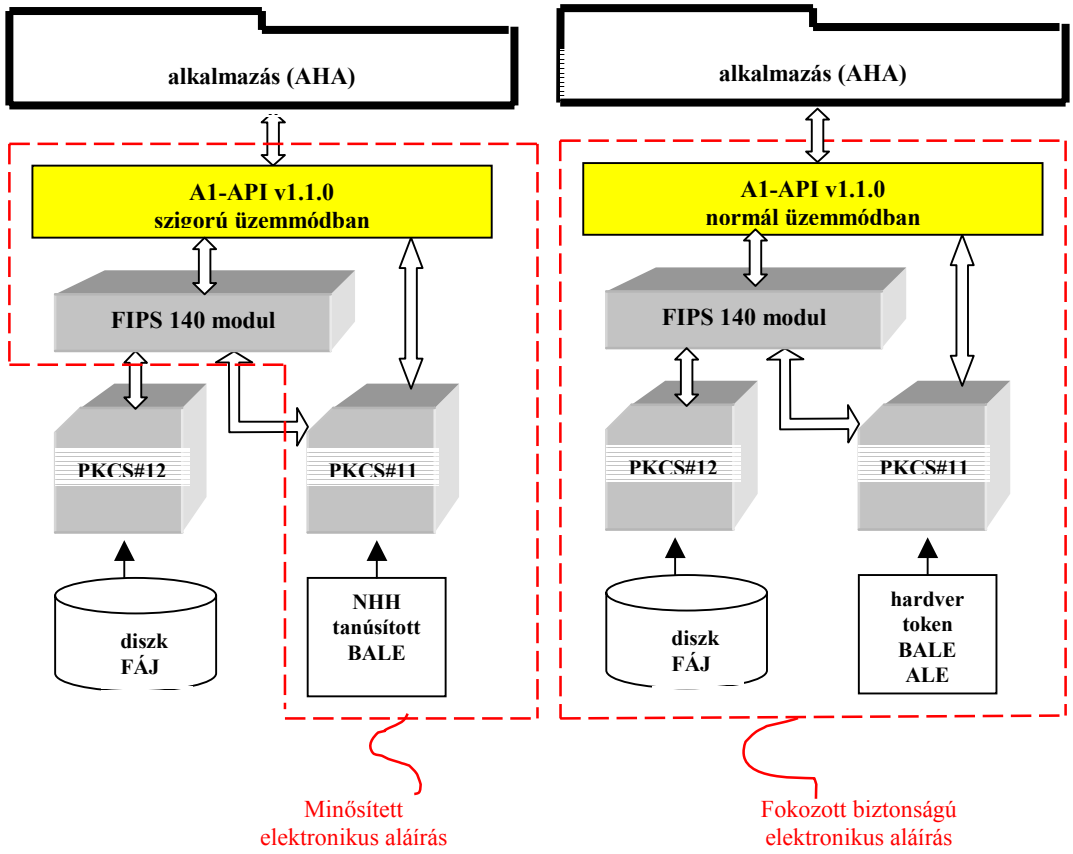
Ez a fejezet azokat a szabályokat írja le, melyek alapján az A1-API v1.1.0 irányítja az erőforrásaihoz való hozzáférést, s ezen keresztül minden általa ellenőrzött információt és szolgáltatást.

Először az A1-API v1.1.0 két üzemmódját határozzuk meg, melyekre eltérő szabályok vonatkoznak. Ezt követően a szabályokat érvényre juttató biztonsági funkciókat tekintjük át.

3.1 Üzemmódok

Az A1-Polysys CryptoSigno v1.1.0-nak két használati módja különböztethető meg:

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



1. ábra: Az A1-API v1.1.0 üzemmódjai

Mindkét üzemmód előfeltétele az alábbi:

- SUN JAVA JRE 1.5 vagy magasabb futtató környezet (benne egy PKCS#11 kompatibilis, FIPS 140 legalább 1-es szintjének megfelelő kriptográfiai szolgáltató modul).
  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.

A normál üzemmód kiegészítő előfeltétele:

- PKCS#12 vagy PKCS#11 kompatibilis kulcstároló

A szigorú üzemmód kiegészítő előfeltétele:

- PKCS#11 kompatibilis, tanúsított biztonságos aláírás létrehozó eszköz (BALE).

3.2 Biztonsági funkciók

Az A1-API v1.1.0-nek az alábbi nyolc biztonsági funkciója van:

BF1: Alap (SF.BASE)
Ez a biztonsági funkció az AHA számára biztosítja a modell létrehozásának, valamint a vezérlő megszerzésének a lehetőségét, valamint az A1-Polysys CryptoSigno v1.1.0 többi biztonsági funkciója számára belső támogatást, alapozást biztosít.

BF2: Inicializálás (SF.INIT)
Ez a biztonsági funkció biztosítja az A1-Polysys CryptoSigno v1.1.0 hitelességét, annak sértetlenségének és megváltozatlanságának fenntartását.

BF3: Azonosítás, hitelesítés és jogosultság ellenőrzés (SF.IAA)
Ez a biztonsági funkció kikényszeríti, hogy az AHA felhasználója, azaz az A1-Polysys CryptoSigno v1.1.0 szolgáltatásaihoz hozzáférést kérő személy sikeresen azonosítva, majd közvetlenül ezután (hitelesítő adatának megadásával) sikeresen hitelesítve legyen, valamint jogosultsága ellenőrzésre kerüljön, mielőtt engedélyezné az A1-Polysys CryptoSigno v1.1.0 valamely szolgáltatásának igénybe vételét.

BF4: Menedzsment (SF.MAN)
Ez a biztonsági funkció a biztonságot érintő jellemzők menedzsmentjét valósítja meg, az AHA számára lehetővé teszi:

- a PKI biztonsági jellemzők menedzsmentjét,
- az A1-Polysys CryptoSigno v1.1.0 működését befolyásoló biztonsági jellemzők menedzsmentjét,
- a biztonságot érintő jellemzők alapállapotának előidézését.

BF5: Tanúsítási útvonal érvényesítés (SF.CPV)
Ez a biztonsági funkció végzi:

- a tanúsítványok ellenőrzését,
- a tanúsítási útvonalak felépítését, majd annak érvényesség ellenőrzését.

BF6: Visszavonási információ érvényesítés (SF.CRL)
Ez a biztonsági funkció a visszavonási információk (CRL) érvényességét ellenőrzi.

BF7: Elektronikus aláírás létrehozása és ellenőrzése (SF.SIGSIV)
Ez a biztonsági funkció az alábbi két feladatkör végrehajtásra képes:

- a felhasználó aláíró magánkulcsának felhasználásával elektronikus aláírást, valamint azt kiegészítő aláírási információkat hoz létre,
- az elektronikus aláírást, valamint az azt kiegészítő aláírási információk érvényességét ellenőrzi az aláíró nyilvános kulcsát tartalmazó tanúsítványának felhasználásával.

BF8: Titkosítás és dekódolás (SF.ENCDEC)
Ez a biztonsági funkció az alábbi három feladatkör végrehajtására képes:

- a címzett(ek) titkosító nyilvános kulcsát tartalmazó tanúsítvány(ok) felhasználásával titkosítja a címzett(ek)nek továbbítandó információkat,
- a titkosított információkat az AHA felhasználó dekódoló magánkulcsának felhasználásával dekódolja,
- a titkosított információkat az AHA felhasználó dekódoló magánkulcsának felhasználásával dekódolja, majd egy megadott címzett számára újratitkosítja.

3.2.1 Alap biztonsági funkció (BF1, SF.BASE)

Ennek a biztonsági funkciónak az a fő célja, hogy az AHA számára lehetővé tegye a modell létrehozását. A modell birtokában az AHA megszerezheti az A1-API biztonsági politikáját érvényesítő vezérlőt. A vezérlő működik közre az A1-API szolgáltatásainak az AHA számára történő kiközvetítésében. Így ez a biztonsági funkció az A1-API összes biztonsági funkciójában közreműködik.

A biztonsági funkció az alábbi szolgáltatásokat nyújtja az AHA számára:

- modell létrehozása
- vezérlő megszerzése

A modell létrehozása az első kötelező lépés, amelyet az AHA-nak meg kell tennie ahhoz, hogy az A1-API szolgáltatásokat igénybe vehesse. Általában a modell létrehozása az első alkalom, amikor az AHA az A1-API-t megszólítja, ezért ha az még előzőleg nem történt meg, a BF2 biztonsági funkció inicializálási öntesztje automatikusan lefut. Így ez a biztonsági funkció függ a BF2 biztonsági funkciótól.

Ennek a biztonsági funkciónak az a célja, hogy az AHA szigorúan ellenőrzött módon megadhassa azokat az AHA-tól vagy környezettől függő információkat, melyek az A1-API számára bemenő adatok.

A modell létrehozása három fázisban történik:

- első (kötelező) fázis: az azonosításhoz, hitelesítéshez és jogosultság ellenőrzéshez használt hitelesítő kulcs elérését leíró információk és az általános adatok megadása,
- második (opcionális) fázis: az aláíró kulcs elérését leíró információk megadása,
- harmadik (opcionális) fázis: a dekódoló kulcs elérését leíró információk megadása.

A vezérlő megszerzése a második kötelező lépés, amelyet az AHA-nak meg kell tennie ahhoz, hogy az A1-API szolgáltatásokat igénybe vehesse. A vezérlőt az AHA a modell birtokában szerezheti meg. A vezérlő működik közre az A1-API lehetőségeknek az AHA által történő igénybe vételében, az A1-API biztonsági funkcióiban megnyilvánuló szolgáltatásoknak a kiközvetítésében.

3.2.2 Inicializálás biztonsági funkció (BF2, SF.INIT)

Ez a biztonsági funkció öntesztet hajt végre, amelynek fő feladata az A1-API hitelességének ellenőrzése, annak sértetlenségének és megváltozatlanságának fenntartása.

Használatának fő célja, hogy megakadályozza az A1-API-nak a szándékos megváltoztatását (rossz indulatú személyek általi beavatkozás) vagy nem szándékos megváltozását (az informatikai környezet hibájából adódó sérülés, adatvesztés).

Az inicializálási öntesztre akkor kerül sor, amikor az AHA először szólítja meg az A1-API-t.

A külső interfész egy látvány elem (GUI), amely a következő információkat jelzi vissza az AHA felhasználója számára: az A1-API megnevezése és verziószáma. A látvány elem mindaddig látható, amíg a biztonsági funkció az A1-API ellenőrzését (öntesztet) végzi.

Az önteszt során a biztonsági funkció az A1-API futtatható kódjának a csatolt elektronikus aláírását ellenőrzi.

3.2.3 Azonosítás, hitelesítés és jogosultság ellenőrzés biztonsági funkció (BF3, SF.IAA)

Ennek a biztonsági funkciónak az a fő feladata, hogy biztosítsa, hogy az A1-API szolgáltatásait csak az AHA azonosított, hitelesített és jogosult felhasználója, illetve egy annak nevében eljáró folyamat vehesse igénybe. A biztonsági funkció minden A1-API szolgáltatás igénybe vétele előtt és után működésbe lép. A biztonsági funkció a szolgáltatás kérésekor a folyamatot (annak felhasználóját) azonosítja, hitelesíti, majd jogosultságát ellenőrzi (IAA). A biztonsági funkció a sikeres IAA hatására a szolgáltatás igénybe vételét engedélyezi. A biztonsági funkció az IAA-t a szolgáltatás igénybe vétele után alapesetben lebontja.

Használatának fő célja, hogy a hozzáférést kérő személy (az AHA felhasználó) bizonyítsa, hogy birtokol egy olyan kulcstárolót, amelyben a személyes tanúsítványa és az ahhoz tartozó hitelesítő magánkulcsa rendelkezésre áll, és azokat használni tudja.

3.2.4 Menedzsment biztonsági funkció (BF4, SF.MAN)

Ennek a biztonsági funkciónak az a célja, hogy az AHA számára lehetővé tegye a következő biztonságot érintő információk menedzsmentjét:

- PKI biztonsági jellemzők,
- az A1-API működését befolyásoló biztonsági jellemzők,

valamint az AHA előidézhesse a jellemzők alapállapotát:

- biztonságot érintő jellemzők alapállapota.

A PKI biztonsági jellemzők a következők:

- tanúsítvány jellegű:
  - megbízható legfelső szintű hitelesítő tanúsítványok,
  - közbenső tanúsítványok,
  - saját tanúsítványok,
  - más személyek tanúsítványai,
- CRL jellegű:
  - visszavonási információk

A tanúsítvány jellegű PKI biztonsági jellemző menedzsment alfunkció a következő szolgáltatásokat nyújtja az AHA számára:

- egy tanúsítvány nyilvántartásba vétele,
- több tanúsítvány nyilvántartásba vétele,
- ismertség vizsgálat,
- tanúsítványok kikeresése,
- nyilvántartás méretének (tanúsítványok száma) lekérdezése,
- az összes tanúsítvány lekérdezése,
- egy tanúsítvány törlése a nyilvántartásból,
- több tanúsítvány törlése a nyilvántartásból
- a nyilvántartás üresítése.

A CRL jellegű biztonsági jellemző menedzsment alfunkció a következő szolgáltatásokat nyújtja az AHA számára:

- egy CRL nyilvántartásba vétele,
- több CRL nyilvántartásba vétele,
- ismertség vizsgálat,
- CRL-ek kikeresése,
- nyilvántartás méretének (CRL-ek száma) lekérdezése,
- az összes CRL lekérdezése,
- egy CRL törlése a nyilvántartásból,
- több CRL törlése a nyilvántartásból,
- a nyilvántartás üresítése.

Az A1-API működését befolyásoló biztonsági jellemzők a következők:

- a CRL a kibocsátást követő hány napig tekinthető aktuálisnak (CRLAfterThisUpdateLimit),
- a CRL a következő kibocsátási dátumot követő hány napig tekinthető aktuálisnak (CRLAfterNextUpdateLimit),
- a CRL frissesség ellenőrzés engedélyezése,
- visszavonás ellenőrzés kihagyásának engedélyezése,
- megbízható időszerverek,
- szolgáltatás igénybevétele után kikényszerített kijelentkeztetés engedélyezése.

Biztonságot érintő jellemzők alapállapota biztosításának az a célja, hogy a biztonsági jellemzőket egy alapértelmezett, kezdeti állapotba hozza. Az alapállapotok a következők:

- PKI biztonsági jellemzők
    - megbízható legfelső szintű tanúsítványok nyilvántartás: **üres állapot**
    - közbenső tanúsítványok nyilvántartás: **üres állapot**
    - saját tanúsítványok nyilvántartás: **üres állapot**
    - más személyek tanúsítványai nyilvántartás: **üres állapot**
    - visszavonási információk (CRL) nyilvántartás: **üres állapot**
- A1-API működését befolyásoló biztonsági jellemzők
    - CRLAfterThisUpdateLimit: **2 nap,**
    - CRLAfterNextUpdateLimit: **0 nap,**
    - a CRL frissesség ellenőrzés engedélyezése:„**true**”,
    - a visszavonás ellenőrzés kihagyásának engedélyezése:„**false**”,
    - megbízható időszerverek: **üres állapot,**
    - szolgáltatás igénybevétele után kikényszerített kijelentkeztetés engedélyezése: „**true**”.

3.2.5 Tanúsítási útvonal érvényesítés biztonsági funkció (BF5, SF.CPV)

Ennek a biztonsági funkciónak a célja kettős:

- az AHA számára tanúsítvány ellenőrzés, PKIX szabvány szerinti tanúsítási útvonal felépítés és érvényesítés szolgáltatások nyújtása,
- az A1-API biztonsági funkciók támogatása a tanúsítvány ellenőrzés, PKIX szabvány szerinti tanúsítási útvonal felépítés és érvényesítés ellenőrzésekkel.

A biztonsági funkció minden ellenőrzést a "megbízható időszerverek" biztonsági jellemző által meghatározott megbízható forrásból megszerzett pontos idővel, mint aktuális idővel végez.

Ez a biztonsági funkció az AHA, valamint a többi biztonsági funkció számára a következő szolgáltatásokat nyújtja:

- tanúsítvány ellenőrzés jellegű:
  - megbízható legfelső szintű tanúsítvány ellenőrzése,
  - közbenső tanúsítvány ellenőrzése,
  - végtanúsítvány (saját vagy más személy) ellenőrzése,
  - kulcshasználat ellenőrzése,
- tanúsítási útvonal felépítés és érvényesítés jellegű:
  - tanúsítási útvonal felépítése,
  - tanúsítási útvonal érvényesítése,
  - tanúsítási útvonal együttes felépítése és érvényesítése.

A tanúsítvány ellenőrzés célja, hogy az AHA, vagy az A1-API egy megadott tanúsítványt a típusának megfelelően az aktuális időpontra nézve ellenőrizhessen.
A tanúsítvány ellenőrzés jellegű alfunkciók által végzett ellenőrzések csak a megadott tanúsítványra vonatkoznak, a tanúsítási útvonal felépítését és érvényesítését nem foglalják magukban.
A biztonsági funkció minden tanúsítványtípus esetén érvénytelennek minősíti azokat a tanúsítványokat, amelyekben a tanúsítvány alanya mező (Subject Distinguished Name) hiányzik.

A megbízható legfelső szintű tanúsítvány ellenőrzése a következők ellenőrzését jelenti:

1. a kibocsátó és az alany azonos-e,
2. az érvényességi időtartam rendben van-e,
3. az önaláírt tanúsítványon az aláírás hiteles-e,
4. a tanúsítvány tartalmaz-e kritikus, nem támogatott kiterjesztést.

A közbenső tanúsítvány ellenőrzése a következők ellenőrzését jelenti:

1. az érvényességi időtartam rendben van-e,
2. a kibocsátó ismert-e a megbízható legfelső szintű tanúsítványok vagy a közbenső tanúsítványok nyilvántartásában,
3. a tanúsítványon a kibocsátó aláírása hiteles-e,
4. a tanúsítvány tartalmaz-e kritikus, nem támogatott kiterjesztést,
5. a tanúsítvány tartalmazza-e a kötelező basicConstraints kiterjesztést, és abban a cA flag be van-e állítva,
6. ha a tanúsítványban jelen van kritikus keyUsage kiterjesztés, akkor abban a keyCertSign bit be van-e állítva.

A végtanúsítvány ellenőrzése a következők ellenőrzését jelenti:

1. az érvényességi időtartam rendben van-e,
2. a kibocsátó ismert-e a megbízható legfelső szintű tanúsítványok vagy a közbenső tanúsítványok nyilvántartásában,
3. a tanúsítványon a kibocsátó aláírása hiteles-e,
4. a tanúsítvány tartalmaz-e kritikus, nem támogatott kiterjesztést.

A kulcshasználat ellenőrzése annak ellenőrzését jelenti, hogy a tanúsítvány keyUsage kiterjesztésében az alábbi táblázat szerinti bit be van-e állítva:

Művelet típus	**a keyUsage kiterjesztésben ellenőrzött bit**
hitelesítés	digitalSignature
aláírás létrehozása, aláírás ellenőrzése	nonRepudiation
titkosítás, dekódolás	keyEncipherment

Aláírás létrehozása és aláírás ellenőrzése művelet típus esetén az is ellenőrzésre kerül, hogy a keyUsage kiterjesztésben kizárólag csak a nonRepudiation bit van-e beállítva.

A tanúsítási útvonal felépítés és ellenőrzés jellegű alfunkciók célja, a megadott tanúsítványhoz a PKIX szabványnak megfelelően a tanúsítási útvonal felépítése és érvényesítése, az aktuális időpontban.

A tanúsítási útvonal felépítése funkciónak az a célja, hogy az AHA, vagy az A1-API meggyőződhessen arról, hogy a kérdéses tanúsítványhoz az aktuális időpontban az útvonal a PKIX szabványnak megfelelően felépíthető, és azt fel is építse. Az útvonal egy tanúsítvány lánc, amely a megbízható tanúsítvánnyal kezdődik, nulla vagy több közbenső tanúsítványokkal folytatódik, és a végtanúsítvánnyal végződik.
Ez a funkció használja a BF4 biztonsági funkció által menedzselt PKI jellemzőkből a tanúsítvány nyilvántartásokat.

A tanúsítási útvonal érvényesítése funkciónak az a célja, hogy az AHA, vagy az A1-API meggyőződhessen arról, hogy a kérdéses tanúsítványhoz az előzőleg a tanúsítási útvonal felépítése funkcióval felépített útvonal a PKIX szabványnak megfelelően érvényes-e az aktuális időpontban.
Ez a funkció használja a BF4 biztonsági funkció által menedzselt PKI jellemzőkből a visszavonási információ nyilvántartást, valamint az A1-API működését befolyásoló biztonsági jellemzők közül a "visszavonás ellenőrzés kihagyásának engedélyezése" jellemzőt.

A tanúsítási útvonal együttes felépítése és érvényesítése funkciónak az a célja, hogy az AHA, vagy az A1-API meggyőződhessen arról, hogy a kérdéses tanúsítványhoz az útvonal a PKIX szabványnak megfelelően felépíthető és érvényesíthető az aktuális időpontban.
Ez a funkció használja a BF4 biztonsági funkció által menedzselt PKI jellemzőkből a tanúsítvány és a visszavonási információ nyilvántartásokat, valamint az A1-API működését befolyásoló biztonsági jellemzők közül a "visszavonás ellenőrzés kihagyásának engedélyezése" jellemzőt.

3.2.6 Visszavonási információ érvényesítés biztonsági funkció (BF6, SF.CRL)

A biztonsági funkció célja kettős:
- az AHA számára visszavonási információ ellenőrzés szolgáltatás nyújtása,
- az A1-API biztonsági funkciók támogatása a visszavonási információk ellenőrzésével.

A biztonsági funkció minden ellenőrzést a "megbízható időszerverek" biztonsági jellemző által meghatározott megbízható forrásból megszerzett pontos idővel, mint aktuális idővel végez.
A biztonsági funkció az AHA, valamint a többi biztonsági funkció számára a következő szolgáltatásokat nyújtja:
- visszavonási lista (CRL) ellenőrzése.

A visszavonási lista (CRL) ellenőrzése funkciónak az a célja, hogy az AHA, vagy az A1-API egy megadott CRL érvényességét az aktuális időpontra nézve ellenőrizze.
A funkció használja a BF4 biztonsági funkció által menedzselt PKI jellemzőkből a tanúsítvány nyilvántartásokat, valamint az A1-API működését befolyásoló biztonsági jellemzők közül a "CRLAfterThisUpdateLimit", "CRLAfterNextUpdateLimit" és "a CRL frissesség ellenőrzés engedélyezése" jellemzőket.
A biztonsági funkció csak teljes (nem delta) CRL-t fogad el érvényesnek. Érvénytelennek minősíti azokat a CRL-eket, amelyek a következő kritikus kiterjesztések valamelyikét tartalmazzák:
- deltaCRLIndicatorExtension (2.5.29.27),
- issuingDistributionPointExtension (2.5.29.28).

A biztonsági funkció a megadott CRL-en a következő ellenőrzéseket végzi el:

1. érvényességi időtartam rendben van-e
   1.1. ellenőrzés időpontja > thisUpdate
   1.2. ha a CRL frissesség ellenőrzés engedélyezve van, akkor ellenőrzés időpontja <= thisUpdate + CRLThisUpdateLimit
   1.3. ha a CRL frissesség ellenőrzés engedélyezve van, akkor ellenőrzés időpontja <= nextUpdate + CRLNextUpdateLimit
2. a kibocsátó ismert-e a megbízható legfelső szintű tanúsítványok vagy a közbenső tanúsítványok nyilvántartásában
3. a CRL-en a kibocsátó aláírása hiteles-e
4. a CRL tartalmaz-e kritikus, nem támogatott kiterjesztést
5. ha a CRL kibocsátó tanúsítványában jelen van kritikus keyUsage kiterjesztés, akkor abban a keyCRLSign bit be van-e állítva

3.2.7 Elektronikus aláírás létrehozása és ellenőrzése biztonsági funkció (BF7, SF.SIGSIV)

Ennek a biztonsági funkciónak a következő két fő feladatköre van:

- az AHA felhasználó aláíró magánkulcsával elektronikus aláírás és kiegészítő aláírási információk létrehozása (elektronikus aláírás létrehozása),
- elektronikus aláírás és az azt kiegészítő aláírási információk ellenőrzése az aláíró tanúsítványának felhasználásával (elektronikus aláírás ellenőrzése).

A biztonsági funkció az elektronikus aláírás létrehozását és ellenőrzését az XMLDSIG szabvány és az XAdES szabvány XAdES-BES formátumának (továbbiakban szabványos XML formátum) megfelelően végzi.
A biztonsági funkció igénybe veszi a BF5 biztonsági funkció (tanúsítási útvonal felépítése és érvényesítése) alfunkcióját.

Az elektronikus aláírás létrehozása funkció igénybe veszi a BF3 biztonsági funkció (azonosítás, hitelesítés és jogosultság ellenőrzés) közreműködését az AHA felhasználónak az aláíró kulcsot tartalmazó kulcstárolóhoz történő bejelentkeztetéséhez. A funkció az aláírás időpontját a "megbízható időszerverek" biztonsági jellemző által meghatározott megbízható forrásból megszerzett pontos idővel képzi.

Minősített elektronikus aláírás előfeltétele a következő:

- az A1-API „szigorú” üzemmódja,
- az aláíró kulcs elérési információit az AHA megadta,
- a BF3 biztonsági funkció az AHA felhasználót az aláíró kulcsot tartalmazó kulcstárolóhoz sikeresen bejelentkeztette,
- a kulcstárolóban jelen levő, az aláíró kulcshoz tartozó tanúsítvány (aláírás létrehozásához használt tanúsítvány) minősített tanúsítvány.

Fokozott biztonságú elektronikus aláíráshoz:

- bejelentkezési látvány komponens megfelelő,
- az aláíró kulcs elérési információkat az AHA megadta,
- a BF3 biztonsági funkció az AHA felhasználót az aláíró kulcsot tartalmazó kulcstárolóhoz sikeresen bejelentkeztette.

Az elektronikus aláírás létrehozásának lépései az alábbiak:

- a bemenetként megadott adatok megfelelőségének ellenőrzése,
- a BF3 biztonsági funkció általi bejelentkeztetés az aláíró kulcsot tartalmazó kulcstárolóhoz, az aláíró tanúsítvány kiválasz(ta)tása, majd az aláíró tanúsítvány beolvasása,
- az aláíráshoz használt tanúsítványra a BF5 biztonsági funkció "tanúsítási útvonal felépítése és érvényesítése" alfunkciójával az útvonal felépítése és érvényesítése, úgy, hogy bemenő paraméterként „aláírás létrehozása” művelet típus van megadva,
- minősített elektronikus aláírás létrehozása esetén az aláírás létrehozásához használt tanúsítványban a kötelező qCStatements tanúsítvány kiterjesztés meglétének ellenőrzése,
- aláírási algoritmus (RSA-SHA1 vagy DSA-SHA1) kiválasztása az aláíró kulcs algoritmusának megfelelően,
- aláírást kísérő információk összeállítása a bemenő adatokból,
- az aláírás elkészítése az aláírandó tartalmakra és bemenő adatokkal és a pontos idővel mint aláírási időponttal, a BF3 biztonsági funkció által bejelentkeztetett aláíró kulcsot tartalmazó kulcstárolóból kiválasz(ta)tott aláírói magánkulccsal, a szabványos XML formátumban,
- az elkészített aláírás automatikus ellenőrzése, a BF5 biztonsági funkció "tanúsítási útvonal felépítése és érvényesítése" alfunkciójának kimenetéből származó nyilvános kulccsal,
- a szabványos XML formátum kimenetként történő visszaadása.

Az elektronikus aláírás ellenőrzése funkció az aláírás ellenőrzését a "megbízható időszerverek" biztonsági jellemző által meghatározott megbízható forrásból megszerzett pontos idővel, mint aktuális idővel végzi. Ez a funkció működéséhez igénybe veszi a BF5 biztonsági funkció "tanúsítási útvonal felépítése és érvényesítése" alfunkcióját.
Az elektronikus aláírás ellenőrzésének lépései az alábbiak:

- az aláírási formátum megfelelőségének a vizsgálata,
- az aláírást kísérő információkból az aláíró nyilvános kulcsának és tanúsítványának meghatározása,
- az aláíráshoz használt tanúsítványra a BF5 biztonsági funkció "tanúsítási útvonal felépítése és érvényesítése" alfunkciójával az útvonal felépítése és érvényesítése, úgy, hogy bemenő paraméterként „aláírás ellenőrzése” művelet típus van megadva,
- minősített elektronikus aláírás ellenőrzése esetén az aláírás létrehozásához használt tanúsítványban a kötelező qCStatements tanúsítvány kiterjesztés meglétének ellenőrzése,
- az URI-val hivatkozott aláírt tartalmak beolvasása,
- az aláírás ellenőrzése az aláírt tartalmakra vonatkozóan.

3.2.8 Titkosítás és dekódolás biztonsági funkció (BF8, SF.ENCDEC)

Ennek a biztonsági funkciónak az alábbi három fő feladatköre van:

- titkosítás (a címzett(ek) titkosító nyilvános kulcsát tartalmazó tanúsítvány(ok) felhasználásával titkosítja a címzett(ek)nek továbbítandó információkat),
- dekódolás (a titkosított információkat az AHA felhasználó visszafejtő magánkulcsának felhasználásával dekódolja),
- dekódolás és újratitkosítás (a titkosított információkat az AHA felhasználó visszafejtő magánkulcsának felhasználásával dekódolja, majd egy megadott címzett részére újratitkosítja).

Ez a funkció a működéséhez igénybe veszi a BF5 biztonsági funkció "tanúsítási útvonal felépítése és érvényesítése" alfunkcióját.

A titkosítás funkció két szolgáltatást nyújt az AHA számára:

- stream titkosítás,
- fájl titkosítás.

A titkosítás funkció a titkosítás időpontját a "megbízható időszerverek" biztonsági jellemző által meghatározott megbízható forrásból megszerzett pontos idővel, mint aktuális idővel tölti ki.

A titkosítás lépései az alábbiak:

- minden egyes címzett tanúsítványra, a BF5 biztonsági funkció "tanúsítási útvonal felépítése és érvényesítése" alfunkciójával az útvonal felépítése és érvényesítése, úgy, hogy bemenő paraméterként „titkosítás” művelet típus van megadva,
- 256 bites véletlen szimmetrikus AES titkos kulcs generálása,
- a titkos kulcs aszimmetrikus titkosítása RSA algoritmussal,
- minden egyes címzett számára a leíró információ létrehozása,
- az input stream vagy fájl tartalmára AES/256 szimmetrikus titkosítás elvégzése.

A dekódolás funkció két szolgáltatást nyújt az AHA számára:

- stream dekódolás,
- fájl dekódolás.

A dekódolás funkció a BF3 biztonsági funkció közreműködését veszi igénybe az AHA felhasználónak a dekódoló kulcsot tartalmazó kulcstárolóhoz történő bejelentkeztetéséhez.

A dekódolás előfeltételei az alábbiak:

- bejelentkezési látvány komponens megfelelősége,
- a visszafejtő kulcs elérési információkat az AHA megadta,
- a BF3 biztonsági funkció az AHA felhasználót a visszafejtő kulcsot tartalmazó kulcstárolóhoz sikeresen bejelentkeztette.

A dekódolás lépései az alábbiak:

- a titkosítási formátum megfelelőségének ellenőrzése,
- annak ellenőrzése, hogy az AHA felhasználójának, a BF3 biztonsági funkció által bejelentkeztetett dekódoló kulcshoz tartalmazó kulcstárolóból beolvasott dekódoló tanúsítványa szerepel-e a titkosítás címzettjei között,
- a visszafejtő tanúsítványra, a BF5 biztonsági funkció "tanúsítási útvonal felépítése és érvényesítése" alfunkciójával az útvonal felépítése és érvényesítése, úgy, hogy bemenő paraméterként „dekódolás” művelet típus van megadva,
- a leíró információból a visszafejtő tanúsítvánnyal rendelkező felhasználó számára csomagolt AES kulcs kicsomagolása, a BF3 biztonsági funkció által bejelentkeztetett, dekódoló kulcsot tartalmazó kulcstárolóból a dekódoló magánkulccsal,
- az AES/256 szimmetrikus dekódolás elvégzése, egyidejűleg a dekódolt tartalomra lenyomat képzés,
- a leíró információból a nyílt tartalomra képzett lenyomat kiolvasása, és annak egyezőségének vizsgálata a dekódolt tartalomra képzett lenyomattal.

A dekódolás és újratitkosítás funkció egy kényelmi szolgáltatás az AHA számára, amely a dekódolás és a titkosítás funkciók egymást követő alkalmazása, azzal a különbséggel, hogy itt csak egy címzett adható meg. A funkció célja az, hogy az AHA felhasználója a dekódolt információt egy olyan címzett számára újratitkosítsa, aki eredetileg nem szerepelt a titkosítás címzettjei között.

A funkció a titkosítás időpontját a "megbízható időszerverek" biztonsági jellemző által meghatározott megbízható forrásból megszerzett pontos idővel, mint aktuális idővel tölti ki.

A dekódolás és újratitkosítás előfeltételei megegyeznek a dekódolás előfeltételeivel.

A dekódolás és újratitkosítás lépései a dekódolás és a titkosítás lépéseiből áll.

4. Feltételezések és hatókör

Az A1-API v1.1.0 egy fejlesztő készlet, melynek segítségével szabványos PKI szolgáltatásokat biztosító alkalmazásokat lehet fejleszteni.

Az A1-API v1.1.0 elsődleges felhasználója a fejlesztő készletet felhasználó alkalmazások fejlesztője. Ugyanakkor az A1-API v1.1.0 szolgáltatása alapvetően a vele fejlesztett alkalmazásokban fog érvényre jutni. Ezért az A1-API v1.1.0 másodlagos felhasználójaként a ráépülő alkalmazások használói (akik valószínűleg felhasználói és adminisztrátori szerepkörökbe lesznek szétválasztva) is megjelennek majd.

A fentiekhez hasonlóan Az A1-API v1.1.0 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.

4.1 Feltételezések az A1-API v1.1.0 informatikai környezetére

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

1. A jogosult felhasználók megbízhatóak a számukra kijelölt funkciók végrehajtására.
2. Az A1-API v1.1.0 helyesen van telepítve és konfigurálva.
3. Az A1-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 képzés (SHA-1 algoritmussal), véletlenszám generálás.
4. Az A1-API v1.1.0 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 modult, 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 A1-API v1.1.0 szembeni támadási potenciált alacsonynak tételezzük fel.
6. Az informatikai környezet gondoskodik a fizikai védelemről, így az A1-API v1.1.0 szoftver elemei jogosulatlan fizikai hozzáférés ellen védettek.
7. Az A1-API v1.1.0 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.

Az alábbi (a biztonsági előirányzatban nem szereplő) feltételezések az informatikai környezet egy-egy speciális elemére vonatkoznak:

11. Szigorú üzemmód esetén (minősített aláírás létrehozásához) az A1-API fejlesztő készlettel készített aláíró alkalmazáshoz olyan PKCS#11 driver-t kell alkalmazni, amely képes egy megbízható útvonalat kiépíteni a BALE-vel, s ezzel biztosítani a BALE-nek továbbított, aláírót 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 kell alkalmazni, 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 A1-API fejlesztő készlettel készített alkalmazásnak kell megvalósítania.

4.2 Feltételezések az A1-API v1.1.0 biztonságos használatára

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

1. A felhasználónak biztosítania kell a rendszeridő megfelelő pontosságát. A rendszeridőt a lehető legpontosabban 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) 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.

4.3 Feltételezések az A1-API v1.1.0 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 az A1-API v1.1.0 informatikai környezetére vonatkozó biztonsági követelmények (lásd 4.1) is szerepeljenek.
2. Az alkalmazás útmutató dokumentumaiban az A1-API v1.1.0 biztonságos használatára vonatkozó feltételezések (lásd 4.2) 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,
   - megbízható időszerverek megadása,
   - a biztonságot érintő jellemzők alapállapota.
4. Az alkalmazás telepítési eljárását úgy kell kialakítani, hogy az magában foglalja az A1-API v1.1.0 megfelelő telepítését is.
5. Az A1-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):
   - a CRL a kibocsátást követő hány napig aktuális,
   - a CRL a következő kibocsátási dátumot követő hány napig aktuális,
   - 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 A1ApiControl 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, ismételje meg az aláírás ellenőrzését a visszavonás ellenőrzés bekapcsolt állapotával.
8. Az alkalmazás használata során a visszavonási lista (CRL) frissesség ellenőrzése legyen bekapcsolva (lásd A1ApiControl 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, ismételje 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 A1ApiControl 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 A1ApiControl osztály, serviceSetCRLAfterThisUpdateLimit és serviceSetCRLAfterNextUpdateLimit metódusok).
11. Az alkalmazás futása során, az azonosítás/hitelesítés-hez tartozó tanúsítványhoz a tanúsítási útvonal felépítését és érvényesítését (lásd A1ApiControl osztály, serviceCheckIAACertificate metódus) a lehető leghamarabb el kell végezni.

4.4 Az értékelés hatóköre

Az értékelés figyelembe vette a biztonsági előirányzat valamennyi fenyegetését és az A1-API v1.1.0 valamennyi biztonsági funkcióját.

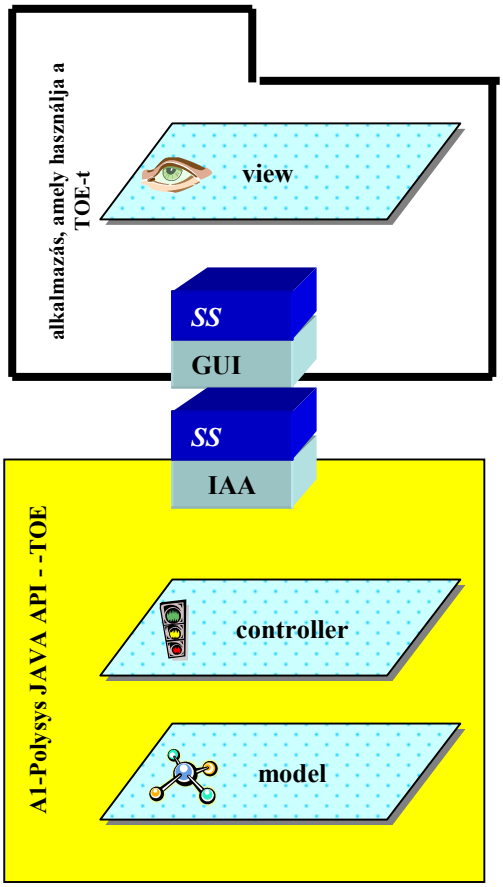
5. *Az A1-Polysys CryptoSigno v1.1.0 szerkezeti leírása*

Az alábbiak megadják és röviden jellemzik az A1-Polysys CryptoSigno v1.1.0 logikailag elkülöníthető fő szerkezeti összetevőit.

5.1 Architektúra

Az A1-Polysys CryptoSigno v1.1.0 architektúrája a Model-Controller-View (MCV) paradigmán alapul:

- a modell (model) leírja egy objektum állapotát
- a vezérlő (controller) képes az objektum állapotának megváltoztatására
- a látvány (view) megjeleníti az objektum állapotát



2. ábra: Az A1-Polysys CryptoSigno v1.1.0 architektúrája

Az A1-Polysys CryptoSigno v1.1.0 az MCV paradigma modell és vezérlő részét teljes egészében, a látvány részét csak a szükséges mértékben fedi le. A látvány jelentős részének a megvalósítása az AHA feladata. Az A1-Polysys CryptoSigno v1.1.0-ban a látványból megvalósított rész az a grafikus felhasználói felület (bejelentkező ablak), amely a szigorú üzemmódban kötelezően használandó az AHA felhasználójának azonosításához, hitelesítéséhez és jogosultságának ellenőrzéséhez szükséges információk bekéréséhez.

Az AHA a modell létrehozásával, majd az érvényes modell alapján megszerzett, az A1-Polysys CryptoSigno v1.1.0 biztonsági politikáját érvényesítő vezérlő közvetítésével veheti igénybe az A1-Polysys CryptoSigno v1.1.0 szolgáltatásait.

5.2 Alrendszerek

Az A1-Polysys CryptoSigno v1.1.0-nek az alábbi öt alrendszere van:

AR1: Azonosítás, hitelesítés és jogosultság ellenőrzés alrendszer (SS.IAA)
Ez az alrendszer az AHA felhasználójának, azaz az A1-Polysys CryptoSigno v1.1.0 szolgáltatásaihoz hozzáférést kérő személy, valamint az annak nevében eljáró folyamatok (AHA folyamat) azonosítását, hitelesítését és jogosultság ellenőrzését, valamint az AHA felhasználójának az aláíró és visszafejtő kulcsot tartalmazó kulcstárolóhoz történő bejelentkeztetését végzi.
Közreműködik az alábbi biztonsági funkció megvalósításában:

- BF3 (Azonosítás, hitelesítés és jogosultság ellenőrzés).

AR2: Felhasználói interfész alrendszer (SS.GUI)
Ez az alrendszer az azonosítás, hitelesítés és jogosultság ellenőrzés során a szükséges információknak (azonosító és hitelesítő adatok) a felhasználótótól való bekéréséhez szükséges látványt, valamint az AHA felhasználójának az aláíró és visszafejtő kulcsot tartalmazó kulcstárolóhoz történő bejelentkeztetéséhez szükséges látványt valósítja meg.
Közreműködik az alábbi biztonsági funkció megvalósításában:

- BF3 (Azonosítás, hitelesítés és jogosultság ellenőrzés).

AR3: AHA interfész alrendszer (SS.SERVICE)
Ez az alrendszer az A1-Polysys CryptoSigno v1.1.0 szolgáltatásait valósítja meg.
Megvalósítja az alábbi biztonsági funkciókat:

- BF1 (Alap)
- BF2 (Inicializálás)
- BF4 (Menedzsment)
- BF5 (Tanúsítási útvonal érvényesítés)
- BF6 (Visszavonási információ érvényesítés)
- BF7 (Elektronikus aláírás létrehozása és ellenőrzése)
- BF8 (Titkosítás és dekódolás)

AR4: Kriptográfiai alrendszer (SS.CRYPTO)
Ez az alrendszer kezeli az A1-Polysys CryptoSigno v1.1.0 és a kriptográfiai szolgáltató modul közötti kommunikációt.
Közreműködik az alábbi biztonsági funkciók megvalósításában:

- BF2 (Inicializálás)
- BF3 (Azonosítás, hitelesítés és jogosultság ellenőrzés)
- BF5 (Tanúsítási útvonal érvényesítés)
- BF6 (Visszavonási információ érvényesítés)
- BF7 (Elektronikus aláírás létrehozása és ellenőrzése)
- BF8 (Titkosítás és dekódolás)

AR5: SCDEV alrendszer (SS.SCDEV)
Ez az alrendszer kezeli az A1-Polysys CryptoSigno v1.1.0 és az aláírás-létrehozó eszköz (hardver token, ALE vagy BALE) közötti kommunikációt.
Közreműködik az alábbi biztonsági funkciók megvalósításában:

- BF3 (Azonosítás, hitelesítés és jogosultság ellenőrzés)
- BF7 (Elektronikus aláírás létrehozása és ellenőrzése)
- BF8 (Titkosítás és dekódolás)

6. Dokumentáció

Az értékelt termék alkotó elemei (a felhasználókhoz, vagyis a fejlesztő készlet felhasználásával alkalmazást fejlesztőkhöz kiszállított tételek) az alábbiak:

1. **a1-api-BIN-1_1_0.jar** (a fejlesztéshez szükséges fájlok)
2. **a1-api-DOC-1_1_0.jar** (JavaDoc dokumentációja)
3. **A1-Polysys_SG_Support_Guide.pdf** (támogató dokumentáció)

Az a1-api-BIN-1_1_0.jar az A1-API v1.1.0-et felhasználó fejlesztésekhez szükséges fájlokat tartalmazza. A fájl tartalmának részletezését, valamint kifejtésének módját az A1-Polysys_SG_Support_Guide.pdf dokumentum tartalmazza.

Az a1-api-DOC-1_1_0.jar az A1-API v1.1.0, valamint a teszt esetek JavaDoc dokumentációját tartalmazza. A fájl tartalmának részletezését, valamint kifejtésének módját az A1-Polysys_SG_Support_Guide.pdf dokumentum tartalmazza.

Az A1-Polysys_SG_Support_Guide.pdf dokumentum bemutatja az A1-API v1.1.0 fejlesztő készletet, tartalmazza az adminisztrátori és felhasználói útmutatást, leírja az A1-API v1.1.0 telepítését megelőzően elvégzendő teendőket, a telepítés menetét, illetve a fejlesztőknek szóló útmutatást.

7. Tesztelés

Az A1-API v1.1.0 fejlesztése során a fejlesztők által kialakított és alkalmazott tesztek három csoportba sorolhatóak:

- PKITS (Public Key Interoperability Public Key Interoperability Test Suite) típusú tesztek
  Automatikusan futtatható tesztrendszer, mely a NIST "Recommendation for X.509 Path Validation" (version 0.5, May 2004) dokumentációban meghatározott 224 teszttel a tanúsítási útvonal felépítését és érvényesítését ellenőrzi, gyakorlatilag teljes körűen, minden reálisan szóba jöhető (224 darab) eset figyelembe vételével.
- funkcionális tesztek
  Automatikusan futtatható tesztrendszer, mely az értékelés tárgyának SS.GUI alrendszerén kívül, az összes többi alrendszert (s ezen keresztül az ezek által támogatott biztonsági funkciókat) teszteli, nagy számú (314 darab) tesztesettel.
- kiegészítő tesztek
  Egy példa alkalmazás segítségével elvégezhető (manuális) tesztrendszer, mely az értékelés tárgya SS.GUI alrendszerének látvány elemeit teszteli.

A fejlesztők különböző platformokon leteszteltek az A1-API v1.1.0 biztonsági funkcióit, az eredményeket pedig részletesen dokumentálták.

A fejlesztők által végzett tesztelésről az értékelők megállapították, hogy:

- minden biztonsági funkciót és ezek minden külső interfészét tesztelték,
- minden alrendszert és ezek minden belső interfészét tesztelték,

így megfelel mind a tesztelés lefedettségére, mind pedig a tesztelés mélységére vonatkozó elvárásoknak.

A fejlesztők a fentieken kívül egy olyan eszközt is alkalmaztak a teszteléshez, mely mérte, hogy a teszt sorozat során az egyes metódusok hányszor kerültek meghívásra, illetve a kód sorokat alkotó utasítások hányszor kerültek végrehajtásra. Ezzel bizonyítékot szolgáltattak arra, hogy (a fokozott garanciaszint teszt lefedettségre és teszt mélységre vonatkozó elvárásain túl) a fejlesztő készletet rendkívül alapossággal tesztelték le. (összesített lefedettségi eredmény: 96,7%).

A fejlesztők tesztelésre átadták az értékelőknek az A1-API v1.1.0 futtatható változatát és automatizált teszt rendszerét, egyúttal saját környezetükben és harmadik helyen is biztosították a közös tesztelést.

Az értékelők független tesztelést végeztek az értékelés tárgyára (a fejlesztőknél, saját tesztkörnyezetükben, illetve harmadik félnél is). Az alkalmazott tesztkonfigurációk különbözők voltak, annak megfelelően, hogy a biztonsági előirányzat deklarálja az értékelés tárgyának platform függetlenségét.

Mivel a fejlesztők automatizálták és gyakorlatilag teljes körűvé tették a tesztelést, ezért az értékelők által végzett független tesztelésre úgy került sor, hogy (miután a rendelkezésükre bocsátott dokumentációk alapján telepítették az A1-API v1.1.0-t és teszt rendszerét) az értékelők különböző platformokon futtatták a teljes tesztrendszert, majd a kapott (automatikusan generált) részletes eredményeket elemezték.

A független tesztelés eredményei megfeleltek a várakozásoknak (a tapasztalt tényleges eredmények megegyeztek a teszt tervben szereplő elvárt eredményekkel).

8. Az értékelt konfiguráció

Az A1-API v1.1.0 egy olyan fejlesztő készlet (könyvtár), amely platform független, Java technológiával készülő alkalmazások számára nyújt támogatást, különböző PKI szolgáltatások biztosításához.

Az értékelés eredményei különböző platformokon és különböző konfigurációban lettek ellenőrizve, tesztelve.

Tesztelt platformok[2]:

	operációs rendszer	alap	hardver
1	Sun Solaris 9	1.5.0 verziójú JAVA	1 darab Ultra Sparc Iii 300MHz-es processzor, 256 MB RAM memória
2	Suse Linux 9.0 Professional	1.5.0 verziójú JAVA	2 darab Pentium II 400 MHz-es processzor, 512 MB RAM memória
3	Microsoft Windows 2000 SP4	1.5.0 verziójú JAVA	1 darab Pentium IV 2,8 GHz-es processzor, 1 GB RAM memória
4	JavaDesktop	1.5.0 verziójú JAVA	4 darab Xeon 3 GHz-es processzor, 3 GB RAM memória
5	Microsoft Windows XP Professional SP1	1.5.0 verziójú JAVA	1 darab Pentium III 936 MHz-es processzor, 512 MB RAM memória
6	Suse Linux Enterprise Server 9	1.5.0 verziójú JAVA	2 darab Xeon 2.5 GHz-es processzor, 2 GB RAM memória (IBM eServerX365 xSeries számítógép)
7	Suse Linux Professional 9.2 (kernel: 2.6.8-24)	1.5.0 verziójú JAVA	1 darab 1.7 GHz-es Mobil Pentium 4-es processzor, 1 GB RAM memória (IBM T41 ThinkPad laptop)
8	RedHat Advanced Server 3 SP3 Linux	1.4.2 verziójú JAVA	1 darab 1.9 GHz-es POWER5-ös processzor, 2 GB RAM memória (IBM eServer P570 pSeries /RS6000/ számítógép)
9	RedHat Advanced Server 3 SP3 Linux	1.4.2 verziójú JAVA	egy darab 1.7 GHz-es POWER5-ös processzor, 1 GB RAM memória (IBM eServer I520 iSeries /AS400/ számítógép)

Tesztelt PKCS#11-es hardver aláírás-létrehozó eszközök:

	eszköz	operációs rendszer	chip
1	Aladdin e-Token PRO	CardOS/M4.01	SLE66CX320P
2	Oberthur CosmopolIC intelligens kártya	nyílt Java platform 2.1 V4 verzió	P8WE5033V0G
3	ORGA intelligens kártya	MICARDO v2.1	SLE66CX320P

Tesztelt üzemmódok:

	üzemmód	alkalmazhatóság[3]
1	szigorú	minősített elektronikus aláírás létrehozására
2	normál	fokozott biztonságú elektronikus aláírás létrehozására

[2] Valamennyi tesztelés a hu.polysys.api.a1.test csomagjának összes (538 darab) tesztjét érintette.

[3] Mindkét üzemmód alkalmazható a többi funkcionalitásra (aláírás ellenőrzése, titkosítás és dekódolás, tanúsítási útvonal felépítése és érvényesítése, tanúsítvány visszavonási listák ellenőrzése, azonosítás, hitelesítés és jogosultság ellenőrzés)

9. Az értékelés eredményei

Az A1-Polysys CryptoSigno JAVA API v1.1.0 fejlesztő készlet a MIBÉTS (Magyar Informatikai Biztonsági Értékelés és Tanúsítási Séma) módszertana szerint független értékelésre és tanúsításra került, fokozott garanciaszinten.

Az értékelés megállapította, a tanúsítás pedig megerősítette, hogy **az A1-Polysys CryptoSigno JAVA API v1.1.0 megfelel a biztonsági előirányzatának, kielégíti az abban megfogalmazott funkcionális és garanciális biztonsági követelményeket.**

A fenti megállapítás a fokozott garanciaszint (EAL3+) követelményeinek teljesítésén alapul. Az alábbi táblázat azt mutatja meg, hogy az egyes garanciaösszetevőket hogyan teljesíti az A1-Polysys CryptoSigno JAVA API v1.1.0 fejlesztő készlet, illetve mely fejlesztői bizonyítékok támogatták ennek kimutatását.

Garancia-osztály	Garancia-összetevő	A követelmények kielégítésének módja, /s az ezt leíró fejlesztői bizonyíték/
Konfiguráció menedzselés	ACM_CAP.3	A futtatható kódot automatizált eszköz (Jedit és Ant fejlesztőeszközök build scriptje) generálja, címkézi és teszteli. A dokumentum típusú konfigurációs tételekre jól kidolgozott kézi eljárásokat használnak. /Konfigurációkezelés dokumentáció v1.0/
	ACM_SCP.1	A konfiguráció menedzselés az alábbi tételekre, azok teljes életciklusára biztosítja a változások azonosítható és ellenőrizhető megvalósítását: terv dokumentációk, támogató dokumentációk, teszt dokumentációk, fejlesztői útmutató, forráskód, futtatható kód. /Konfigurációkezelés dokumentáció v1.0/
Kiszállítás és működtetés	ADO_DEL.1	Az A1-API v1.1.0-t becsomagolt CD-n vagy PenDrive-on juttatják el a felhasználókhoz, vagy Java WebStart technológia alkalmazásával on-line módon lehet azt letölteni. Minden esetben biztosított a módosítások megelőzése, észlelése, a letöltés esetén (digitális aláírás alkalmazása miatt) a forrás hitelesítése is. /A kiszállítás eljárásai v1.0/
	ADO_IGS.1	Útmutató segíti az A1-API v1.1.0 telepítését, illetve az ezt megelőző és az ezt követő teendőket. /Támogató dokumentáció v1.0 (3.-5. fejezetek)/

Fejlesztés	ADV_FSP.1	A funkcionális specifikáció az A1-API v1.1.0 biztonsági funkcióinak magas szintű leírása. Részletezi mindazokat a külső interfészeket, amelyekkel az A1-API v1.1.0-t használó alkalmazás a fejlesztő készletet felhasználhatja, annak szolgáltatásait, lehetőségeit igénybe veheti. Leírja a külső interfészek használatának célját és módszerét, kellő részletességgel megadja a bemeneteket, kimeneteket, a hatások, következmények és hibaüzenetek részleteit. /Funkcionális specifikáció v1.0/
	ADV_HLD.2	Az A1-API v1.1.0 funkcionális specifikációját egy magas-szintű terv finomítja. Ebben a biztonsági funkciókat megvalósító alrendszerek, illetve az alrendszerek közötti belső interfészek kerülnek kellő részletességgel meghatározásra. /Magas szintű terv v1.0/
	ADV_RCR.1	A különböző részletességű terv dokumentációk kölcsönös megfelelése szöveges indoklásra és ábrákkal való szemléltetésre kerül. /Teszt lefedettség és mélység elemzés v1.0 (2. fejezet)/
Útmutató dokumentumok	AGD_ADM.1 AGD_USR.1	Az A1-API v1.1.0 telepítője (adminisztrátor) és felhasználója egyaránt a fejlesztő. A fejlesztő számára készített támogató dokumentáció: • leírja az A1-API v1.1.0 informatikai környezetére vonatkozó biztonsági követelményeket, a biztonságos üzemeltetés szempontjából lényeges feltételezéseket és felhasználói felelősségeket. • leírja a telepítéshez szükséges ismereteket, • összefoglalja az A1-API v1.1.0 rendelkezésre álló funkcióit és interfészeit, • részletezi az A1-API v1.1.0 biztonsági funkciók külső interfészeit, leírja a külső interfészek használatának célját és módszerét, kellő részletességgel megadja a bemeneteket, kimeneteket, a hatások, következmények és hibaüzenetek részleteit, • leírja az A1-API v1.1.0 alrendszereit, megadja a biztonsági funkciók és alrendszerek összefüggéseit, • bemutatja az A1-API v1.1.0-t a megvalósítás szintjén, • leírja az A1-API v1.1.0 helytelen használatát kísérő jelenségeket, azok következményeit, a gyakori hibákat és elhárításuk módját. A Fejlesztői útmutató leírja az A1-API-t alkotó Java osztályok és metódusok pontos részleteit, valamint használatuk módját. /Támogató dokumentáció v1.0/ /Fejlesztői útmutató v1.0 (a1-api-DOC-1_1_0.jar)/
Az életciklus támogatása	ALC_DVS.1	Az A1-API v1.1.0 fejlesztésének biztonságát különböző fizikai, eljárásbeli, személyi és egyéb biztonsági intézkedések garantálják. /Konfigurációkezelés dokumentáció v1.0 (7. fejezet)/
	ALC_FLR.1	Kidolgozott (és a jövőben alkalmazott) eljárások biztosítják, hogy az A1-API a későbbi módosításait követően is megtartsa az értékelés és tanúsítás során bizonyított minőségét, változatlan részeibe a módosítás során hiba nem kerüljön, a javított vagy továbbfejlesztett részek pedig megfelelően teszteltek legyenek. /Módosítás menedzsment v1.0/

Tesztelés	ATE_COV.2	Részletes teszt tervek készültek a biztonsági funkciók és azok külső interfészeinek tesztelésére. A tesztek és eredményeinek ismertetése kiegészül egy teszt lefedettségi elemzéssel, mely kimutatja, hogy a biztonsági funkciók a funkcionális specifikációnak megfelelően kerültek tesztelésre. /Teszt lefedettség és mélység elemzés v1.0 (3. és 4. fejezetek)/
	ATE_DPT.1	Részletes teszt tervek készültek az alrendszerek és azok belső interfészeinek tesztelésére. A tesztek és eredményeinek ismertetése kiegészül egy teszt mélység elemzéssel, mely kimutatja, hogy a biztonsági funkciók a magas-szintű tervnek megfelelően kerültek tesztelésre. /Teszt lefedettség és mélység elemzés v1.0 (3. és 5. fejezetek)/
	ATE_FUN.1	Az A1-API v1.1.0 különböző platformokon és különböző aláíró eszközzel került tesztelésre, összhangban a biztonsági előirányzat azon állításaival, hogy a fejlesztő készlet platform független, s együtt tud működni különböző (PKCS#11 kompatibilis) aláíró eszközzel. /Tesztelési dokumentáció v1.0/
	ATE_IND.2	A fejlesztők tesztelésre átadták az értékelőknek az A1-API v1.1.0 futtatható változatát és automatizált teszt rendszerét, egyúttal saját környezetükben és harmadik helyen is biztosították a közös tesztelést.
A sebezhetőség felmérése	AVA_MSU.1	A fejlesztők egy "útmutatás vizsgálata" című elemzést készítettek, mely kimutatja, hogy: • a különböző útmutatók az alkalmazás fejlesztőknek megadnak minden szükséges információt a biztonságos használatra vonatkozóan, egyben • nem mondanak ellent a csak az értékelőknek átadott egyéb fejlesztői bizonyítékoknak sem. /Sebezhetőség elemzés v1.0 (2. fejezet)/
	AVA_SOF.1	A fejlesztők kimutatták, hogy az A1-API v1.1.0 nem alkalmaz olyan biztonsági mechanizmust, melyre funkcióerősséget kellene állítaniuk. /Sebezhetőség elemzés v1.0 (3. fejezet)/
	AVA_VLA.1+	A fejlesztő egy sebezhetőség elemzést készített, melyben azonosította az A1-API v1.1.0 nyilvánvaló sebezhetőségi pontjait, egyúttal kimutatta, hogy a megvalósított különböző (megelőző, észlelő és javító) ellenintézkedések, valamint a környezetre tett feltételezések eredményeként, ezeket a sebezhetőségeket a tervezett környezetben nem lehet kihasználni. /Sebezhetőség elemzés v1.0 (4.-5. fejezetek)/

10. Értékelői megjegyzések és javaslatok

Az értékelt termék alábbi tulajdonságai különös fontossággal bírhatnak:

10.1 Platform függetlenség

Az A1-API v1.1.0 egy platform független fejlesztő készlet, mely a ráépülő, Java technológiával készülő alkalmazások számára nyújt különböző támogatásokat.

Az értékelés eredményei különböző platformokra érvényes, 9 különböző operációs rendszeren lett sikeresen tesztelve (lásd 8. fejezet).

10.2 Mintaszerű fejlesztői bizonyítékok

Az A1-API v1.1.0 értékelés az első olyan hazai értékelés, mely teljes mértékben a MIBÉTS séma értékelési módszertanát alkalmazta.

Ennek egyik előfeltétele az volt, hogy a fejlesztők mindenben a MIBÉTS fokozott (lényegében a CC EAL3+) garanciaszintjének megfelelő bizonyítékokat szolgáltassanak az értékeléshez. Ezt az előfeltételt a fejlesztők mintaszerűen, példa értékűen teljesítették.

10.3 Alapos tesztelés

A egész fejlesztő készletben kritikus fontossággal bíró tanúsítási útvonal felépítésre és érvényesítésre nézve, a fejlesztők megvalósították a NIST által kidolgozott, gyakorlatilag teljes körű ellenőrzést biztosító, automatikus tesztrendszert.

Ezen kívül egy olyan eszközt is alkalmaztak a teszteléshez, mely mérte, hogy a teszt sorozat során az egyes metódusok hányszor kerültek meghívásra, illetve a kód sorokat alkotó utasítások hányszor kerültek végrehajtásra. Ezzel bizonyítékot szolgáltattak arra, hogy (a fokozott garanciaszint teszt lefedettségre és teszt mélységre vonatkozó elvárásain túl) a fejlesztő készletet rendkívül alapossággal tesztelték le. (összesített lefedettségi eredmény: 96,7%).

Az alábbi javaslat az A1-API v1.1.0 fejlesztő készlet iránt érdeklődő alkalmazás fejlesztőknek szól.

10.4 A biztonsági előirányzat megismerése

Az A1-API v1.1.0 fejlesztő készlet iránt érdeklődő alkalmazás fejlesztők tanulmányozzák át a teljes biztonsági előirányzatot is. A biztonsági előirányzat a fejlesztőktől szerezhető be.

11. Mellékletek

A 9. fejezetben foglaltak szerint az értékelés döntően annak megállapítására irányult, hogy az értékelés tárgya kielégíti-e a biztonsági előirányzatban megfogalmazott funkcionális és garanciális biztonsági követelményeket.

Az A1-API fejlesztő készletre (mint elektronikus aláírás létrehozásának és ellenőrzésének megvalósítására felhasználható elektronikus aláírási termékre) ugyanakkor az alábbi két nemzetközi követelményrendszer is vonatkozik:

- CEN/ISSS/E-Sign 14170:2004 CEN Workshop Agreement: Security requirements for signature creation applications /May 2004/
- CEN/ISSS/E-Sign 14171:2004 CEN Workshop Agreement: General guidelines for electronic signature verification /May 2004/

A fenti dokumentumokban megfogalmazott funkcionális és biztonsági követelményeknek való megfelelőséget külön is vizsgálta az értékelés, melynek módszere a következő volt:
Az értékelés az egyes követelményekre külön-külön határozatot hozott, hogy az alábbiakból melyik vonatkozik az adott követelményre:

- megfelel,
- nem felel meg,
- nem vonatkozik rá a követelmény,
- feltétellel megfelel.

Egyetlen követelményre sem születhet "nem megfelel" határozat, mert ez az egész értékelés tárgyára nézve "nem megfelelt" eredménnyel járna.

A "feltétellel megfelel" határozat olyan feltételt támaszt (nem az értékelés tárgyára, hanem annak működtetési környezetére, vagy egy kiegészítő termékre), melynek kielégítése szükséges az értékelés tárgyának jövőbeli biztonságos használathoz.

Az egyes követelményekre meghozott határozatok az alábbiak alapján születhetnek:

- interjú: a fejlesztőkkel való személyes konzultációk során kapott információk alapján,
- dokumentáció: a fejlesztők által készített írásos dokumentációk alapján,
- tapasztalat: a program felhasználói felületének működtetése, illetve a tesztelés során szerzett „felhasználói” tapasztalatokból leszűrt következtetések alapján,
- teszt: az értékelők által végzett tesztelés eredményei alapján,
- forrás kód: a fejlesztők által átadott forráskód értékelők általi elemzése alapján.

A fent leírt külön vizsgálatnak a következtetése az alábbi:

Az A1-Polysys CryptoSigno JAVA API v1.1.0 minősített elektronikus aláíráshoz fejlesztő készlet (a fejlesztő készlet működtetési környezetére, valamint a PKCS#11 kezelőre és PKCS#11 driver-re vonatkozó feltételek teljesülése esetén) **megfelel a CEN CWA 14170 és CEN CWA 14171 által az elektronikus aláíró alkalmazásokra támasztott valamennyi olyan funkcionális és garanciális biztonsági követelménynek, mely a fejlesztő készletre vonatkozik.**

Mivel az értékelés 9. fejezetben megfogalmazott fő következtetése ettől látszólag független állítást fogalmaz meg, így indoklásra szorul.

A jelen tanúsítási jelentés alapját képező értékelés egy olyan biztonsági előirányzatból indult ki, mely a korábbi hazai (aláíró alkalmazások támogatását megvalósító fejlesztő készletekre vonatkozó) értékelésektől eltérően nem a CWA 14170 és CWA 14171 mértékadó követelményrendszer általános, hanem egy tanúsított védelmi profilon (PKE-PP) alapuló, az A1-API v1.1.0-ra vonatkozó konkrét követelményrendszert határozza meg az értékelés viszonyítási alapjaként. Ez teljes mértékben összhangban van a MIBÉTS (és a CC) módszertanával, ugyanakkor nem teszi összehasonlíthatóvá a jelen értékelés eredményét a korábbi értékelési eredményekkel.

Tovább nehezíti az értékelés eredményének értelmezhetőségét, hogy tudomásunk szerint a fejlesztők (átmenetileg, versenyelőnyük megtartása érdekében) nem kívánják publikálni biztonsági előirányzatukat.

A fentiek indokolják, hogy a biztonsági előirányzatnak való megfelelés mellett (ami az értékelés fő következtetése), megfogalmazásra került a CEN követelményeknek való megfelelőség is.

A két következtetés nincs ellentmondásban egymással, kiegészítik egymást.

Az alábbiak (táblázatos formában) a CEN követelményeknek való megfelelésre vonatkozó vizsgálat eredményét foglalja össze.

/A táblázatokban szereplő "feltétellel megfelelt" teljesülés egy-egy olyan feltételre vonatkozik, melyek szerepelnek a 4.1 alfejezet, az A1-API v1.1.0 informatikai környezetére vonatkozó feltételei között./

11.1 Megfelelés a CEN CWA 14170 és 14171 funkcionális követelményeinek

Funkcionális követelmény	Teljesülés
F_SCA_1	megfelel
F_SDP_1	nem vonatkozik rá a követelmény
F_SDP_2	nem vonatkozik rá a követelmény
F_SDP_3	nem vonatkozik rá a követelmény
F_SDP_4	nem vonatkozik rá a követelmény
F_SAV_1	megfelel
F_SAV_2	megfelel
F_SIC_1	nem vonatkozik rá a követelmény
F_SIC_2	nem vonatkozik rá a követelmény
F_SIC_3	megfelel
F_DTBSF_1	megfelel
F_DTBSF_2	megfelel
F_DHC_1	megfelel
F_DHC_2	megfelel
F_SSC_1	megfelel
F_SSC_2	megfelel
F_SSC_3	megfelel
F_SSC_4	megfelel
F_SSC_5	nem vonatkozik rá a követelmény
F_SSC_6	nem vonatkozik rá a követelmény
F_SSC_7	feltétellel megfelel
F_SSC_8	megfelel
F_SSC_9	nem vonatkozik rá a követelmény
F_SSA_1	nem vonatkozik rá a követelmény
F_SDC_1	nem vonatkozik rá a követelmény
F_SDOC_1	megfelel
F_SLC_1	nem vonatkozik rá a követelmény
F_SCPC_1	nem vonatkozik rá a követelmény
F_I/O-1	nem vonatkozik rá a követelmény
F_I/O-2	megfelel
F_I/O-3	megfelel
F_ISV-1	megfelel
F_ISV-2	megfelel
F_USV-1	megfelel
F_human_1	nem vonatkozik rá a követelmény
F_human_2	nem vonatkozik rá a követelmény
F_human_3	nem vonatkozik rá a követelmény
F_human_4	megfelel
F_human_5	nem vonatkozik rá a követelmény
F_human_6	nem vonatkozik rá a követelmény
F_machine_1	megfelel
F_machine_2	megfelel
F_general_1	nem vonatkozik rá a követelmény
F_protocol	megfelel
F_format	megfelel
F_principles	nem vonatkozik rá a követelmény

11.2 Megfelelés a CEN CWA 14170 és 14171 biztonsági követelményeinek

Biztonsági követelmény	Teljesülés
Bizt_köv1	feltétellel megfelel
Bizt_köv2	feltétellel megfelel
Bizt_köv3	megfelel
Bizt_köv4	megfelel
Bizt_köv5	nem vonatkozik rá a követelmény
Bizt_köv6	nem vonatkozik rá a követelmény
Bizt_köv7	megfelel
Bizt_köv8	megfelel
Bizt_köv9	nem vonatkozik rá a követelmény
Bizt_köv10	nem vonatkozik rá a követelmény
Bizt_köv11	feltétellel megfelel
Bizt_köv12	megfelel
Bizt_köv13	megfelel
Bizt_köv14	megfelel
Bizt_köv15	megfelel
Bizt_köv16	megfelel
Bizt_köv17	megfelel
Bizt_köv18	nem vonatkozik rá a követelmény
Bizt_köv19	nem vonatkozik rá a követelmény
Bizt_köv20	nem vonatkozik rá a követelmény
Bizt_köv21	nem vonatkozik rá a követelmény
Bizt_köv22	nem vonatkozik rá a követelmény
Bizt_köv23	nem vonatkozik rá a követelmény
Bizt_köv24	nem vonatkozik rá a követelmény
Bizt_köv25	nem vonatkozik rá a követelmény
Bizt_köv26	megfelel
Bizt_köv27	megfelel
Bizt_köv28	nem vonatkozik rá a követelmény
Bizt_köv29	megfelel
Bizt_köv30	megfelel
Bizt_köv31	megfelel
Bizt_köv32	nem vonatkozik rá a követelmény
Bizt_köv33	nem vonatkozik rá a követelmény
Bizt_köv34	nem vonatkozik rá a követelmény
Bizt_köv35	nem vonatkozik rá a követelmény
Bizt_köv36	feltétellel megfelel
Bizt_köv37	feltétellel megfelel
Bizt_köv38	megfelel
Bizt_köv39	feltétellel megfelel
Bizt_köv40	megfelel
Bizt_köv41	megfelel
Bizt_köv42	feltétellel megfelel
Bizt_köv43	feltétellel megfelel
Bizt_köv44	megfelel
Bizt_köv45	feltétellel megfelel
Bizt_köv46	nem vonatkozik rá a követelmény
Bizt_köv47	nem vonatkozik rá a követelmény
Bizt_köv48	megfelel
Bizt_köv49	megfelel
Bizt_köv50	megfelel
Bizt_köv51	megfelel
Bizt_köv52	megfelel

Bizt_köv53	feltétellel megfelel
Bizt_köv54	megfelel
Bizt_köv55	feltétellel megfelel
Bizt_köv56	nem vonatkozik rá a követelmény
Bizt_köv57	feltétellel megfelel
Bizt_köv58	feltétellel megfelel
Bizt_köv59	nem vonatkozik rá a követelmény
Bizt_köv60	feltétellel megfelel

11.3 A tanúsított termékek listájába javasolt szöveg

Jelenleg még nincs tanúsított termékek listája. Amennyiben lenne ilyen lista, abba az alábbi szöveg felvételét javasolnánk:

"Az A1-Polysys CryptoSigno JAVA API API minősített elektronikus aláíráshoz v1.1.0 egy olyan platform független fejlesztő készlet, mely a ráépülő, Java technológiával készülő alkalmazások számára támogatást nyújt:

- *minősített vagy fokozott biztonságú elektronikus aláírás létrehozására és ellenőrzésére,*
- *titkosításra és ennek dekódolására,*
- *tanúsítási útvonal felépítésére és érvényesítésére,*
- *tanúsítvány visszavonási listák ellenőrzésére,*
- *azonosításra, hitelesítésre és jogosultság ellenőrzésre*

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

Az A1-Polysys CryptoSigno JAVA API API minősített elektronikus aláíráshoz v1.1.0 fejlesztő készlet a MIBÉTS (Magyar Informatikai Biztonsági Értékelés és Tanúsítási Séma) módszertana szerint független értékelésre és tanúsításra került a Közös szempontrendszer [MSZ ISO/IEC 15408:2002]-nek való megfelelőség szempontjából, fokozott (EAL3+) garanciaszinten. Az értékelés megállapította, a tanúsítás pedig megerősítette, hogy az A1-Polysys CryptoSigno JAVA API minősített elektronikus aláíráshoz v1.1.0 megfelel a biztonsági előirányzatának, kielégíti az abban megfogalmazott funkcionális és garanciális biztonsági követelményeket."

12. Biztonsági előirányzat

Az A1-API v1.1.0 fejlesztő készlet biztonsági előirányzata egy különálló dokumentum, amely a fejlesztőktől szerezhető be.

13. Fogalmak és rövidítések

13.1 Fogalmak

Az alábbiakban meghatározzuk a jelen tanúsításban használt (nem nyilvánvaló) fogalmak jelentését.

A1-API
Az A1-Polysys CryptoSigno JAVA API minősített elektronikus aláíráshoz fejlesztőkészlet.

biztonsági előirányzat
Biztonsági követelmények és előírások olyan összessége, amelyet valamilyen adott tárgy értékelésének alapjaként használnak.

biztonsági funkció
Az értékelés tárgyának olyan része vagy részei, amelyben meg kell bízni ahhoz, hogy a vonatkozó biztonsági szabályzatból egy szorosan összefüggő szabályhalmaznak érvényt lehessen szerezni.

biztonsági jellemző
Szubjektumokkal, használókkal és/vagy objektumokkal társított olyan információ, amelyet az értékelés tárgyára vonatkozó biztonsági szabályzat érvényre juttatására használnak.

biztonsági szabályzat
Szabályok olyan összessége, amely szabályozza a vagyontárgyak kezelését, védelmét, elosztását az értékelés tárgyán belül.

dekódolás
Az A1-API dokumentációiban PKI, hibrid kulcsátviteli algoritmusokkal történő dekódolást (visszafejtést) jelent.

értékelés
A biztonsági előirányzat, illetve az értékelés tárgyának felmérése meghatározott szempontrendszer (pl. a CC vagy a MIBÉTS módszertana) alapján.

értékelés tárgya
Az az informatikai termék vagy rendszer valamint a hozzá kapcsolódó adminisztrátori és használati útmutatók, amelyre az értékelés irányul.

értékelési garanciaszint
A CC. 3 rész olyan garanciaösszetevőiből álló csomag, amelyek egy-egy pontot képviselnek a CC előre meghatározott garanciális skáláján.

értékelési séma
Olyan igazgatási és szabályozási keret, amely szerint az értékelő szervezet egy adott közösségben alkalmazza a CC-t.

értékelő szervezet
Az a testület, amely egy adott közösség keretein belül az úgynevezett értékelési séma révén valósítja meg a CC-t.

felhasználó, AHA felhasználó
A személy, aki az A1-API-t használó alkalmazást, az AHA-t használja, azaz az A1-API szolgáltatásait igénybe kívánja venni.

frissesség, a CRL frissességének ellenőrzése
Az az eljárás, amely elbírálja, hogy egy megadott CRL thisUpdate és nextUpdate mezőinek az értéke bizonyos megszorításoknak eleget tesz-e.

funkcióerősség
Az értékelés tárgya valamelyik biztonsági funkciójának minősítése, amely azt fejezi ki, hogy minimálisan mekkora erőkifejtést tartanak szükségesnek az elvárt biztonsági működés legyőzéséhez a mögöttes biztonsági mechanizmusok közvetlen megtámadása esetén.

felhasználó alkalmazás, AHA
Az A1-API-t használó, annak szolgáltatásait igénybe vevő alkalmazás, amely platform független JAVA technológiával van megvalósítva.

hitelesítő adat
Az az információ, amely a felhasználó állítólagos személyazonosságát igazolja.

időszerver, megbízható időszerver
Egy SNTP protokollal megszólítható, az AHA folyamat által megadott időszerver, amelytől a pontos idő meg lesz szerezve.

ismertség vizsgálat
Annak vizsgálata, hogy egy megadott elem egy bizonyos nyilvántartásban szerepel-e.

kulcs, aláíró kulcs
Elektronikus aláírás létrehozásához használt magánkulcs.

kulcs, hitelesítő kulcs
Az azonosításhoz, hitelesítéshez és jogosultság ellenőrzéséhez használt magánkulcs.

kulcs, dekódoló kulcs
Dekódoláshoz használt magánkulcs.

kulcstároló
Kulcsot tároló hardver eszköz (token, PKCS#11, ALE, BALE), vagy titkosítással védett kulcsot tároló fájl (PKCS#12).

látvány
A Model-Controller-View paradigma látvány összetevője, egy objektum állapotának vizuális megjelenítése.

látvány elem
A látvány valamely eleme.

MCV paradigma
Az a tervezési minta, amely a modell (model), a vezérlő (control) és a látvány (view) összetevőként azonosítja és különíti el egy rendszer elemeit.

modell
A Model-Controller-View paradigma modell összetevője, egy objektum állapotának leírása.

önteszt
A BF2, INIT biztonsági funkció által végzett önellenőrzés, amely az A1-API hitelességének, sértetlenségének és megváltozatlanságának vizsgálatára irányul, és amely akkor fut le, amikor az AHA először megszólítja az A1-API-t.

összetevő
Valamely csomag, védelmi profil vagy biztonsági előirányzat számára választható elemek legkisebb összessége.

PKI biztonsági jellemzők
Az A1-API dokumentációiban a tanúsítványok és visszavonási információk (CRL) együttes megnevezése.

PKI biztonsági jellemzők, menedzsment
A BF4, MAN biztonsági funkció által nyújtott szolgáltatások, amelyek segítségével az AHA, illetve annak felhasználója a PK biztonsági jellemzők nyilvántartásait ellenőrzött módon karban tarthatja.

tanúsítási útvonal felépítése
Egy tanúsítványhoz a tanúsítvány lánc kialakítása, úgy, hogy minden tanúsítványt az azt kibocsátó hitelesítés szolgáltató tanúsítványa kövessen. A tanúsítvány lánc a megbízható legfelső szintű tanúsítvánnyal kezdődik, ezt nulla vagy több közbenső tanúsítvány követi, és a végtanúsítvánnyal végződik.

tanúsítási útvonal érvényesítése
A tanúsítási útvonalat érvényesíteni kell, mielőtt a végtanúsítvány hitelessége elfogadásra kerülne. A tanúsítási útvonal érvényesítése a tanúsítási útvonalban szereplő minden egyes tanúsítványra a PKIX szabvány szerint előírt ellenőrzések elvégzését jelenti.

tanúsítvány, megbízható legfelső szintű tanúsítvány
Olyan önaláírt tanúsítvány, amely nem igényel tanúsítási útvonal érvényesítést. A tanúsítvány láncban az első helyen szerepel.

tanúsítvány, közbenső tanúsítvány
Olyan, hitelesítés szolgáltató számára kiadott tanúsítvány, amely a tanúsítvány láncban nem az első és nem az utolsó helyen szerepel.

tanúsítvány, lejárt
Olyan tanúsítvány, melynek a notAfter értéke korábbi, mint az aktuális időpont. A lejárt tanúsítvány szerepel vagy nem szerepel a tanúsítvány visszavonási listában (CRL).

tanúsítvány, saját tanúsítvány
Az AHA felhasználó számára kiadott végtanúsítvány.

tanúsítvány, más személy tanúsítványa
Olyan személy számára kiadott végtanúsítvány, aki az AHA felhasználójával kapcsolatban áll.

tanúsítvány, végtanúsítvány
Olyan, általában személyes tanúsítvány, amely a tanúsítvány láncban az utolsó helyen szerepel.

tanúsítvány, visszavont
Olyan tanúsítvány, amely már nem használható vagy nem megbízható. A hitelesítés-szolgáltató, amely a tanúsítvány kibocsátotta, a tanúsítványt különféle okokból vonhatja vissza. Az okok között szerepel a kulcs feltételezett vagy tényleges kompromittálódása, a tanúsítvány alanynak távozása az adott szervezettől, stb. A tanúsítvány visszavonási lista tartalmazza az összes visszavont és még nem lejárt tanúsítványt. Opcionálisan a tanúsítvány visszavonási lista tartalmazhat visszavont és már lejárt tanúsítványokat is.

tanúsítvány lánc
A tanúsítási útvonal felépítése során keletkező, tanúsítványokból álló sorozat, amelyben az első helyen egy megbízható legfelső szintű tanúsítvány áll, azt opcionális közbenső tanúsítványok követnek, az utolsó helyen egy végtanúsítvány szerepel.

tanúsítvány visszavonási lista (CRL, Certificate Revocation List)
Azoknak a visszavont tanúsítványoknak a felsorolása, amelyeket már nem használhatóak vagy nem megbízhatóak. Általában a hitelesítés szolgáltató, amely a tanúsítványt kibocsátotta, adja ki a CRL-t. A tanúsítvány visszavonási listát a kibocsátó elektronikus aláírással látja el.

termék
Informatikai szoftver, förmver és/vagy hardver által alkotott csomag, amely adott használatra vagy különböző rendszerekbe való beépítésre tervezett funkciókészletet szolgáltat.

titkosítás
Az A1-API dokumentációiban PKI, hibrid kulcsátviteli algoritmusokkal történő titkosítást jelent.

üzemmód
Az A1-Polysys CryptoSigno JAVA API üzemmódja. Az A1-API-t két üzemmódban használhatja az AHA, normál vagy szigorú üzemmódban.

üzemmód, normál
Az A1-Polysys CryptoSigno JAVA API-nak a fokozott biztonságú elektronikus aláírás létrehozására alkalmas üzemmódja.

üzemmód, szigorú
Az A1-Polysys CryptoSigno JAVA API-nak a minősített elektronikus aláírás létrehozására alkalmas üzemmódja.

vezérlő
A Model-Controller-View paradigma vezérlő összetevője, amely az objektum állapotát képes megváltoztatni. Az A1-API-ban az értékelés tárgya biztonságpolitikáját érvényesítő vezérlés.

védelmi profil
Megvalósítástól független, olyan biztonsági követelményrendszer az értékelés tárgyainak egy kategóriájára, amely adott fogyasztói igényeket elégít ki.

XAdES
Az XMLDSIG szabvány továbbfejlesztése, az EU elektronikus aláírásra vonatkozó (1999/93/EC) direktívája szerint.

XMLDSIG
XML elektronikus aláírás szintaktikáját és feldolgozását leíró szabvány.

13.2 Rövidítések

Az alábbiakban meghatározzuk a jelen tanúsításban használt betűszavak jelentését.

AHA	Az A1-Polysys CryptoSigno JAVA **A**PI-t **h**asználó **a**lkalmazás rövidített megnevezése
AES	Advanced Encryption Standard
ALE	Aláírás-létrehozó eszköz
API	Application Programming Interface
AR	**Al**rendszer
BALE	Biztonságos aláírás-létrehozó eszköz
BF	Biztonsági funkció
CC	Common Criteria (Közös szempontok)
CEN	Comité Europeen de Normalization (Európai Szabványügyi Bizottság)
CRL	Certificate Revocation List (tanúsítvány visszavonási lista)
CWA	CEN Work Agreement (CEN munka megállapodás)
DTBS	Data to be Signed (aláírandó adat)
DTBSF	Data to be Signed Formatter (aláírandó adat formattáló)
EAL	Evaluation Assurance Level (értékelési garanciaszint)
ETSI	European Telecommunication Standard Institute
FIPS	Federal Information Processing Standard
IT	Információ technológia
JRE	Java Runtime Environment (Java futtató környezet)
MCV	Model-Controller-View paradigma (model-vezérlő-látvány paradigma)
MIBÉTS	Magyar Informatikai Biztonsági és Értékelési Séma
PKCS	Public Key Cryptography Standard
PKCS#11	Cryptographic Token Interface Standard
PKCS#12	Personal Information Exchange Information Standard
PKI	Public Key Infrastructure
RSA	Rivest, Shamir, and Adleman (az RSA algoritmus)
SHA-1	Secure Hash Algorithm
SS	**Subs**ystem
TOE	Target of Evaluation (az értékelés tárgya)
XAdES	**X**ML **Ad**vanced **E**lectronic **S**ignature (XML formátumú elektronikus aláírás)
XML	E**x**tensible **M**arkup **L**anguage
XMLDSIG	**XML-D**igital **Sig**nature Syntax and Processing

14. Felhasznált dokumentumok

14.1 Az értékeléshez felhasznált kiinduló dokumentumok

- 2001. évi XXXV. törvény az elektronikus aláírásról
- 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 - V2.5 - 2002.10.31/

14.2 Az értékeléshez felhasznált fejlesztői bizonyítékok

Az értékelés az alábbi, fejlesztők által készített bizonyítékokat használta fel:

- Biztonsági előirányzat v1.0
- Funkcionális specifikáció v1.0
- Magas szintű terv v1.0
- Teszt lefedettség és mélység elemzés v1.0
- Tesztelési dokumentáció v1.0
- Konfigurációkezelés dokumentáció v1.0
- Módosítás menedzsment v1.0
- A kiszállítás eljárásai v1.0
- Támogató dokumentáció v1.0
- Fejlesztői útmutató v1.0 /a1-api-DOC-1_1_0.jar/
- Sebezhetőség elemzés v1.0
- Melléklet v1.0

14.3 Az értékeléshez felhasznált módszertani anyagok

Az értékelés az alábbi dokumentumokban leírt módszertant és eljárásrendet követte:

- 1. számú MIBÉTS kiadvány: A MIBÉTS nemzeti séma általános modellezése /0.9 verzió, 2003 augusztus/,
- 2. számú MIBÉTS kiadvány: Az értékelés és a tanúsítás folyamatai /0.9 verzió, 2003 szeptember/,
- 3. számú MIBÉTS kiadvány: Az értékelés módszertana 1 - A biztonsági előirányzat értékelésének módszertana /0.9 verzió, 2003 október/,
- 3. számú MIBÉTS kiadvány: Az értékelés módszertana 3 - A fokozott garanciaszint értékelésének módszertana /0.9 verzió, 2003 október/,

14.4 Az értékeléshez felhasznált egyéb dokumentumok

Az értékelés figyelembe vette az alábbi mértékadó követelményrendszereket is:

- 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)