Tanúsítási Jelentés

A2-Polysys CryptoSigno JAVA API for Qualified Electronic Signature and Seal v2.5.0

mint informatikai biztonsági funkciókat megvalósító szoftver termék

HUNG-TJ-MIBÉTS-014-2018

Digitálisan aláírta: HUNGUARD

Verzió:	1.0
Fájl:	HUNG-TJ-MIBETS-014-2018_v10.pdf
Minősítés:	Nyilvános
Oldalak:	16

Változáskezelés

Verzió	Dátum	A változás leírása
v0.1	2018.12.10.	A szerkezet felállítása
v0.2	2018.12.18.	Belső egyeztetésre kiadott verzió
v0.9	2018.12.21.	Külső egyeztetésre kiadott verzió
v1.0	**2018.12.28.**	**Végleges verzió**

A Tanúsítási Jelentést készítette:

dr. Szabó István
HUNGUARD Kft.
Tanúsítási divízió

Tartalom

I. Összefoglaló

I.1. A tanúsítás (és az értékelés, melyen a tanúsítás alapul) jellemzői

TOE név:	**A2-Polysys CryptoSigno JAVA API for Qualified Electronic Signature and Seal**
TOE rövid neve:	A2-Polysys CryptoSigno Interop JAVA API
TOE verzió:	v2.5.0
Fejlesztő:	Polysys Kft. 1162 Budapest, Margitháza u. 1.
Értékelő:	HUNGUARD Kft. Értékelési Divízió 1123 Budapest, Kékgolyó u. 6.
Értékelés befejezése:	2018. december 17.
Az értékelés módszere:	MIBÉTS:2009
Az értékelés garanciaszintje:	Fokozott (EAL3)

I.2. A tanúsítás tárgya

Az A2-Polysys CryptoSigno Interop JAVA API egy platform független JAVA technológiát alkalmazó szoftverfejlesztő készlet (könyvtár), ami a ráépülő alkalmazások számára támogatást nyújt az alábbiakhoz:

- minősített vagy fokozott biztonságú elektronikus aláírások és bélyegzők 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.

I.2.1. A TOE szolgáltatásainak összefoglalása

I.2.1.1. Elektronikus aláírás / bélyegző készítés és ellenőrzés

A TOE elektronikus aláírás / bélyegző készítés és ellenőrzést végez az alábbi formátumokban:

- XML-Signature Syntax and Processing (XMLDSIG)
- XML Advanced Electronic Signature (XAdES) v1.2.2, v1.3.2, v1.4.1, v1.4.2, valamint ezek Baseline Profile változatai
- ETSI EN 319 132 v1.1.1 (2016-04) szerinti XAdES, valamint ennek Baseline Profile változata
- Egységes MELASZ formátum elektronikus aláírásokra” v1.0, v2.0 formátum.

Elektronikus aláírás vagy bélyegző készítésekor a XAdES BES, EPES, T, vagy C formátumát támogatja. Azokat az ellenőrzés folyamatában T, C, X, X-L vagy A formátumra képes kibővíteni. Az elektronikus

aláírásokhoz időbélyeget kér egy hitelesítés szolgáltatótól és azt ellenőrzi az RFC 3161 szabványnak megfelelően. A tanúsítványlánc érvényesítéséhez OCSP kérést állít elő és küld az OCSP válaszadó felé, valamint az OCSP választ ellenőrzi az RFC 2560, illetve 6960 szabványnak megfelelően.

I.2.1.2. Titkosítás és visszafejtés

A TOE képes hibrid típusú (PKI kulcs továbbítás algoritmus és szimmetrikus algoritmus kombinációjával) titkosítás és visszafejtés funkciókra. Szimmetrikus rejtjelezésre az AES256 algoritmust, míg a titkos kulcs védelmére RSA2048 algoritmust alkalmaz.

I.2.1.3. Tanúsítványok és visszavonási információk érvényesítése

A TOE "PKIX, Internet X.509 Public Key Infrastructure Certificate and Certificate Revocation List Profile" (RFC 5280). szabvány szerint építi fel és érvényesíti a tanúsítvány láncot, felhasználva mind a CRL alapú, mind az OCSP alapú visszavonási információkat.

I.2.1.4. Azonosítás, hitelesítés feljogosítás

A TOE PKI alapú azonosítás, hitelesítés és feljogosítás szolgáltatást nyúlt a Java Authentication and Authorization Service (JAAS) architektúrának megfelelően.

I.2.1.5. TOE üzemmódok

Az A2-Polysys CryptoSigno Interop JAVA API-nak két használati módja különböztethető meg:

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

I.3. A TOE biztonsági környezete és határai

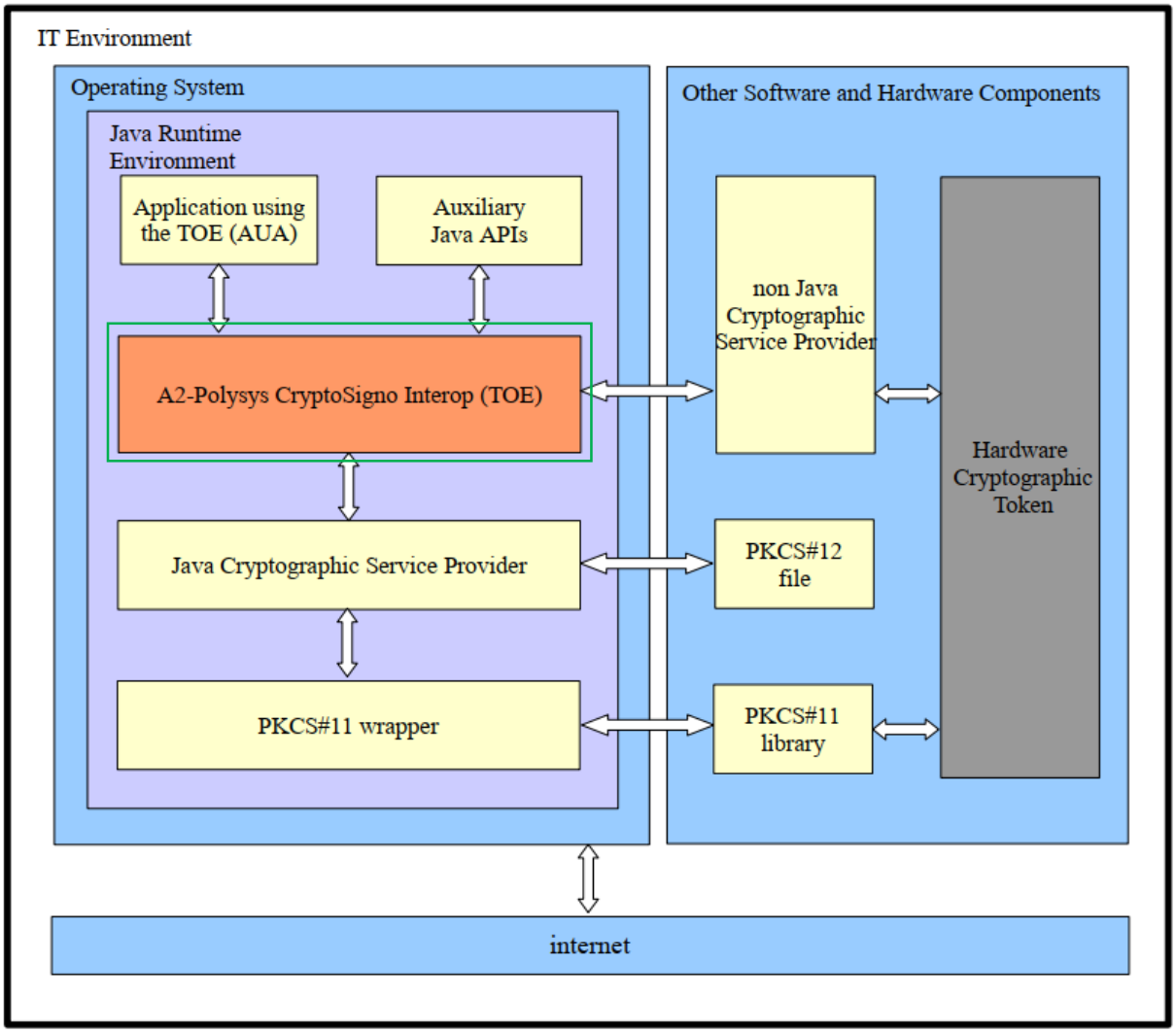
A TOE működőképességéhez Java futtató környezetre van szükség. A TOE bármely hardver vagy operációs rendszer környezetben képes működni, amennyiben az előírt Java verzió azt támogatja és kielégíti a biztonsági előirányzatban megfogalmazott környezeti biztonsági célokban leírtakat (lásd továbbá jelen dokumentum IV.1 fejezetét). A tanúsítás során tesztelt környezetek a III.1.5 fejezetben azonosítottak.

Szigorú üzemmódban a TOE elvárja a működési környezetében megfelelően telepített és konfigurált QSCD jelenlétét. Normál üzemmódban a TOE használható különböző megfelelően telepített és konfigurált hardver alapú aláírás létrehozó eszközzel. Ezen eszközöknek, legyen az intelligens kártya vagy HSM modul PKCS#11 interfésszel kell rendelkezniük. A TOE a kriptográfiai eszközök szolgáltatásait a saját PKCS#11 interfészükön éri el.

A szoftverkomponenseket az alábbi táblázat mutatja be

TOE vagy környezeti elem	Komponens	Leírás
TOE	A2-Polysys CryptoSigno Interop JAVA API	JAVA programozói könyvtár, aláírt Java archív file formátumban.
Környezeti elem	Operációs rendszer	Bármely operációs rendszer, ahol a JRE elérhető
Környezeti elem	Java Runtime Enviroment	Java 7 vagy a preferált Java 8 futtató környezet
Környezeti elem	FIPS 140 kompatibilis kriptográfiai szolgáltatás	Egy vagy több FIPS 140-2 Level 1 szintű kriptográfiai szolgáltatás a Java Kriptográfiai kiegészítéshez telepítve.
Környezeti elem	PKCS#11 API	Operációs rendszer függő TOE által alkalmazni kívánt kriptográfiai eszköz natív programozói könyvtára.
Környezeti elemek	Kiegészítő Java API-k	Xerces XML parser 2.7.2 vagy magasabb Xalan XSLT támogató and XPath feldolgozó 2.11.0 vagy magasabb PolysysGUI GUI komponens könyvtár 2.0.0 vagy magasabb Log4j naplózó könyvtár 1.2.17 vagy magasabb

A TOE és környezetét az 1. számú ábra mutatja be.



1. számú ábra A TOE és környezete

I.4. A rendszer főbb komponenseinek azonosítása

Értékelt TOE verzió:

Fájlnév	Verzió
a2-api-BIN-2_5_0.jar	2.5
SHA256: 4C1AF3D96AE7783304EE1F24D5EBF8A385D3D6E1C4E35ABC2EE44AD8A098AF03	

A TOE környezeteként megjelenő, a gyártó által fejlesztett további komponensek:

Fájlnév	Verzió
a2-api-DOC-2_5_0.jar	2.5
SHA256: B1C538356E4820F0AC954BA7E444E5808E6F410A0805C1DFBC15F890878D12E8	
a2-api-TST-2_5_0.jar	2.5
SHA256: 80EAF58FB1B79C62784B60824FF55D5268F32A5F9EBAA24A8A03E5FACF4A8A88	
a2-api-PolysysGUI-2_5_0.jar	2.5
SHA256: 3EB60E0683EF649C723DD121510959EABD3536305F0FE6D8A2E456AB6C5BFA25	
a2-api-EXAMPLES-2_5_0.jar	2.5
SHA256: 888FB75C3405B81B6D02211E54915B787B38B4DFEC6E2B38F9422C4DDC7BD0EE	

II. A tanúsítás jellemzése

Jelen tanúsítás a termék biztonsági előirányzatában lefektetetett követelmények teljesülését vizsgálja.

II.1. Az alkalmazott értékelési módszer

Az A2-Polysys CryptoSigno Interop JAVA API modul termék értékelésére a MIBÉTS (Magyar Informatikai Biztonsági Értékelési és Tanúsítási Séma) értékelési módszertant alkalmazták. A MIBÉTS értékelési módszertana a KIB (Közigazgatási Informatikai Bizottság) 28. számú ajánlásának (Az E-közigazgatási Keretrendszer követelménytár, 2009) részét képezi az alábbi címen: „Termékekre vonatkozó értékelési módszertan".

Az értékelés garanciaszintje MIBÉTS fokozott, mely a CC (Common Criteria, MSZ ISO/IEC 15408) szerinti EAL3-as szintnek feleltethető meg.

II.2. A tanúsításhoz felhasznált értékelési jelentések azonosítása

Értékelési Jelentés:

- A2-Polysys CryptoSigno JAVA API for Qualified Electronic Signature and Seal V2.5.0 ÉRTÉKELÉSI JELENTÉS v1.0, száma: C077-02/P/E

II.3. Az értékeléshez felhasznált fejlesztői bizonyítékok

Az értékelés, a fejlesztőkkel történt folyamatos konzultáció mellett, az alábbi fejlesztői bizonyítékok végleges verzióit használta fel:

Fájlnév	Verzió
A2-Polysys_ST_Security_Target v3.1.pdf	v3.1
A2-Polysys_HLD_HighLevel_Design.docx	v3.1
A2-Polysys_FS_Functional_Specification.docx	v3.1
A2-Polysys_CM_Configuration_Management.docx	v3.1
A2-Polysys_DO_Delivery_and_Operation.docx	v3.1
A2-Polysys_SG_Support_Guide.docx	v3.1
A2-Polysys_TG_Test_Guide.docx	v3.1
A2-Polysys_TCD_Test_Coverage_Depth_Analysis.docx	v3.0
A2-Polysys_VU_Vulnerability_Analysis.docx	v3.0
A2-Polysys_MM_Modification_Management.docx	v3.1
A2-Polysys_ACM_Assurance_Continuity_Maintenance.docx	v3.0
A2-Polysys_AX_Appendix.docx	v3.1

II.4. Az értékelési folyamat tanúsítási szempontú ellenőrzése

A Tanúsítási Jelentés készítői a teljes értékelési folyamatot figyelemmel kísérték, ellenőrizték:

- az értékelési folyamatok módszertani szempontú ellenőrzésével;
- különböző szakértői megbeszéléseken való részvétellel.

III. Az értékelés eredményei

III.1. A garanciális biztonsági követelményeknek való megfelelés

Az értékelés módszertana a MIBÉTS termékekre vonatkozó értékelési módszertanát (KIB 28. számú ajánlása) követte, az eredmények leírása is az ott meghatározott jelöléseket alkalmazza.

III.1.1. A biztonsági előirányzat értékelése

Értékelői feladatelem	határozat
ASE_INT: Biztonsági előirányzat, Bevezetés	megfelelt
ASE_CCL: Biztonsági előirányzat, Megfelelőségi nyilatkozatok	megfelelt
ASE_SPD: Biztonsági előirányzat, Biztonsági probléma meghatározás	megfelelt
ASE_OBJ: Biztonsági előirányzat, Biztonsági célok	megfelelt
ASE_ECD: Biztonsági előirányzat, Kiterjesztett biztonsági követelmények	megfelelt
ASE_REQ: Biztonsági előirányzat, Biztonsági követelmények	megfelelt
ASE_TSS: Biztonsági előirányzat, Az értékelés tárgya összefoglaló előírása	megfelelt

III.1.2. A fejlesztés értékelése

Értékelői feladatelem	határozat
ADV_ARC.1: Biztonsági szerkezet leírás	megfelelt
ADV_FSP.3: Funkcionális specifikáció teljes összegzéssel	megfelelt
ADV_TDS.2: Szerkezeti terv	megfelelt

III.1.3. Az útmutatók értékelése

Értékelői feladatelem	határozat
AGD_OPE.1: Üzemeltetési felhasználói útmutató	megfelelt
AGD_PRE.1: Előkészítő eljárások	megfelelt

III.1.4. Az életciklus támogatás értékelése

Értékelői feladatelem	határozat
ALC_CMC.3: Engedélyezéssel kapcsolatos intézkedések	megfelelt
ALC_CMS.3: A megvalósítási reprezentáció CM lefedettsége	megfelelt
ALC_DEL.1: Szállítási eljárások	megfelelt
ALC_DVS.1: A biztonsági intézkedések azonosítása	megfelelt
ALC_LCD.1: A fejlesztő által meghatározott életciklus modell	megfelelt

III.1.5. A tesztelés értékelése

Értékelői feladatelem	határozat
ATE_FUN.1: Funkcionális tesztelés	megfelelt
ATE_COV.2: A lefedettség vizsgálata	megfelelt
ATE_DPT.1: Az alap terv tesztelése	megfelelt
ATE_IND.2: Független tesztelés - minta	megfelelt

III.1.5.1. A2-Polysys CryptoSigno Interop JAVA API -val tesztelt platformok

A fejlesztői tesztek az alábbi szoftverkörnyezetben zajlottak:

#	Operációs rendszer	JAVA verzió
1	OS X High Sierra 10.13.3	Java 1.8.0_162
2	OS X High Sierra 10.13.3	Java 1.7.0_79
3	Windows 7 64 bit	Java 1.8.0_171
4	CentOS 7 (1708) x86_64	Java 1.8.0_161
5	Windows 7 64 bit	Java 1.8.0_171
6	Windows 7 64 bit	Java 1.8.0_171
7	Windows 10 64 bit	Java 1.8.0_171 Java 1.8.0_192
8	Ubuntu 14.04	Java 1.8.0_181
9	Ubuntu 18.04	Java 1.8.0_181

III.1.5.2. A2-Polysys CryptoSigno Interop JAVA API-val tesztelt PKCS#11-es hardver aláírás-létrehozó eszközök

A TOE az alábbi aláírás létrehozó eszközökkel tesztelték.

#	Típus	Verzió	Típus
1.	eSzemélyi	IDentity Applet Suite Version 3.2 alkalmazás, NXP J2E120_M65 / J3E120_M65 / J2E082_M65 / J3E082_M65 v2.4.2 R3 Secure Smart Card Controllerekből álló intelligens kártya	QSCD
2.	Gemalto IDClassic 340	MultiApp ID v2.1 Java Card platform, P5CC081V1A mikrochip, MPH117 V2.2 szűrővel	QSCD
3.	Bit4Id Touch & Sign 2048	ST19WR661 mikrochip, Touch & SIGN 2048 V1.00 alkalmazás	QSCD
4.	Gemalto IDPrime 840	MultiApp v3 Java Card paltform, M7820 A12 mikrochip, IAS v.4 alkalmazás	QSCD
5.	SafeNet eToken	9.1-es verzió, Athena IDProtect/OS755 Java Card kártya, Atmel AT90SC25672RCT-USB Microcontrolleren, IDSign applet beágyazással	QSCD
6.	Thales nShield F3 500e+ PCI Express	NC4433E-500	HSM modul
7.	Thales nShield Connect 1500+ F3	NH2061	HSM modul

III.1.6. A sebezhetőség értékelése

Az értékelő áttekintette a tesztelési dokumentációt, jegyzőkönyveket, valamint a fejlesztői Sebezhetőség elemzés Developer Vulnerability Analysis VU dokumentációt, annak érdekében, hogy meghatározza a TOE-ban esetlegesen előforduló lehetséges sebezhetőségeket. A TOE üzemeltetési környezetében nem érzékeny a nyilvános forrásokban az értékelés időpontjáig megjelent kereséssel azonosított lehetséges sebezhetőségekre.

Az értékelő tanulmányozta a nyilvános adatbázisokat, információ forrásokat a TOE lehetséges sebezhetőségeinek meghatározása céljából. Ellenőrzésre kerültek a TOE által használt harmadik feles alkalmazások a nyílt sérülékenység adatbázisok által.

A fenti vizsgálatok nem tártak fel kockázatokat, így az értékelés eredménye alapján a TOE üzemeltetési környezetében ellenáll egy alap támadó képességgel rendelkező támadónak.

Értékelői feladatelem	határozat
AVA_VAN.2: Sebezhetőség vizsgálat	megfelelt

IV. Következtetés

A rendszer értékelés fő következtetése az alábbi:

Az A2-Polysys CryptoSigno Interop JAVA API megfelel biztonsági előirányzatának, kielégíti az abban megfogalmazott funkcionális és garanciális biztonsági követelményeket.

Az értékelés eredménye alapján a Tanúsító megállapítja, hogy az A2-Polysys CryptoSigno Interop JAVA API, mint informatikai biztonsági funkciókat megvalósító szoftver termék megfelel a KIB 28-as Ajánlásában szereplő MIBÉTS módszertan szerinti fokozott biztonsági szintnek (ami megfeleltethető a CC EAL 3-es szintjének).

IV.1. Feltételek

Az értékelés következtetései a biztonsági előirányzatban megfogalmazott, az üzemeltetési környezetre vonatkozó feltételezések teljesülésén múlnak.

Ezek a feltételek (melyeket az A2-Polysys CryptoSigno Interop JAVA API nem kezel, nem kényszerít ki, hanem elvárja, hogy az informatikai és a nem informatikai környezet teljesítse) az alábbiak:

OE.AUDIT_GENERATION Az IT környezetnek észlelni és naplózni kell a felhasználóra vonatkozó biztonsági eseményeket.

OE.AUDIT_PROTECTION Az IT környezet biztosítsa a napló információk védelmét.

OE.AUDIT_REVIEW Az IT környezet biztosítson szelektív megjelenítést a napló információk tekintetében.

OE.Configuration A TOE megfelelően telepített és a konfigurált legyen a biztonságos állapotban történő elindításhoz.

OE.CORRECT_TSF_OPERATION Az IT környezet biztosítsa a TOE biztonsági funkcióinak tesztelését biztosítva azok ügyféloldali megfelelő működését.

OE.CRYPTOGRAPHY Az IT környezetnek FIPS 140-2 szabványnak megfelelő kriptográfiai szolgáltatásokat kell nyújtania a TOE számára. Minősített elektronikus aláírás vagy elektronikus bélyegző létrehozása esetén a TOE-nak véletlenszám generátort és QSCD által biztosított kriptográfiai szolgáltatást kell használnia.

OE.DISPLAY_BANNER Az IT környezetnek tájékoztató figyelmeztetést kell adnia a TOE használatával kapcsolatban.

OE.Basic A TOE tervezése és megvalósítása alap támadópotenciál elleni védelmet biztosít, ahogy a sérülékenység elemzés megállapította. (Az IT környezetet nem fenyegetheti ennél nagyobb támadópotenciál.)

OE.NO_EVIL A TOE felhasználási helyein az adminisztrátorok nem lehetnek rosszindulatúak, megfelelően képzettek és követik az adminisztrátori útmutató előírásait.

OE.PHYSICAL A TOE fizikai környezete elfogadható szintű biztonságot nyújtson, így a TOE nem manipulálható, illetve nem lehet alanya különböző típusú (pl. áramfelvétel analízis) side-channel támadásnak.

OE.RESIDUAL_INFORMATION Az IT környezet biztosítsa, hogy a tárgykörbe tartozó védett erőforrások által kezelt információk bizalmassága az erőforrások újra alkalmazása esetén sem sérül.

OE.SELF_PROTECTION Az IT környezet olyan működési környeztetett biztosítson, ami védi önmagát és erőforrásait a külső káros megzavarástól, módosítástól vagy jogosulatlan felfedéstől.

OE.TIME_STAMPS Az IT környezet megbízható időszolgáltatást biztosítson, ahol az adminisztrátor képes az alkalmazandó idő beállítására.

OE.TIME_TOE Az IT környezet megbízható idő jelzést biztosítson a TOE számára

OE.TOE_ACCESS Az IT környezet kontroll mechanizmust biztosítson a felhasználók TOE-hez való logikai hozzáférése tekintetében.

OE.TOE_PROTECTION Az IT környezet védje meg a TOE-t és erőforrásait a külső káros megzavarástól, módosítástól vagy jogosulatlan felfedéstől.

V. Hivatkozások, rövidítések

V.1. A követelményeket tartalmazó dokumentum

MIBÉTS 2009 Termékekre vonatkozó értékelési módszertan (az „e-Közigazgatási Keretrendszer Kialakítása” projekt keretében kidolgozott dokumentum, v4 2008.09.19) (a KIB 28-as számú Ajánlás része)

V.2. Figyelembe módszertani dokumentumok

Common Criteria for Information Technology Security Evaluation (September 2012 -version 3.1, revision 4) – Part 1: Introduction and general model

Common Criteria for Information Technology Security Evaluation (September 2012 -version 3.1, revision 4) – Part 2: Security functional components

Common Criteria for Information Technology Security Evaluation (September 2012 -version 3.1, revision 4) – Part 3: Security assurance components

Common Methodology for Information Technology Security Evaluation (September 2012 - version 3.1, revision 4)

ETSI TS 119 101 V1.1.1 (2016-03) Policy and security requirements for applications for signature creation and signature validation

V.3. Rövidítések

ADV (Assurance: Development)	Fejlesztés értékelése
AGD (Assurance: Guidance documents)	Útmutató dokumentumok értékelése
ALC (Assurance: Life cycle support)	Életciklus támogatás értékelése
ASE (Assurance: Security Target)	Biztonsági előirányzat értékelése
ATE (Assurance: Tests)	Tesztelés értékelése
AVA (Assurance: Vulnerability assessment)	Sebezhetőségi elemzés értékelése
CC (Common Criteria)	Közös szempontok
CM (Configuration management)	Konfiguráció kezelés
EAL (Evaluation Assurance Level)	Értékelési garanciaszint
ETR (Evaluation Technical Report)	Értékelési jelentés
KIB	Közigazgatási Informatikai Bizottság
MIBÉTS	Magyar Informatikai Biztonsági Értékelési és Tanúsítási Séma
ST (Security Target)	Biztonsági előirányzat
TOE (Target of Evaluation)	TOE, Értékelés tárgya
API (Application programming Interface)	Alkalmazás programozói felület
ETSI	European Telecommunications Standards Institute
XAdES (XML Advanced Electronic Signatures)	Kiterjesztett XML alapú elektronikus aláírás
OCSP (Online Certificate Status Protocol)	Azonnali tanúsítvány állapot protokoll
CRL (Certificate Revocation List)	Tanúsítvány visszavonási lista
HSM (Hardware Security Module)	hardver biztonsági modul
QSCD (Qualified electronic Signature Creation Device)	Minősített elektronikus aláírás létrehozó eszköz
FIPS	Federal Information Processing Standard Publication
GUI (Graphical User Interface)	Grafikus felhasználói felület