TANÚSÍTÁSI JELENTÉS

XadesMagic v1.0 elektronikus aláírás alkalmazás fejlesztő készletről fokozott biztonságú elektronikus aláíráshoz

HUNG-TJ-34-2006

Verzió:	1.0
Fájl:	HUNG_TJ_34_2006_v10.doc
Minősítés:	Nyilvános
Oldalak:	34

Változáskezelés

Verzió	Dátum	A változás leírása
v0.1	2006.10.30	A szerkezet felállítása
v0.8	2006.11.03	A tanúsítás eredményeit tartalmazó teljes változat
v0.81	2006.11.07	A tanúsítás eredményeit tartalmazó az értékelővel egyeztetett teljes változat
v0.9	2006.11.10	Utolsó egyeztetésre kiadott változat
v1.0	2006.11.20	Végleges verzió

A tanúsítási jelentést készítette:

Farkas Gábor
HunGuard Kft
Tanúsítási divízió

Tartalomjegyzék

1 Összefoglaló

1.1 Az értékelés jellemzői

Az értékelt termék neve:	**XadesMagic elektronikus aláírás alkalmazás fejlesztő készlet fokozott biztonságú elektronikus aláíráshoz**
Verzió szám:	**v1.0**
Rövid elnevezés:	**XadesMagic v1.0**
Az értékelt termék típusa:	Fejlesztő készlet (könyvtár)
Értékelő szervezet:	HunGuard Kft.
Értékelés befejezése:	2006. október 15
Az értékelés módszere:	CEM, Common Evaluation Methodology, v2.3
Az értékelés garanciaszintje:	EAL3
Az értékelt termék funkcionalitása:	A fejlesztő készlet által támogatott nyilvános kulcsú szolgáltatások az alábbiak: • elektronikus aláírás létrehozása; • elektronikus aláírás ellenőrzése, a kapcsolódó tanúsítvány útvonal felépítési és érvényesítési szolgáltatásokkal; • időbélyegzés (kérése és ellenőrzése); • PKI-alapú felhasználói hitelesítés (SSL/TLS) távoli szolgáltatás elérésénél.
Konfigurációs követelmények:	Hardver konfiguráció (minimum): • *CPU: 1000 MHz vagy magasabb (Pentium, AMD Opteron, AMD Athlon64, AMD Athlon XP)* • *RAM: 256 MByte vagy több* • *merevlemez: 20 MByte vagy több* Hardver konfiguráció (javasolt): • *CPU: 2000 MHz vagy magasabb (Pentium, AMD Opteron, AMD Athlon64, AMD Athlon XP)* • *RAM: 512 MByte vagy több* • *merevlemez: 20 MByte vagy több* Szoftver konfiguráció: • *operációs rendszer: MS Windows 2000, XP, 2003 Server* • *környezet: MS .NET Framework 1.1*

2 Azonosítás

Az értékelt termék neve:	**XadesMagic elektronikus aláírás alkalmazás fejlesztő készlet fokozott biztonságú elektronikus aláíráshoz**
Verzió szám:	**v1.0**
Az értékelt termék alkotó elemei (a felhasználókhoz, vagyis a fejlesztő készlet felhasználásával alkalmazást fejlesztőkhöz kiszállított tételek):	• SDA.XadesMagic.dll • SDA.Cryptography.dll • SDA.Cryptography.Framework.dll • SDA.TimestampProtocol.dll • dokumentáció

3 Biztonsági szabályzat

Ez a fejezet azokat a szabályokat írja le, melyek alapján a XadesMagic v1.0 irányítja az erőforrásaihoz való hozzáférést, s ezen keresztül minden általa ellenőrzött információt és szolgáltatást.
Először a XadesMagic v1.0 egy üzemmódját határozzuk meg. Ezt követően a szabályokat érvényre juttató biztonsági funkciókat tekintjük át.

3.1 Üzemmód

Fokozott biztonságú aláírás létrehozás esetén a XadesMagic v1.0 képes együttműködni mint kriptográfiai hardver eszközzel, mint PKCS#12 szoftveres kulcstároló állománnyal.

3.2 Biztonsági funkciók

A XadesMagic v1.0 az alábbi biztonsági funkciókat valósítja meg:

- BF1 Lenyomat és digitális aláírás kezelése
- BF2 Tanúsítvány kezelése
- BF3 Időbélyeg kezelése
- BF4 OCSP kezelése
- BF5 CRL kezelése
- BF6 A TSF (biztonsági funkciók összessége) védelme és kezelése

3.2.1 BF1 Lenyomat és digitális aláírás kezelése

A BF1 (Lenyomat és digitális aláírás kezelése) biztonsági funkció a lenyomat készítését, valamint az aszimmetrikus RSA kódolás elkészítésének, ellenőrzésének Microsoft Crypto API-n keresztüli aktiválását végzi el.
Az AR2 (Kriptográfiai kiegészítő függvények) és az AR3 (Aláírás-struktúra kezelő) alrendszerek valósítják meg.

3.2.2 BF2 Tanúsítvány kezelése

A BF2 (Tanúsítvány kezelése) biztonsági funkció a tanúsítványok sértetlenségének és hitelességének az ellenőrzését, illetve a tanúsítványlánc érvényesítését végzi el.
Az AR2 (Kriptográfiai kiegészítő függvények) alrendszer valósítja meg.

3.2.3 BF3 Időbélyeg kezelése

A BF3 (Időbélyeg kezelése) biztonsági funkció az időbélyeg kérések és válaszok létrehozását, küldését, fogadását és feldolgozását foglalja magában.
Az AR2 (Kriptográfiai kiegészítő függvények) és az AR4 (Időbélyegző) alrendszerek valósítják meg.

3.2.4 BF4 OCSP kezelése

A BF4 (OCSP kezelése) biztonsági funkció az OCSP kérések létrehozását, elküldését, majd a válaszok fogadását és feldolgozását foglalja magában.
Az AR2 (Kriptográfiai kiegészítő függvények) alrendszer valósítja meg.

3.2.5 BF5 CRL kezelése

A BF5 (CRL kezelése) biztonsági funkció a CRL elérését, lekérését és feldolgozását végzi el.

Az AR2 (Kriptográfiai kiegészítő függvények) alrendszer valósítja meg.

3.2.6 BF6 A TSF védelme és kezelése

A BF6 (A TSF védelme és kezelése) biztonsági funkció a bizalmas adatok memóriában, tárolón való kezelését, a különböző biztonsági beállításokat és az események naplózását foglalja magában.
Valamennyi alrendszer közreműködik megvalósításában.

Az AR1 (Segédfüggvények) alrendszer valamennyi biztonsági funkció megvalósításában közreműködik.

4 Feltételezések és hatókör

Az értékelés pozitív következtetése az alábbi feltétel csoportok teljesülésén múlik:

- a biztonsági előirányzat feltételezései (az értékelés tárgyát képező fejlesztő készlet biztonságához szükséges, az informatikai környezetre vonatkozó feltételek),
- a biztonságos felhasználás feltételei (az értékelés tárgyát képező fejlesztő készlet felhasználásával készített alkalmazások biztonságához szükséges, ezen alkalmazások megfelelő kialakítására vonatkozó feltételezések, javaslatok).

4.1 Feltételezések a XadesMagic v1.0 informatikai környezetére

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

1. Az engedéllyel rendelkező felhasználók megbízhatók a tekintetben, hogy a számukra kijelölt funkciókat megfelelően hajtják végre (AE.Authorized_Users)
2. A XadesMagic v1.0 fejlesztő készletet megfelelően telepítik és konfigurálják. (AE.Configuration)
3. A XadesMagic v1.0 környezete tartalmaz egy megbízható kriptográfiai modult (CryptoAPI), mely modul a kriptográfiai műveleteket hajtja végre. (AE.Crypto_Module)
4. A XadesMagic v1.0 környezete fizikailag megvédi a XadesMagic v1.0–t a jogosulatlan fizikai hozzáféréssel szemben. (AE.Physical_Protection)
5. A tanúsítvány és tanúsítvány visszavonási információk a XadesMagic v1.0 rendelkezésére állnak. (AE.PKI_Info)
6. A XadesMagic v1.0 környezete GMT formában és a megkívánt pontossággal gondoskodik a pontos rendszeridőről. (AE.Time)
7. A XadesMagic v1.0 környezete biztosítja az időbélyegzés szolgáltatóhoz való hozzáférést. (AE.TimeStamp)

4.2 A biztonságos felhasználás egyéb feltételei

1. A XadesMagic v1.0 fejlesztő készlettel létrehozott aláíró alkalmazás csak olyan aláírási szabályzat szerint működhet, amely legfeljebb az alábbi X509v3 tanúsítvány kiterjesztéseket használja fel:
   - ExtendedKeyUsage
   - KeyUsage
   - BasicConstraints
   - CRLDistributionPoints
   - SubjectAlternativeName
   - IssuerAlternativeName

2. A XadesMagic v1.0 fejlesztő készlettel létrehozott aláíró alkalmazáshoz olyan CSP driver-t kell alkalmazni, amely képes megőrizni az aláírandó adat reprezentáns (DTBSR) és valamennyi protokoll adat sértetlenségét.

3. A XadesMagic v1.0 fejlesztő készlettel létrehozott aláíró alkalmazáshoz vagy olyan CSP driver-t kell alkalmazni, amely képes megőrizni az aláírót hitelesítő adatok bizalmasságát, vagy az aláíró alkalmazást olyan védett környezetben kell használni, ahol menedzsment, üzemeltetési és műszaki intézkedések garantálják az aláírót hitelesítő adatok bizalmasságát.

4. A XadesMagic v1.0 fejlesztő készletet használó aláíró alkalmazás működtetési környezetében menedzsment, üzemeltetési és műszaki intézkedésekkel biztosítani kell, hogy az aláírási folyamatba ne avatkozhassanak be olyan nem megbízható rendszer és alkalmazási folyamatok, perifériák és kommunikációs csatornák, amelyek nem szükségesek az aláírás-létrehozás alkalmazás működéséhez.

5. A XadesMagic v1.0 fejlesztő készletet használó aláíró alkalmazáshoz:
   - vagy olyan CSP driver-t kell alkalmazni, amely képes egy időkorlátot megadni arra az időtartamra, ami az aláírót hitelesítő adatok megadásától az aláírás kiváltásáig eltelhet,
   - vagy az alkalmazásnak kell biztosítania az elvárást azáltal, hogy az aláírás kiváltása után kéri be a hitelesítő adatot.

6. A XadesMagic v1.0 fejlesztő készletet használó aláíró alkalmazáshoz:
   - vagy olyan CSP driver-t kell alkalmazni, amely képes egy időkorlát letelte után az aláírási folyamatot félbeszakítani, az aláírót hitelesítő adatok újra megadását megkövetelve a folyamatot újrakezdeni, és az újraindítás szükségességéről az aláírót tájékoztatni,
   - vagy az alkalmazásnak kell biztosítania az elvárást azáltal, hogy az aláírás kiváltása után kéri be a hitelesítő adatot.

7. A XadesMagic v1.0 működtetési környezetében menedzsment, üzemeltetési és műszaki intézkedéseket kell tenni az alábbiak biztosítására:
   - vírusok ne ronthassák el az aláíró alkalmazást és az általa meghívott egyéb aláíró összetevőket, valamint
   - az esetlegesen vírussal fertőzött aláíró összetevőket megfelelően helyre lehessen állítani.

8. A XadesMagic v1.0 működtetési környezetében menedzsment, üzemeltetési és műszaki intézkedésekkel kell megvédeni a XadesMagic v1.0 funkcionális összetevőinek sértetlenségét, megakadályozva, hogy behatolók elrontsák ezt.

9. A XadesMagic v1.0 működtetési környezetében menedzsment, üzemeltetési és műszaki intézkedésekkel biztosítani kell, hogy magát a XadesMagic v1.0-t, valamint az aláírás-létrehozás és aláírás-ellenőrzés folyamatokkal kölcsönhatásba lépő összes összetevőt egy biztonságos területen valósítsák meg.

4.3 Az értékelés hatóköre

Az értékelés figyelembe vette a biztonsági előirányzat valamennyi fenyegetését és a XadesMagic v1.0 valamennyi biztonsági funkcióját.

5 A XadesMagic v1.0 szerkezeti leírása

Az értékelés tárgya egy olyan fejlesztő készlet, melynek segítségével szabványos (X.509 szabványon alapuló) nyilvános kulcsú szolgáltatásokat biztosító alkalmazások fejleszthetők. A fejlesztő készlet által támogatott nyilvános kulcsú szolgáltatások az alábbiak:

- Fokozott biztonságú elektronikus aláírás létrehozása a Crypto API által támogatott algoritmus paraméterekkel, Windows tanúsítványtárban vagy kriptográfiai hardver eszközben tárolt magánkulcs használatával.
- Elektronikus aláírás ellenőrzése, a kapcsolódó tanúsítvány útvonal felépítési és érvényesítési szolgáltatásokkal.
- Aláírás létrehozáshoz lenyomat készítése SHA-1, SHA-256, SHA-384, SHA-512, Ripemd-160 algoritmusokkal.
- Időbélyeg kérése és ellenőrzése.
- Visszavonási információ kérése és ellenőrzése (CRL, OCSP).

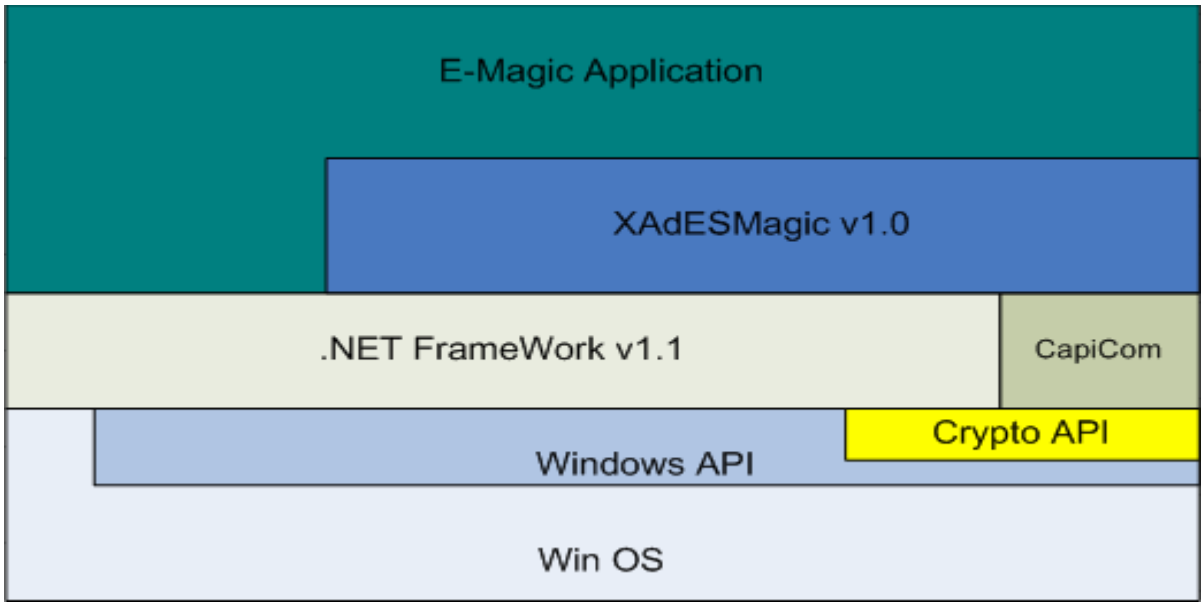
Ennek alapján a XadesMagic v1.0 fejlesztői készlet segítségével olyan alkalmazások fejleszthetők, melyek a nyilvános kulcsú technológia alapján bizalmasságot, sértetlenséget, hitelesítést és letagadhatatlanságot biztosító szolgáltatásokat képesek nyújtani.

A XadesMagic v1.0 fejlesztői függvénykönyvtár az alábbi nyilvános kulcs szolgáltatásokkal rendelkezik:

- biztonságosan kezel kulcsokat, megbízható pontokat és tanúsítványokat;
- elfogad és feldolgoz X.509 v3 nyilvános kulcs tanúsítványokat;
- képes a szükséges tanúsítványok és visszavonási adatok megszerzésére (a tanúsítványban szereplő CDP kiterjesztésben meghatározott helyről);
- ellenőrzi minden tanúsítvány érvényességét, az X.509 szabványban [ISO 9594-8] leírt eljárások felhasználásával, beleértve a visszavonás ellenőrzését is;
- hozzáfér pontos és megbízható időforráshoz a tanúsítványok, visszavonási adatok és alkalmazási adatok dátumának, idejének ellenőrzése érdekében;
- beszerzi, tárolja (beágyazza az aláírás struktúrába) a digitális aláírás jövőbeni ellenőrzéséhez szükséges adatokat;
- támogatja a Melasz-Ready XAdES elektronikus aláírás formátumot.

5.1 Architektúra

Az 1. ábra a XadesMagic v1.0 struktúráját és az IT környezetbe való beágyazódását mutatja be.



1. ábra A XadesMagic v1.0 és környezete

A XadesMagic v1.0 függvénykönyvtárat felhasználva lehet kifejleszteni az IT környezet részét képező, a XadesMagic v1.0 függvényeit meghívó alkalmazást (pl. E-Magic Application).

Szintén az IT környezethez tartoznak a .NET Framework v1.1, a CryptoAPI és a CAPICOM (CryptoAPI Component Object Model) kriptográfiai ActiveX vezérlő, illetve a Windows API és Windows OS (operációs rendszer) egyéb függvényei.

5.2 Alrendszerek

A XadesMagic v1.0-nak az alábbi alrendszerekből áll:

- AR1: Segédfüggvények (alrendszer)
- AR2: Kriptográfiai kiegészítő függvények (alrendszer)
- AR3: Aláírás-struktúra kezelő (alrendszer)
- AR4: Időbélyegző (alrendszer)

5.2.1 AR1 Segédfüggvények

Az AR1 (Segédfüggvények) alrendszer különböző alapvető transzformációs (pl. base64), hibakezeléshez, naplózáshoz kötődő, beállításokért felelős osztályokat kezeli.
Az alrendszer osztályai az SDA.Cryptography.Framework.dll állományban helyezkednek el.

5.2.2 AR2 Kriptográfiai kiegészítő függvények

Az AR2 (Kriptográfiai kiegészítő függvények) alrendszer a Microsoft CryptoAPI hatáskörén kívül eső kriptográfiai osztályokat kezeli. Ezen osztályok a tanúsítványláncok felépítését, a tanúsítványok és visszavonási adatok (CRL, OCSP) ellenőrzését (tartalmi, formai szempontok alapján), lenyomatok előállítását és ellenőrzését végzik.
Az alrendszer osztályai az SDA.Cryptography.dll állományban helyezkednek el.

5.2.3 AR3 Aláírás-struktúra kezelő

Az AR3 (Aláírás-struktúra kezelő) alrendszer az ETSI TS 101 903 v1.2.2 (XAdES) szabványban meghatározott XML sémának megfelelő struktúra felépítését, kezelését végzi. Az egyes elemekhez (XML tag) egy-egy osztály tartozik, de külön osztályok vonatkoznak a hibakezelésekre, ellenőrzésekre is.
Az alrendszer osztályai döntően az SDA.XadesMagic.dll állományban helyezkednek el.

5.2.4 AR4 Időbélyegző összetevő

Az AR4 (Időbélyegző összetevő) alrendszer az IETF RFC 3161 szabványban meghatározott ASN.1 leírásnak megfelelő időbélyeg kéréseket és válaszokat kezeli. Az alrendszer egyes osztályai felelősek a kérés összeállításáért, illetve a válaszok ellenőrzéséért (tartalmi, formai szempontok alapján).
Az alrenszer osztályai az SDA.TimeStampProtocol.dll állományban helyezkednek el.
A 2. ábra a XadesMagic v1.0 alrendszereinek belső függőségeit mutatja be:

2. ábra: A XadesMagic v1.0 alrendszerei, és ezek belső függési viszonyai

6 Dokumentáció

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

- a fejlesztéshez szükséges SDA.XadesMagic.dll, SDA.Cryptography.dll, SDA.Cryptography.Framework.dll, SDA.TimestampProtocol.dll
- Adminisztrátori útmutató v1.0 (XM_AGD_v10.pdf)

7 Tesztelés

7.1 A fejlesztők tesztelése

A XadesMagic v1.0 fejlesztői tesztelését egy Windows XP SP2 operációs rendszerű, Microsoft .Net 1.1 Framework-öt tartalmazó számítógépen, egy saját fejlesztésű tesztelő program segítségével végezték.

A fejlesztői tesztek a XadesMagic v1.0 különböző funkcióinak ellenőrzését végzik el. Egyaránt lefedik az ST-ben meghatározott biztonsági funkciókat, valamint a HLD–ben meghatározott alrendszereket, ahogyan ezt a teszt lefedettségi és a teszt mélységi elemzés ki is mutatja.

Minden fejlesztői tesztre pozitív és negatív teszt eset is rendelkezésre állt. A negatív teszt esetek lényegében az XMLDSig csomag ellenőrzésére vonatkoznak. A pozitív teszt esetek indirekt módon tesztelik az XMLDSig csomag előállítását (aláírását) is.

A fejlesztői tesztek 7 nagyobb csoportra oszthatók:

- XMLDSig struktúra ellenőrzése,
- tanúsítvány ellenőrzése,
- XAdES formátum ellenőrzése,
- időbélyeg ellenőrzése,
- OCSP ellenőrzése,
- CRL ellenőrzése,
- többszörös aláírás ellenőrzése.

A fejlesztői tesztek esetén a várt és a tényleges teszt eredmény minden esetben megegyezett.

7.2 Az értékelők tesztelése

Az értékelői tesztelés első lépéseként a fejlesztői tesztelés részleges megismétlésére, annak eredményeinek ellenőrzésére került sor.

A fejlesztői tesztelés részleges megismétlése a fejlesztői tesztelés bázisán (XP SP2 operációs rendszer, MS .Net Framework 1.1, SDA.E-Magic program) történt. Az eredmények megfelelőek voltak.

Az értékelői tesztelés második lépéseként független (értékelői) tesztelésre került sor.

Az értékelői tesztelés egy XP SP2 operációs rendszerű, Microsoft .Net Framework 1.1-et tartalmazó számítógépen, az értékelők által készített teszt programok segítségével történt.

A független (értékelői) tesztelés az alábbi három témakörre koncentrált:

- tanúsítványlánc ellenőrzés,
- CRL kezelés ellenőrzése,
- időbélyeg szolgáltatás elérés.

A tanúsítványlánc ellenőrzés a PKITS teszt csomag felhasználásával, külön (az értékelők által fejlesztett) teszt program segítségével történt. Ez a teszt program a PKITS csomag azon teszt eseteit ellenőrzi, amely a XadesMagic v1.0 által felvállalt X509v3 tanúsítvány kiterjesztéseket vizsgálja (azaz a következőket: ExtendedKeyUsage, KeyUsage, BasicConstraints, CRLDistributionPoints, SubjectAlternativeName, IssuerAlternativeName). A teszt program nem ellenőrizte a PKITS tesztkészlet 4. fejezetének teszt eseteit sem (melyek a CRL helyes kezelését ellenőrzik), mivel a XadesMagic v1.0 az off-line CRL-eket nem támogatja.

CRL kezelés ellenőrzése keretén belül a CRL letöltés értékelése külön (az értékelők által fejlesztett) teszt program segítségével történt.

Az időbélyeg szolgáltatás elérése és a válasz értékelése is külön értékelői teszt programok segítségével történt. Ezekben interaktív felületre lettek kivezetve a XadesMagic v1.0 időbélyeg szolgáltatással kapcsolatos állítható belső paraméterei (AutoGenerate-RequestNonceIfEmpty, IgnoreMissingCertificate, IgnoreMissingNonce).

A tesztelés a http://152.66.10.216:8080/ teszt időbélyeg szolgáltatót használta.

A tesztelésnél a következő paraméterek lettek igaz értékre állítva:

1. AutoGenerateRequestNonceIfEmpty
2. AutoGenerateRequestNonceIfEmpty, IgnoreMissingCertificate
3. AutoGenerateRequestNonceIfEmpty, IgnoreMissingNonce

/Ha az AutoGenerateRequestNonceIfEmpty időbélyeg konfigurálási paraméter nincs bekapcsolva, akkor a teszt időbélyeg szolgáltató nem működik megfelelően./

A létrehozott XML csomagban az időbélyeg mindhárom esetben megfelelő volt.

8 Az értékelt konfiguráció

8.1 Hardver

Hardver konfiguráció (minimum):

- CPU: 1000 MHz vagy magasabb (Pentium, AMD Opteron, AMD Athlon64, AMD Athlon XP)
- RAM: 256 MByte vagy több
- merevlemez: 20 MByte vagy több

Hardver konfiguráció (javasolt):

- CPU: 2000 MHz vagy magasabb (Pentium, AMD Opteron, AMD Athlon64, AMD Athlon XP)
- RAM: 512 MByte vagy több
- merevlemez: 20 MByte vagy több

8.2 Szoftver

Szoftver konfiguráció:

- operációs rendszer: MS Windows 2000, XP, 2003 Server
- környezet: MS .NET Framework 1.1

9 Az értékelés eredményei

A XadesMagic v1.0 fejlesztő készlet a CEM (Common Evaluation Methodology) v2.3 módszertana szerint független értékelésre és tanúsításra került, EAL3 garanciaszinten.

Az értékelés fő következtetése az alábbi:

Az értékelés megállapította, a tanúsítás pedig megerősítette, hogy a XadesMagic v1.0 megfelel a biztonsági előirányzatának, kielégíti az abban megfogalmazott funkcionális és garanciális biztonsági követelményeket.

A fenti megállapítás az EAL3 követelményeinek teljesítésén alapul. Az alábbiak azt mutatják meg, hogy az egyes garanciaösszetevőket hogyan teljesíti a XadesMagic v1.0 fejlesztő készlet, illetve mely fejlesztői bizonyítékok támogatták ennek kimutatását.

Garancia-osztály	Garancia-összetevő	A követelmények kielégítésének módja, /s az ezt leíró fejlesztői bizonyíték/
Biztonsági előirányzat	ASE_DES.1	A TOE leírása kellően részletes, következetes és belső ellentmondás mentes. **Biztonsági előirányzat** v1.0, XM_ST_v10.pdf
	ASE_ENV.1	A TOE biztonsági környezetéről szóló nyilatkozat következetes és belső ellentmondás mentes. **Biztonsági előirányzat** v1.0, XM_ST_v10.pdf
	ASE_INT.1	Az ST helyesen van azonosítva és ez az azonosítás az ST összes többi részével ellentmondás mentesen összefér. **Biztonsági előirányzat** v1.0, XM_ST_v10.pdf
	ASE_OBJ.1	A biztonsági célokról szóló nyilatkozat következetes, teljes és belső ellentmondás mentes. **Biztonsági előirányzat** v1.0, XM_ST_v10.pdf
	ASE_PPC.1	Az ST szerzői védelmi profilnak való megfelelőséget nem állítanak. **Biztonsági előirányzat** v1.0, XM_ST_v10.pdf
	ASE_REQ.1	Az informatikai biztonsági követelményekről szóló nyilatkozat következetes, teljes és belső ellentmondás mentes. **Biztonsági előirányzat** v1.0, XM_ST_v10.pdf
	ASE_SRE.1	Minden explicit módon kifejezett funkcionális követelményre a CC 3. részbeli garanciális követelmények alkalmazhatóak és alkalmasak. Az ST szerzői nem hagytak figyelmen kívül egyetlen alkalmazandó függési viszonyt sem. **Biztonsági előirányzat** v1.0, XM_ST_v10.pdf
	ASE_TSS.1	A TOE összefoglaló előírás következetes, teljes és ellentmondás mentes. **Biztonsági előirányzat** v1.0, XM_ST_v10.pdf
Konfiguráció menedzselés	ACM_CAP.3	A konfiguráció lista egyértelműen azonosítja az TOE-t alkotó összes konfiguráció elemet. A konfiguráció elemek a konfiguráció menedzselés dokumentációval összhangban azonosítottak. A konfiguráció menedzselés rendszer a konfiguráció menedzselés tervnek megfelelően működik **A konfiguráció menedzselés dokumentációja** v1.0, XM_CM_v10.pdf

	ACM_SCP.1	A konfiguráció lista tartalmazza a CC által megkövetelt minimális konfiguráció elem készletet: • szoftver komponensek, • forráskódok, • tervezési dokumentáció, • fejlesztői útmutató, • konfiguráció menedzselés dokumentáció, • teszt dokumentáció és teszt szoftver, • dokumentációk (specifikációk, kézikönyvek, tesztdokumentumok,). **A konfiguráció menedzselés dokumentációja** v1.0, XM_CM_v10.pdf
Kiszállítás és működtetés	ADO_DEL.1	A XadesMagic v1.0 fejlesztő készlet szállítása nem önálló feladat, azt a fejlesztő készletet meghívó alkalmazások végzik majd el. Következésképpen a szállítás értékelésére vonatkozó értékelői munkaegységek teljesítettnek tekinthetők. **Adminisztrátori útmutató** v1.0, XM_AGD_v10.pdf **tesztelésre alkalmas XadesMagic v1.0**
	ADO_IGS.1	A XadesMagic v1.0 fejlesztő készlet telepítése és működtetése nem önálló feladat, azt a fejlesztő készletet meghívó alkalmazások végzik majd el. Következésképpen a telepítés és működtetés értékelésére vonatkozó értékelői munkaegységek teljesítettnek tekinthetők **Adminisztrátori útmutató** v1.0, XM_AGD_v10.pdf **tesztelésre alkalmas XadesMagic v1.0**
Fejlesztés	ADV_FSP.1	A funkcionális specifikáció (FS) tartalmazza az összes szükséges informális magyarázatot, belső ellentmondásoktól mentes, azonosít minden külső TOE biztonsági funkció interfészt és leírja az összes külső TOE biztonsági funkció interfészt. Az FS a TOE funkcionális biztonsági követelmények pontos megvalósulása és teljes mértékben bemutatja a TSF-t. **Funkcionális specifikáció** v1.0, XM_FS_v10.pdf és XadesMagic_Documentation.chm
	ADV_HLD.2	A magas szintű terv (HLD) tartalmazza az összes szükséges informális magyarázatot, belső ellentmondásoktól mentes és alrendszerek szerint leírja a TSF-et. A HLD leírja minden alrendszer biztonsági funkcionalitását, azonosítja a TSF által megkövetelt összes hardvert, förmvert és szoftvert. A HLD a TOE funkcionális biztonsági követelményeinek pontos és teljes megvalósulása. **Magas szintű terv** v1.0, XM_HLD_v10.pdf
	ADV_RCR.1	A funkcionális specifikáció a TOE biztonsági funkcióinak helyes és teljes reprezentációja. A magas szintű terv helyes és teljes megvalósulása a funkcionális specifikációnak **Megfeleltetés elemzések** v1.0, XM_RCR_v10.pdf

Útmutató dokumentumok	AGD_ADM.1	Az adminisztrátoroknak (is) szóló útmutatás: • leírja az adminisztrátor rendelkezésére álló adminisztratív biztonsági funkciókat és interfészeket, • leírja a TOE biztonságos üzemeltetéséhez szükséges adminisztrálás módját, • tartalmazza az azokkal a funkciókkal és jogosultságokkal kapcsolatos figyelmeztetéseket, melyeket egy biztonságos feldolgozási környezetben felügyelni kell, • leír minden olyan feltételezést, mely a biztonságos üzemeltetés szempontjából lényeges felhasználói viselkedéssel kapcsolatos, • leír az adminisztrátor ellenőrzése alá tartozó minden biztonsági paramétert, szükség esetén jelezve a biztonságos értékeket is. • leírja a végrehajtandó adminisztrátori funkcióhoz kapcsolódó, biztonsági szempontból lényeges események típusát, beleértve a biztonsági tulajdonságok megváltoztatását is, • konzisztens az értékeléshez beadott többi dokumentációval, • leír minden, a TOE informatikai környezetére vonatkozó, az adminisztrátor számára lényeges biztonsági követelményt. **Adminisztrátori útmutató** v1.0, XM_AGD_v10.pdf
	AGD_USR.1	Nem készült külön adminisztrátori és felhasználói útmutató, mivel a XadesMagic v1.0 egy függvénykönyvtár, amellyel aláíró és aláírás ellenőrző alkalmazások készíthetők. A függvénykönyvtárat pedig a fejlesztő (alkalmazás programozó) használja. Következésképpen a felhasználói útmutatóval kapcsolatos értékelői munkaegységek teljesítettnek tekinthetők. **Adminisztrátori útmutató** v1.0, XM_AGD_v10.pdf
Az életciklus támogatása	ALC_DVS.1	A fejlesztői biztonsági dokumentáció részletezi az összes olyan, fejlesztői környezetben használt biztonsági intézkedést, melyek a TOE tervek és a TOE megvalósítás bizalmasságának és sértetlenségének megőrzését szolgálják. A biztonsági intézkedéseket betartották. **A fejlesztési biztonság dokumentációja** v1.0, XM_DVS_v10.pdf
Tesztelés	ATE_FUN.1	A tesztelési dokumentáció tartalmazza a teszt terveket, a teszt eljárások leírását és a várt eredményeket, valamint a teszt eredményeit. Azonosítja a tesztelendő biztonsági funkciókat és leírja a végrehajtott tesztek célját. A leírt teszt konfiguráció a TOE megfelelő verziójára vonatkozik. A teszt tervek ellentmondás mentesek a teszt eljárások leírásával. A teszt eljárások leírása azonosít minden tesztelendő biztonsági funkció működést. A tesztelési dokumentációban a teszt esetek leírása megfelelő: a leírások alapján a kezdeti feltételek beállíthatók, az egyes teszt esetek megismételhetőek. A teszt esetek leírása ellentmondás mentes a teszteljárásokkal. A tesztelési dokumentációban a várt teszt eredmények megfelelőek. **Tesztelési dokumentáció** készült: 2006.09.26., tartalmazza az alábbi alkönyvtár: XM-TestCollection_v10
	ATE_COV.2	A teszt lefedettség elemzés értékelése megállapította, hogy a tesztelési dokumentációban azonosított tesztek és a funkcionális specifikáció közötti megfeleltetés pontos. A tesztelési dokumentáció és az ennek megfelelő teszt lefedettség elemzés minden biztonsági funkcióra tartalmaz teszt esetet, így a tesztelés teljes **Teszt lefedettség elemzés** v1.0, XM_ATE_COV_v10.pdf

	ATE_DPT.1	A tesztelési dokumentáció tartalmazza, hogy az egyes tesztek mely alrendszer vagy alrendszerek tesztelésére vonatkoznak. A magas szintű tervben megadott TSF megfelelően le van képezve a teszt esetekre. **Teszt mélység elemzés** v1.0, XM_ATE_DPT_v10.pdf
	ATE_IND.2	A fejlesztő a független teszteléshez biztosította az értékelő számára azt a környezetet és erőforrás-készletet, amivel a saját tesztelését végezte. Az értékelő megismételte a tesztelést a fejlesztő tesztelési dokumentációjában leírt tesztek egy mintájára, valamint megtervezett egy teszt készletet, majd végrehajtotta és dokumentálta azokat. **tesztelésre alkalmas XadesMagic v1.0**
A sebezhetőség felmérése	AVA_MSU.1	Az útmutató helytelen használhatóságának elemzése alapján megállapítható, hogy az útmutató a TOE valamennyi működési módjában útmutatást ad a biztonságos működtetésre **Adminisztrátori útmutató** v1.0, XM_AGD_v10.pdf
	AVA_SOF.1	A biztonsági előirányzat nem azonosít egyetlen funkcióerősségi nyilatkozattal rendelkező mechanizmust sem, ezáltal az ehhez tartozó értékelői munkaegységek teljesítettnek tekinthetők.
	AVA_VLA.1	Az értékelő az áthatolás tesztelések eredményei, valamint a sebezhetőségi elemzések következtetései alapján megállapította, hogy a TOE a tervezett (cél)környezetében képes ellenállni egy alacsony támadási képességgel rendelkező támadónak. Az értékelő se kihasználható, se maradvány sebezhetőséget nem talált. **Fejlesztői sebezhetőség elemzés** v1.0, XM_VA_v10.pdf

Az értékelés másik következtetése az alábbi:
A XadesMagic v1.0 fejlesztő készlet (A 4.2 fejezetben megfogalmazott feltételek teljesülése esetén) **megfelel a CEN CWA 14170:2004 és CEN CWA 14171:2004 által az elektronikus aláíró alkalmazásokra támasztott valamennyi olyan funkcionális és garanciális biztonsági követelménynek, mely a fejlesztő készletre vonatkozik.**

10 Értékelői megjegyzések és javaslatok

Az értékelő nem adott a tanúsítási jelentésbe megjelenítendő megjegyzést, illetve javaslatot.

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.

A XadesMagic v1.0 fejlesztő készletre (mint elektronikus aláírás létrehozásának és ellenőrzésének megvalósítására felhasználható elektronikus aláírási termékre) ugyanakkor az alábbi két nemzetközi követelményrendszer is vonatkozik:

- CEN CWA 14170:2004 munkacsoport egyezmény: Security requirements for signature creation applications /May 2004/
- CEN CWA 14171:2004 munkacsoport egyezmény: 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 felel meg" 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:

A XadesMagic v1.0 fejlesztő készlet (A 4.2 fejezetben megfogalmazott feltételek teljesülése esetén) **megfelel a CEN CWA 14170:2004 és CEN CWA 14171:2004 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 a XadesMagic v1.0-ra vonatkozó konkrét követelményrendszert határozza meg az értékelés viszonyítási alapjaként. Ez teljes mértékben összhangban van a CC módszertanával, ugyanakkor nem teszi összehasonlíthatóvá a jelen értékelés eredményét a korábbi értékelési eredményekkel.

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.

11.1 A XadesMagic v1.0 megfelelése a funkcionális követelményeknek

Funkcionális követelmény	Teljesülés
F_SCA_1	**Megfelel**
F_SDP_1	**Megfelel**
F_SDP_2	**Megfelel**
F_SDP_3	**Megfelel**
F_SAV_1	**megfelel**
F_SAV_2	**megfelel**
F_SAV_3	**megfelel**
F_SIC_1	**nem vonatkozik rá a követelmény**
F_SIC_2	**nem vonatkozik rá a követelmény**
F_SIC_3	**nem vonatkozik rá a követelmény**
F_DTBSF_1	**megfelel**
F_DTBSF_2	**megfelel**
F_DHC_1	**megfelel**
F_DHC_2	**nem vonatkozik rá a követelmény**
F_SSC_1	**nem vonatkozik rá a követelmény**
F_SSC_2	**nem vonatkozik rá a követelmény**
F_SSC_3	**nem vonatkozik rá a követelmény**
F_SSC_4	**nem vonatkozik rá a követelmény**
F_SSC_5	**nem vonatkozik rá a követelmény**
F_SSC_6	**nem vonatkozik rá a követelmény**
F_SSC_7	**nem vonatkozik rá a követelmény**
F_SSC_8	**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_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_ISV-3	**Feltétellel megfelel (1)**
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_human_7	**megfelel**
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 A XadesMagic v1.0 megfelelése a biztonsági követelményeknek

Biztonsági követelmény	Teljesülés
S_SCA_1	**feltétellel megfelel (2)**
S_SCA_2	**feltétellel megfelel (3)**
S_SCA_3	**megfelel**
S_SCA_4	**megfelel**
S_SCA_5	**megfelel**
S_SCA_6	**megfelel**
S_SCA_7	**nem vonatkozik rá a követelmény**
S_SCA_8	**nem vonatkozik rá a követelmény**
S_SCA_9	**feltétellel megfelel (4)**
S_SCA_10	**megfelel**
S_SCA_11	**megfelel**
S_SCA_12	**megfelel**
S_SDP_1	**megfelel**
S_SDP_2	**nem vonatkozik rá a követelmény**
S_SDP_3	**nem vonatkozik rá a követelmény**
S_SDP_4	**nem vonatkozik rá a követelmény**
S_SDP_5	**nem vonatkozik rá a követelmény**
S_SDP_6	**nem vonatkozik rá a követelmény**
S_SDP_7	**nem vonatkozik rá a követelmény**
S_SDP_8	**nem vonatkozik rá a követelmény**
S_SDP_9	**nem vonatkozik rá a követelmény**
S_SDP_10	**megfelel**
S_SDP_11	**megfelel**
S_SDP_12	**nem vonatkozik rá a követelmény**
S_SAV_1	**megfelel**
S_SAV_2	**megfelel**
S_SAV_3	**megfelel**
S_SAV_4	**nem vonatkozik rá a követelmény**
S_SAV_5	**nem vonatkozik rá a követelmény**

S_SAV_6	**nem vonatkozik rá a követelmény**
S_SAV_7	**nem vonatkozik rá a követelmény**
S_SAV_8	**nem vonatkozik rá a követelmény**
S_SIC_1	**nem vonatkozik rá a követelmény**
S_SIC_2	**feltétellel megfelel (5)**
S_SIC_3	**feltétellel megfelel (6)**
S_SIC_4	**nem vonatkozik rá a követelmény**
S_SIC_5	**nem vonatkozik rá a követelmény**
S_SAC_1	**nem vonatkozik rá a követelmény**
S_SAC_2	**feltétellel megfelel (3)**
S_SAC_3	**nem vonatkozik rá a követelmény**
S_SAC_4	**nem vonatkozik rá a követelmény**
S_SAC_5	**nem vonatkozik rá a követelmény**
S_SAC_6	**nem vonatkozik rá a követelmény**
S_SAC_7	**nem vonatkozik rá a követelmény**
S_SAC_8	**nem vonatkozik rá a követelmény**
S_SAC_9	**nem vonatkozik rá a követelmény**
S_SAC_10	**nem vonatkozik rá a követelmény**
S_SAC_11	**nem vonatkozik rá a követelmény**
S_SAC_12	**nem vonatkozik rá a követelmény**
S_DTBSF_1	**megfelel**
S_DHC_1	**megfelel**
S_DHC_2	**nem vonatkozik rá a követelmény**
S_DHC_3	**megfelel**
S_SSC_1	**nem vonatkozik rá a követelmény**
S_SSC_2	**nem vonatkozik rá a követelmény**
S_SSC_3	**nem vonatkozik rá a követelmény**
S_SSC_4	**nem vonatkozik rá a követelmény**
S_SSA_1	**nem vonatkozik rá a követelmény**
S_SDC_1	**nem vonatkozik rá a követelmény**
S_I/O_1	**feltétellel megfelel (7)**
S_I/O_2	**feltétellel megfelel (8)**
S_I/O_3	**nem vonatkozik rá a követelmény**
S_VER_1	**feltétellel megfelel (9)**

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 értékelés tárgya egy olyan fejlesztő készlet, melynek segítségével szabványos (X.509 szabványon alapuló) nyilvános kulcsú szolgáltatásokat biztosító alkalmazások fejleszthetők. A fejlesztő készlet által támogatott nyilvános kulcsú szolgáltatások az alábbiak:

- *Fokozott biztonságú elektronikus aláírás létrehozása a Crypto API által támogatott algoritmus paraméterekkel, Windows tanúsítványtárban vagy kriptográfiai hardver eszközben tárolt magánkulcs használatával.*
- *Elektronikus aláírás ellenőrzése, a kapcsolódó tanúsítvány útvonal felépítési és érvényesítési szolgáltatásokkal.*
- *Aláírás létrehozáshoz lenyomat készítése SHA-1, SHA-256, SHA-384, SHA-512, Ripemd-160 algoritmusokkal.*
- *Időbélyeg kérése és ellenőrzése.*
- *Visszavonási információ kérése és ellenőrzése (CRL, OCSP).*

Ennek alapján a XadesMagic v1.0 fejlesztői készlet segítségével olyan alkalmazások fejleszthetők, melyek a nyilvános kulcsú technológia alapján bizalmasságot, sértetlenséget, hitelesítést és letagadhatatlanságot biztosító szolgáltatásokat képesek nyújtani.

A XadesMagic v1.0 fejlesztő készlet a CEM (Common Evaluation Methodology) v2.3 módszertana szerint független értékelésre és tanúsításra került, EAL3 garanciaszinten. Az értékelés megállapította, a tanúsítás pedig megerősítette, hogy a XadesMagic v1.0 megfelel biztonsági előirányzatának, kielégíti az abban megfogalmazott funkcionális és garanciális biztonsági követelményeket."

12 Biztonsági előirányzat

A jelen tanúsítási jelentés részét képező végleges biztonsági előirányzatot különálló dokumentumként csatoljuk.

13 Fogalmak és rövidítések

13.1 Fogalmak

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

biztonsági cél
Szándéknyilatkozat azonosított fenyegetések elleni fellépésről és/vagy meghatározott szervezeti biztonsági szabályzatoknak és feltételezésnek való megfelelésről.

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

értékelés
A biztonsági előirányzat, illetve az értékelés tárgyának felmérése meghatározott szempontrendszer (pl. a CC vagy a CEM 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 garancia összetevőiből 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
Az a személy, aki a XadesMagic v1.0-t fejlesztőkészletet, vagy az erre épülő aláíró alkalmazásokat használja, azaz a XadesMagic v1.0 szolgáltatásait igénybe veszi.

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.

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

tanúsítási útvonal felépítése
Egy tanúsítványhoz a tanúsítványlánc kialakítása, úgy, hogy minden tanúsítványt az azt kibocsátó hitelesítés szolgáltató tanúsítványa kövessen. A tanúsítványlánc 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 tanúsítványláncban az első helyen szerepel.

tanúsítvány, közbenső tanúsítvány
Olyan, hitelesítés szolgáltató számára kiadott tanúsítvány, amely a tanúsítványláncban 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, végtanúsítvány
Olyan, általában személyes tanúsítvány, amely a tanúsítványláncban 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.

tanúsítványlánc
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.

XAdES

Az XMLDSIG szabvány továbbfejlesztése.

XMLDSIG

Az XML elektronikus aláírás szintaktikáját és feldolgozását leíró szabvány.

13.2 Rövidítések

Az alábbiakban meghatározzuk a jelen értékelési jelentésben használt betűszavak jelentését.

API	**A**pplication **P**rogramming **I**nterface
AR	**Al**rendszer
BF	**B**iztonsági **f**unkció
CAPICOM	**C**rypto**API** **C**omponent **O**bject **M**odel)
CC	**C**ommon **C**riteria (Közös szempontok)
CDP	**C**RL **D**istribution **P**oint (CRL terjesztési pont)
CEM	**C**ommon **E**valuation **M**ethodology (Közös értékelési módszertan)
CEN	**C**omité **E**uropeen de **N**ormalization (Európai Szabványügyi Bizottság)
CRL	**C**ertificate **R**evocation **L**ist (tanúsítvány visszavonási lista)
CWA	**C**EN **W**ork **A**greement (CEN munka megállapodás)
DHC	**D**ata **H**ashing **C**omponent (adatlenyomat-készítő összetevő)
DTBS	**D**ata **t**o **b**e **S**igned (aláírandó adat)
DTBSF	**D**ata **t**o **b**e **S**igned **F**ormatter (aláírandó adat formattáló)
DTBSR	**D**ata **t**o **b**e **S**igned Representation (aláírandó adat reprezentáció)
EAL	**E**valuation **A**ssurance **L**evel (értékelési garanciaszint)
ETSI	**E**uropean **T**elecommunication **S**tandard **I**nstitute
ETSI SR	**ETSI S**pecial **R**eport
ETSI TS	**ETSI T**echnical **S**pecification
FS	**F**unctional **S**pecification (funkcionális specifikáció)
GMT	**G**reenwich **M**ean **T**ime (greenwich-i középidő)
HLD	**H**igh **L**evel **D**esign (magas szintű terv)
ISO	**I**nternational **O**rganization for **S**tandardization
IT	**I**nformatin **T**echnology (informatika, információ technológia)
OCSP	**O**nline **C**ertificate **S**tatus **P**rotocol (valósidejű tanúsítvány állapot protokoll)
PKI	**P**ublic **K**ey **I**nfrastructure
PKITS	**P**ublic **K**ey **I**nteroperability **T**est **S**uite
PKIX	Internet **X**509 **PKI**
RFC	**R**equest **f**or **C**omment
RSA	**R**ivest, **S**hamir, and **A**dleman (az RSA algoritmus)
SAC	**S**igner's **A**uthentication **C**omponent (aláírót hitelesítő összetevő)
SAV	**S**ignature **A**ttribute **V**iewer (aláírási tulajdonság megjelenítő összetevő)
SCA	**S**ecure **C**reation **A**pplication (aláírás-létrehozó alkalmazás)
SCDev	**S**ignature-**C**reation **Dev**ice (aláírás-létrehozó eszköz)

SDC	**S**igner's **D**ocument **C**omposer (aláírói dokumentum szerkesztő)
SDOC	**S**igned **D**ata **O**bject **C**omposer (aláírt adat objektum szerkesztő)
SDP	**S**igner's **D**ocument **P**resenter (aláírói dokumentumot megjelenítő összetevő)
SHA	**S**ecure **H**ash **A**lgorithm
SIC	**S**igner's **I**nteraction **C**omponent (aláíróval kölcsönható összetevő)
SSA	**S**CDev - **S**CA **A**uthenticator (az aláírás-létrehozó eszköz és az aláírás-létrehozó alkalmazás közötti hitelesítés összetevője)
SSA	**S**CDev - **S**CA **A**uthenticator (az aláírás-létrehozó eszköz és az aláírás-létrehozó alkalmazás közötti hitelesítés összetevője)
SSL	**S**ecure **S**ockets **L**ayer -
ST	**S**ecurity **T**arget (biztonsági előirányzat)
SOF	**S**trenght **o**f **F**unction (funkcióerősség)
TLS	**T**ransaction **L**evel **S**ecurity
TOE	**T**arget **o**f **E**valuation (az értékelés tárgya)
TSF	**T**OE **S**ecurity **F**unctions (a TOE biztonsági funkcióinak összessége)
XML	E**x**tensible **M**arkup **L**anguage
XAdES	**X**ML **Ad**vanced **E**lectronic **S**ignature (XML formátumú elektronikus aláírás)
XMLDSIG	**XML-D**igital **Sig**nature Syntax and Processing

14 Felhasznált dokumentumok

14.1 A tanúsításhoz felhasznált kiinduló dokumentumok

- Kérdőív a tanúsítás kérelmezéséhez
- XadesMagic v1.0 Biztonsági előirányzat v1.0
- XadesMagic v1.0 Értékelési jelentés v1.0

14.2 Az értékeléshez felhasznált fejlesztői bizonyítékok

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

Cím	verzió	fájl név
XadesMagic elektronikus aláírás alkalmazás fejlesztő készlet fokozott biztonságú elektronikus aláíráshoz v1.0 - Biztonsági előirányzat	v1.0	XM_ST_v10.pdf
XadesMagic elektronikus aláírás alkalmazás fejlesztő készlet fokozott biztonságú elektronikus aláíráshoz v1.0 - Funkcionális specifikáció	v1.0	XM_FS_v10.doc és XadesMagic_Documentation.chm
XadesMagic elektronikus aláírás alkalmazás fejlesztő készlet fokozott biztonságú elektronikus aláíráshoz v1.0 - Magas szintű terv	v1.0	XM_HLD_v10.doc
XadesMagic elektronikus aláírás alkalmazás fejlesztő készlet fokozott biztonságú elektronikus aláíráshoz v1.0 - Megfeleltetés elemzések	v1.0	XM_RCR_v10.doc
XadesMagic elektronikus aláírás alkalmazás fejlesztő készlet fokozott biztonságú elektronikus aláíráshoz v1.0 - Adminisztrátori útmutató	v1.0	XM_AGD_v10.pdf
XadesMagic elektronikus aláírás alkalmazás fejlesztő készlet fokozott biztonságú elektronikus aláíráshoz v1.0 - Tesztelési dokumentáció	2006.09. 26.	XM-TestCollection_v10 (alkönyvtár, benne sok fájl)
XadesMagic elektronikus aláírás alkalmazás fejlesztő készlet fokozott biztonságú elektronikus aláíráshoz v1.0 - Teszt lefedettség elemzés	v1.0	XM_ATE_COV_v10.doc
XadesMagic elektronikus aláírás alkalmazás fejlesztő készlet fokozott biztonságú elektronikus aláíráshoz v1.0 - Teszt mélység elemzés	v1.0	XM_ATE_DPT_v10.doc
XadesMagic elektronikus aláírás alkalmazás fejlesztő készlet fokozott biztonságú elektronikus aláíráshoz v1.0 - A konfiguráció menedzselés dokumentációja	v1.0	XM_CM_v10.doc
XadesMagic elektronikus aláírás alkalmazás fejlesztő készlet fokozott biztonságú elektronikus aláíráshoz v1.0 - A fejlesztési biztonság dokumentációja	v1.0	XM_DVS_v10.doc
XadesMagic elektronikus aláírás alkalmazás fejlesztő készlet fokozott biztonságú elektronikus aláíráshoz v1.0 - Fejlesztői sebezhetőség elemzés	v1.0	XM_VA_v10.doc
A tesztelésre alkalmas értékelés tárgya (az SDA.E-Magic program segítségével tesztelhető fejlesztő készlet)		

14.3 Az értékeléshez felhasznált módszertani anyagok

Az értékelés az alábbi dokumentumokban leírt módszertant és eljárásrendet követte:

- MSZ/ISO/IEC 15408:2003 Informatika – Biztonságtechnika - Az informatikai biztonságértékelés közös szempontjai
- Common Criteria for Information Technology Security Evaluation (CC) Part 1: Introduction and general model - Version 2.3, August 2005
- Common Criteria for Information Technology Security Evaluation (CC) Part 2: Security functional requirements - Version 2.3, August 2005
- Common Criteria for Information Technology Security Evaluation (CC) Part 3: Security assurance requirements - Version 2.3, August 2005
- Common Methodology for Information Security Evaluation (CEM), Version 2.3, August 2005

14.4 Az értékeléshez felhasznált egyéb dokumentumok

Az értékelés figyelembe vette az alábbi mértékadó követelményrendszereket is:

- Az elektronikus aláírásról szóló 2001. évi XXXV.törvény
- CEN CWA 14170:2004 - Security requirements for signature creation applications
- CEN CWA 14171:2004 - General guidelines for electronic signature verification
- ETSI SR 102 176-1 v1.2.1 Electronic Signatures and Infrastructures (ESI) Algorithms and Parameters for Secure Electronic Signatures Part 1: Hash functions and asymmetric algorithms
- ETSI TS 101 903 v1.2.2 XML Advanced Electronic Signatures (XAdES)
- RFC 2560: PKIX - Online Certificate Status Protocol – OCSP
- RFC 3161 PKIX - Time-Stamp Protocol
- RFC 3275 XML Digital Signature Syntax and Processing (XMLDSIG)
- RFC 3280 PKIX - Certificate and Certificate Revocation List (CRL) Profile
- CEN CWA 14172-4:2001 munkacsoport egyezmény: Signature-creation application and general gudelines for electronic signature verification
- ETSI TS 101 733 v1.6.3 CMS Advanced Electronic Signatures (CAdES)
- RSA Rivest-Shamir-Adleman (public key cryptosystem) /ANSI X9.31/
- SHA-1 Secure Hash Algorithm /FIPS PUB 180-1/
- PKCS#1 RSA Cryptographic Standard /RFC2313/