TANÚSÍTÁSI JELENTÉS

XadesMagic v2.0.0
elektronikus aláírás alkalmazás
fejlesztő készletről
minősített elektronikus aláíráshoz

HUNG-TJ-53-2010

Verzió:	1.0
Fájl:	HUNG_TJ_53_2010_v10pdf
Minősítés:	Nyilvános
Oldalak:	34

Változáskezelés

Verzió	Dátum	A változás leírása
v0.01	2010.11.02	A szerkezet felállítása
v0.02	2010.11.20	A tanúsítás eredményeit tartalmazó teljes változat
v0.03	2010.11.21	A tanúsítás eredményeit tartalmazó, az értékelővel egyeztetett teljes változat
v1.0	**2010.11.23**	**Végleges verzió**

A tanúsítási jelentést készítette:

Juhász Judit
HunGuard Kft
Tanúsítási divízió

Tartalomjegyzék

1 Összefoglaló

1.1 Az értékelés jellemzői

Az értékelt termék neve:	**XadesMagic elektronikus aláírás alkalmazás fejlesztő készlet minősített elektronikus aláíráshoz**
Verzió szám:	**v2.0.0**
Rövid elnevezés:	**XadesMagic v2.0.0**
Az értékelt termék típusa:	Fejlesztő készlet (könyvtár)
Értékelő szervezet:	HunGuard Kft.
Értékelés befejezése:	2010. november 2.
Az értékelés módszere:	MIBÉTS
Az értékelés garanciaszintje:	Fokozott (EAL3)
Az értékelt termék funkcionalitása:	A fejlesztő készlet által támogatott nyilvános kulcsú szolgáltatások az alábbiak: • elektronikus aláírások létrehozása, • elektronikus aláírások ellenőrzése. Támogatja mind a fokozott biztonságú, mind a minősített elektronikus aláírásokat.
Konfigurációs követelmények:	Operációs rendszerek: • XP SP3, • Windows7, • Vista SP2 Fejlesztő környezet: .NET Framework 4.0 Minősített elektronikus aláírás létrehozásához biztonságos aláírás-létrehozó eszközök: • Gemalto TPC IM CC v3 (middleware: Classic Client Toolbox) • Giesecke StarCert v2.2 (middleware: SmartSign CSP for StarCert v1.0.9.15) Fokozott biztonságú elektronikus aláírás létrehozásához aláírás létrehozó eszköz: • eToken Pro 64K v4.2 (middleware: Aladdin eToken PKI Client v5.0.0.65)

2 Azonosítás

Az értékelt termék neve:	**XadesMagic elektronikus aláírás alkalmazás fejlesztő készlet minősített elektronikus aláíráshoz**
Verzió szám:	**v2.0.0**
Az értékelt termék alkotó elemei (a felhasználókhoz, vagyis a fejlesztő készlet felhasználásával alkalmazást fejlesztőkhöz kiszállított tételek):	• SDA.XadesMagic.dll (v2.0.0.2) • SDA.Cryptography.dll (v2.0.0.2) • SDA.Cryptography.Framework.dll (v2.0.0.2) • SDA.TimestampProtocol.dll (v2.0.0.2)

3 Biztonsági szabályzat

Ez a fejezet azokat a szabályokat írja le, melyek alapján a XadesMagic v2.0.0 irányítja az erőforrásaihoz való hozzáférést, s ezen keresztül minden általa ellenőrzött információt és szolgáltatást.
Először a XadesMagic v2.0.0 üzemmódjait határozzuk meg. Ezt követően a szabályokat érvényre juttató biztonsági funkciókat tekintjük át.

3.1 Üzemmód

Fokozott biztonságú aláírás létrehozás esetén a XadesMagic v2.0.0 képes együttműködni, mint kriptográfiai hardver eszközzel, mint PKCS#12 szoftveres kulcstároló állománnyal.

Minősített elektronikus aláírás esetén XadesMagic v2.0.0 képes együttműködni biztonságos aláírás létrehozó eszközzel (BALE).

3.2 Biztonsági funkciók

3.2.1 Elektronikus aláírás létrehozása

Egy elektronikus aláírás létrehozó rendszer (összhangban a [CWA 14170]-ben bevezetett modell elnevezéseivel) a következő **funkcionális összetevőkből** áll:

- az aláíróval kölcsönható összetevő,
- az aláírói dokumentumot megjelenítő összetevő,
- a dokumentumok szemantikai stabilitását ellenőrző összetevő,
- az aláírási tulajdonságokat megjelenítő összetevő,
- az aláírási szabályzatot kezelő/megvalósító összetevő,
- az aláírandó adatot formattáló és lenyomatoló összetevő,
- az aláírás-létrehozó eszköz interfészét irányító összetevő.

A XadesMagic függvényei egy aláírás létrehozó rendszer alábbi funkcionális összetevőit támogatják:

Az aláírási szabályzatot kezelő/megvalósító összetevő
A XadesMagic lehetővé teszi az aláíró számára az alkalmazandó aláírási szabályzat alábbi részeinek kezelését

- Aláírás helye (város, megye, ország, irányítószám)
- Szerepkör
- Xades típus (Xades-BES, Xades-EPES vagy Xades–T)
- Tartalom-formátum
- Lenyomatképző algoritmus
- Aláírás fajtája *(*Fokozott vagy Minősített)
- A kivárási idő figyelembe vételének kikapcsolása
- Időbélyeg szolgáltató kiválasztása
- Aláírás előtti időbélyeg használatának beállítása
- CRL és OCSP használata közötti választás (CRL(nincs OCSP) vagy Explicit OCSP szolgáltató vagy Tanúsítványban szereplő OCSP szolgáltató)
- Megtekinthető és aláírható típusok (dokumentum formátum/megjelenítő alkalmazás lista)
- Aláírás típusa (Elektronikus adat aláírása / Közjegyzői (ellenjegyző) aláírás)

Az aláírandó adatot formattáló és lenyomatoló összetevő
Az aláírandó adatot formattáló és lenyomatoló összetevő formattálja az aláírói dokumentumot és az aláírási tulajdonságokat, majd lenyomatolással (hash képzéssel) elkészíti a "Data To Be Signed Representation (DTBSR)"–nak nevezett információt, mely az SCDev-nek lesz továbbítva az aláírás végrehajtásához.

Az XadesMagic a FIPS PUB 180-3 dokumentumban specifikált lenyomatoló algoritmusokat (SHA1, SHA224, SHA256, SHA384, SHA512) támogatja:

Az aláírás-létrehozó eszköz interfészét irányító összetevő
Az aláírás-létrehozó eszköz interfészét irányító összetevő az SCDev-vel való kölcsönhatásra szoftver és/vagy middleware komponenseket használ.

A XadesMagic az értékelt konfigurációban az SCDev-el való kölcsönhatásra az alábbi middleware komponenseket használja:
Fokozott biztonságú elektronikus aláírás esetén:
- Aladdin eToken PKI Client v5.0.0.65 (eToken Pro 64K v4.2 SCDev esetén)

Minősített elektronikus aláírás esetén:
- SmartSign CSP for StarCert v1.0.9.15 (Giesecke StarCert v2.2 SSCD esetén)
- Classic Client Toolbox (Gemalto TPC IM CC v3 SSCD esetén)

A fenti middleware-ek a TOE hatókörén kívül áll.

3.2.2 Elektronikus aláírás ellenőrzése

Egy általános aláírás ellenőrző modul az alábbi **funkcionális összetevők**et tartalmazza:
- a felhasználóval kölcsönható összetevő,
- az alkalmazandó aláírási szabályzatot kiválasztó összetevő,
- a dokumentumok szemantikai stabilitását ellenőrző összetevő,
- a dokumentum megjelenítő alkalmazásokat végrehajtó összetevő,
- az érvényesítő adatokat összegyűjtő és feldolgozó összetevő,
- a digitális aláírásokat ellenőrző összetevő,
- az aláírási szabályzatokat adminisztráló összetevő.

A XadesMagic függvényei az E-Magic (és más aláírás ellenőrző modulok) alábbi funkcionális összetevőit támogatják:

Az érvényesítő adatokat összegyűjtő és feldolgozó összetevő

A XadesMagic a következő módon képes begyűjteni az érvényesítő adatokat:
- letölti a tanúsítványban szereplő helyről a CRL-t,
- letölti a tanúsítványban szereplő helyről az OCSP-t.

Az érvényességi adatok összegyűjtésénél HTTP hálózati protokollt használ.

A XadesMagic az érvényesítő adatok feldolgozása során a következő funkciókat biztosítja:
- a digitális aláírás elhelyezése az időben,
- az aláíró tanúsítványának megfelelőség ellenőrzése,
- érvényes tanúsítványlánc felépítése,
- tanúsítványlánc érvényességének ellenőrzése.

A XadesMagic a ***digitális aláírás időbeli elhelyezése*** során eltérően viselkedik a két működési módjában:

- A „kezdeti ellenőrzés” működési módban, ha még nincs időhivatkozás, összegyűjti ezt az aláírási szabályzatnak megfelelően.
- Az „utólagos ellenőrzés” működési módban felhasználja a kezdeti ellenőrzés során meghatározott időhivatkozást, ha ez létezik. Amennyiben hiányzik, akkor az elektronikus aláírást „érvénytelen” állapotúnak nyilvánítja.

A XadesMagic az ***aláíró tanúsítványának megfelelőség ellenőrzése*** funkción belül az aláíró tanúsítványra (mely közvetlenül, vagy hivatkozásán keresztül közvetve szerepel az aláírási tulajdonságok között) ellenőrzi az aláírási szabályzat követelményeinek teljesülését:

- a tanúsítványhoz tartozó kulcs algoritmusának ellenőrzése (csak az RSA lehet),
- a tanúsítvány kulcs lenyomat algoritmusának ellenőrzése (csak FIPS PUB 180-3 szerintiek lehetnek),
- a tanúsítvány kulcs hosszának ellenőrzése (csak 1020-nál nagyobb lehet),
- a tanúsítvány lejártának az ellenőrzése
- a tanúsítvány visszavonási címének ellenőrzése (van e CDP kiterjesztés),
- a tanúsítvány kritikus kiterjesztéseinek vizsgálata (csak az aláírási szabályzatban meghatározott kritikus kiterjesztést tartalmazhat),
- minősített elektronikus aláírás azonosítása (a tanúsítványban szerepel-e a QCStatement kiterjesztés az id-etsi-qcs-QcCompliance OID-vel),
- a kulcshasználat kiterjesztés helyességének ellenőrzése (minősített elektronikus aláírás esetén a NonRepudiation flag értéke igaz, a többi hamis, fokozott biztonságú elektronikus aláírás esetén csak a DigitalSignature flag vagy a NonRepudiation flag értéke lehet igaz, de legalább az egyiküknek igaznak kell lennie)

A XadesMagic az **érvényes tanúsítványlánc felépítése** funkción belül (annak érdekében, hogy meggyőződjön az aláírói tanúsítvány érvényességéről és hitelességéről a digitális aláírás időpontjában) egy érvényes tanúsítványláncot keres az aláíró tanúsítványa és a Windows tanúsítvány tárban lévő egyik megbízható pont között.
A XadesMagic ezt a két működési módjában eltérő módon valósítja meg:

- A „kezdeti ellenőrzés” működési módban, a tanúsítványlánc felépítése során importálja az érvényesítő adatokat (a hálózatról), egyben ellenőrzi ezek érvényességét az alkalmazott aláírási szabályzatban meghatározott szabályok szerint.
  Amennyiben megállapítja, hogy nem építhető ki tanúsítványlánc, vagy minden felépített tanúsítványlánc érvénytelen, akkor az elektronikus aláírást „érvénytelen” állapotúnak nyilvánítja.
  Amennyiben megállapítja, hogy nem elérhetők olyan adatok, melyek tanúsítják, hogy a tanúsítványlánc egy eleme nem került visszavonásra, akkor az elektronikus aláírást „még nem eldönthető” állapotúnak nyilvánítja, s a kezdeti ellenőrzés később ismét végrehajtható lesz.
- Az „utólagos ellenőrzés” működési módban rekonstruálja a tanúsítványláncot és érvényességét pusztán a kezdeti ellenőrzés során összegyűjtött adatok alapján ellenőrzi.
  Amennyiben megállapítja, hogy az elérhető adatokból nem lehet tanúsítványláncot felépíteni, vagy az ezekből az elérhető adatokból felépíthető összes tanúsítványlánc érvénytelen, akkor az elektronikus aláírást „érvénytelen” állapotúnak nyilvánítja.

Amennyiben a tanúsítványlánc egy elemére hiányzik olyan adat, mely tanúsítja annak nem visszavont állapotát, akkor az elektronikus aláírást „érvénytelen" állapotúnak nyilvánítja.

A XadesMagic a ***tanúsítvány érvényességének ellenőrzése*** funkción belül ellenőrzi a tanúsítványláncot alkotó összes tanúsítvány érvényességét, felhasználva ehhez a digitális aláírásban meghatározott idő referenciát, valamint a tanúsítványban megadott érvényességi periódust.
A tanúsítványlánc egy elemének az érvényesség ellenőrzése során a XadesMagic a következő ellenőrzéseket végzi:

- az elem sértetlensége és eredet hitelessége, a hozzá tartozó aláírás felhasználásával;
- az aláírásban meghatározott idő hivatkozás időpontjának az elem érvényességi periódusba esése;
- az elem nem visszavontsága az aláírásban meghatározott idő hivatkozás időpontjában.

A digitális aláírásokat ellenőrző összetevő
A digitális aláírásokat ellenőrző összetevő a digitális aláírások ellenőrzéséhez szükséges (hash és aláírás ellenőrző) algoritmusokat támogató kriptográfia összetevő, melyet az ellenőrző folyamat hív meg.

Az XadesMagic esetében ez az összetevő az összes alábbi típusú digitális aláírást ellenőrzi:

- a dokumentum digitális aláírása,
- a tanúsítványláncot alkotó tanúsítványok digitális aláírásai,
- a hiteles gyökér tanúsítvány (megbízható pont) digitális aláírása,
- az összegyűjtött érvényesítő adatokhoz (CRL, OCSP válaszok, időbélyeg tokenek,...) tartozó digitális aláírások.

Az aláírási szabályzatokat adminisztráló összetevő

Az XadesMagic 2.0.0 lehetővé teszi az ellenőrző számára, hogy a már beállított aláírási szabályzat alkalmazását pontosítsa:

- Xades-T (az ellenőrzés során időbélyeget helyez el az aláíráson)
- Xades-C (az ellenőrzés során begyűjti és csatolja az ellenőrzési adatokat)
- Xades-X (az ellenőrzés során begyűjti és csatolja az ellenőrzési adatokat és a tanúsítványok adatait időbélyeggel védi meg)
- Xades-X-L (az ellenőrzés során a begyűjtött és csatolt ellenőrzési adatokat (tanúsítványok, visszavonási információk) időbélyeggel védi meg)
- Xades-A (az ellenőrzés során a teljes elektronikus aláírást archív időbélyeggel védi meg)

4 Feltételezések és hatókör

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

Ezek a feltételek (melyeket a XadesMagic nem kezel, nem kényszerít ki, hanem elvárja, hogy az informatikai és a nem informatikai környezete teljesítse) az alábbiak:

4.1 Elektronikus aláírás létrehozására és ellenőrzésére vonatkozó közös feltételek

OE.Host_Platform
Az a hoszt platform, melyre a TOE-t telepítették, vagy közvetlenül az aláíró/ellenőrző, vagy egy olyan szervezet felügyelete alatt álljon, amely garantálja az aláíró/ellenőrző számára, hogy az alábbi biztonsági intézkedéseket ténylegesen alkalmazzák.
A hoszt platform operációs rendszere elkülönített futási környezetet biztosítson az általa futtatott alkalmazások számára, továbbá:

- a hoszt védett legyen a vírustámadásokkal szemben;
- a hoszt platform és nyílt hálózati kapcsolattal rendelkező egyéb IT elemek közötti kommunikáció tűzfallal védett legyen;
- a hoszt platform adminisztrátori funkcióihoz való hozzáférés a platform adminisztrátorokra korlátozott ("hoszt adminisztátor") legyen. A felhasználói fiók különbözzön a hoszt adminisztrátoritól.
- a hoszt platform szoftverének telepítése és frissítése a hoszt adminisztrátor ellenőrzése alatt álljon;
- a hoszt platform operációs rendszere ne engedje meg nem megbízható alkalmazások végrehajtását;
- a hoszt kellő pontosságú rendszeridőt biztosít.

OE.Document_Presentation
Annak a hosztnak, melyre a TOE-t telepítették legyen egy vagy több olyan megjelenítő alkalmazása, mely:

- vagy pontosan megjeleníti az aláírandó/aláírt dokumentumot,
- vagy figyelmezteti az aláírót/ellenőrzőt a megjelenítő alkalmazás és a dokumentum jellemzői közötti lehetséges inkompatibilitási problémákról.

Aláírás létrehozás esetén, amennyiben az aláírandó dokumentum már maga is tartalmaz aláírásokat, a TOE környezete az aláíró számára tegye lehetővé legalább az előzetesen aláírók személyének megismerését, legjobb esetben ezen aláírások ellenőrzését is.

OE .Trusted_Security_Administrator
Az aláíró/ellenőrző legyen megbízható, a TOE használatára kiképzett, s rendelkezzen a feladatai ellátásához szükséges eszközökkel.
A hoszt gép adminisztrátora legyen megbízható, s rendelkezzen a feladatai ellátásához szükséges eszközökkel.

4.2 Kizárólag az elektronikus aláírás létrehozására vonatkozó feltételek

OE.SCDev
Az SCDev-nek képesnek kell lennie a TOE-tól kapott adatokból digitális aláírást létrehozni.
Az SCDev-nek hitelesítenie kell az aláírót, lehetővé téve számára a kiválasztott tanúsítványnak megfelelő magánkulcs aktivizálását.
Az SCDev felelős az aláíró adatainak megvédéséért. Az SCDev-nek az alábbi adatokat biztonságos módon kell tárolnia és használnia:

- az aláírás létrehozásával kapcsolatos adatok:
  - az aláíró magánkulcsa (bizalmasság és sértetlenség)
  - az aktuális tanúsítványok, vagy az aláíró tanúsítványára való hivatkozás (sértetlenség)
  - a magánykulcs és a tanúsítvány összetartozása (sértetlenség)
- az aláíró hitelességével kapcsolatos adatok:
  - az aláíró hitelesítő adata (bizalmasság és sértetlenség)
  - a hitelesítő adatok és a magánkulcs/tanúsítvány pár összetartozása (sértetlenség).

OE.TOE/SCDev_Communications
A TOE és az SCDev közötti interfészt biztosító szoftver és/vagy hardver összetevőknek kezelniük (megnyitni/lezárni) kell tudniuk egy biztonságos csatornát, mely garantálja a kommunikáció kizárólagosságát és sértetlenségét.

OE.Signatory_Authentication_Data_Protection
Azoknak a szoftver és hardver összetevőknek, melyek lehetővé teszik az aláíró hitelesítését az SCDev felé a kiválasztott tanúsítványnak megfelelő magánkulcs aktivizálása érdekében, garantálniuk kell a hitelesítő adatok bizalmasságát és sértetlenségét az adatok bevitele és az SCDev felé történő továbbítás során.

OE.Signatory_Presence
Az aláírónak jelen kell lennie a dokumentumok aláírási szándékának kinyilvánításától kezdve egészen addig, amíg hitelesítő adatainak megadásával aktivizálja aláíró kulcsát.

4.3 Kizárólag az elektronikus aláírás ellenőrzésére vonatkozó feltételek

OE.Validation_Data_Provision
A TOE környezete biztosítsa az aláírás ellenőrzéséhez szükséges érvényesítő adatokat.

5 A XadesMagic v2.0.0 szerkezeti leírása

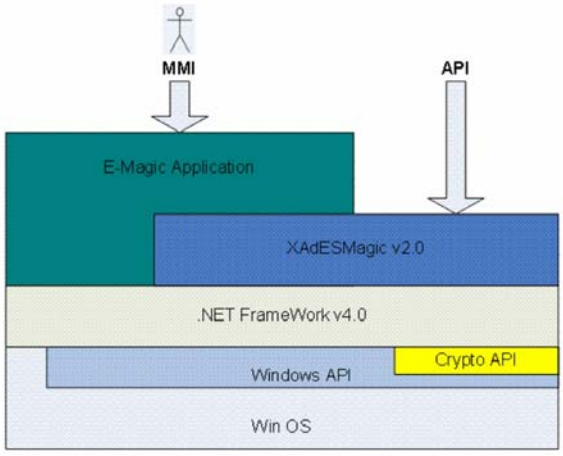
Az E-Magic + XadesMagic egy olyan speciális elektronikus aláírás termék, melynek fő funkciója elektronikus aláírások biztonságos létrehozása és ellenőrzése. A fokozott biztonságú és a minősített elektronikus aláírásokat egyaránt támogatják. Az E-Magic egy Windows alkalmazás, a XadesMagic pedig az ennek alapját képező szoftver fejlesztőkészlet. A XadesMagic számos más aláíró alkalmazásnak is alapja lehet.

Az E-Magic + XadesMagic az alábbi szabványoknak, illetve ajánlásoknak megfelelő működést biztosít:

- RFC 2560 OCSP kérés előállítás, valamint OCSP és OCSP válasz ellenőrzés
- RFC 3161 Időbélyeg kérés, valamint az időbélyeg és időbélyeg válasz ellenőrzés
- RFC 5280 Tanúsítványok és CRL-ek ellenőrzése, tanúsítási útvonal felépítése és érvényesítése. A tanúsítványlánc felépítésénél az alábbi kiterjesztéseket támogatja:
    - ExtendedKeyUsage
    - KeyUsage
    - BasicConstraints
    - CRLDistributionPoints
    - SubjectAlternativeName
    - IssuerAlternativeName
- Egységes MELASZ formátum elektronikus aláírásokra v2.0 (MMM-001: 2008, v2.0)

5.1 Az értékelés tárgya biztonsági környezete és határai

Az (E-Magic + XadesMagic)-t alkotó fizikai összetevőket és környezetét szemlélteti az 1. ábra.



1. ábra Az E-Magic + XadesMagic fizikai elemei

Az értékelés tárgyának összetevői:

- E-Magic aláíró alkalmazás
- XadesMagic (önállóan is meghívható fejlesztő készlet)
- Felhasználói dokumentáció (E-Magic)
- Fejlesztői dokumentáció (XadesMagic)

Az értékelés tárgya az alábbi informatikai elemekből álló környezetben működőképes:

- Windows operációs rendszerek (XP SP3, Windows7, Vista SP2),
- Windows API (benne CryptoAPI),
- fejlesztő környezet (.NET Framework 4.0)
- minősített elektronikus aláírás létrehozásához: biztonságos aláírás-létrehozó eszköz, a hozzátartozó middleware-rel
- fokozott biztonságú elektronikus aláírás létrehozásához: aláírás-létrehozó eszköz a hozzátartozó middleware-rel, vagy Microsoft CryptoAPI (külön hardver eszköz nélkül).

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
- Doc-O-Matic_20101119 a fejlesztő készlet leírása. A dokumentáció leírja a fejlesztő készlet osztályhierarchiáját, és az egyes osztályok felépítését

7 Tesztelés

7.1 A fejlesztők tesztelése

Teszt környezet:
A tesztelést a következő környezetekben végezte el a fejlesztő:

- Windows 7, .Net Framework 4.0
- Windows Vista SP2, .Net Framework 4.0

A fejlesztői teszt felépítése:
A fejlesztő 7 csoportban 81 tesztesetet futtatott le.

- XMLDsig–re vonatkozó tesztesetek (1.1.- 1.15.) 28 teszt eset.
- Tanúsítvány-ra vonatkozó tesztesetek (2.1.- 2.9) 16 teszt eset.
- XAdES–re vonatkozó tesztesetek (3.1.- 3.7) 16 teszt eset.
- Időbélyeg–re vonatkozó tesztesetek (4.1.- 4.5) 11 teszt eset.
- OCSP–re vonatkozó tesztesetek (5.1.- 5.4) 3 teszt eset.
- CRL–re vonatkozó tesztesetek (6.1.- 6.4) 3 teszt eset.
- CounterSignature–re vonatkozó tesztesetek (7.1.) 4 teszt eset.

A tesztesetek előre elkészített pozitív és esetlegesen ezekből átalakított negatív XML aláírói állományok adott operációs rendszer alatti ellenőrzéséből állnak.

A tesztesetek eredménye minden esetben megfeleltek az elvárt eredményeknek.

7.2 Az értékelők tesztelése

Teszt környezet:
Az értékelés során a következő környezetben került tesztelésre a XadesMagic v2.0.0.2 fejlesztő készlet:

- Windows XP SP3, .Net Framework 4.0

Tesztesetek
A független tesztelés

- a fejlesztői tesztek Windows XP SP3-on történő megismétléséből, valamint
- a XadesMagic v2.0.0.2 fejlesztő készlet RFC 5280-nak való megfelelésének vizsgálatából állt (PKITS-tesztkészlet).

A fejlesztői tesztek megismétlése sikeresen hiba nélkül lefutottak. A tesztesetek eredménye minden esetben megfeleltek az elvárt eredményeknek.

A PKITS tesztekből a XadesMagic v2.0.0.2 az alábbi tesztcsoportokat vállalta fel:

- Aláírás ellenőrzése
- Érvényességi idő ellenőrzése
- Név lánc ellenőrzése
- Alapvető típusmegkötések ellenőrzése
- Kulcshasználat ellenőrzése
- Kritikus és nem kritikus kiterjesztések ellenőrzése

A felvállalt tanúsítvány kiterjesztések kezelése megfelelt a PKITS tesztkörnyezet elvárásainak.

8 Az értékelt konfiguráció

Értékelt E-Magic verzió: 2.0.0.3

Értékelt XadesMagic verzió: 2.0.0.2, mely az alábbi dll-ekből áll:

SDA.XadesMagic.dll v2.0.0.2
```
SHA1:   dd0a3e7f45b4119b9918319fd2aff19c7c9664c2
SHA256: e0c8667cf943a39b3c578ecf600afcf625c308cff122c0b7ae749fb7e491ec08
```

SDA.Cryptography.dll v2.0.0.2
```
SHA1:   8c8ff8a5df17583114d49a5140a9b41525b2de69
SHA256:4da4b1d24aa432bae6d3fc1d3fdbd1c86f318980a89a3f096a31682fba842e70
```

SDA.Cryptography. Framework.dll v2.0.0.2
```
SHA1:   90f03589b9d771158bc55112285c9bce07252429
SHA256: 5afb89495caf6904a157031dba433ad03ea8cd099bae13325880819c5907a911
```

SDA.Cryptography.TimeStampProtocol.dll v2.0.0.2
```
SHA1:   2d910fbbdbefb129d47210b5c6d7f415ee562b43
SHA256: c8754106282793eec196e6d2af1e6eaab13e6a634112c7b1cdbae595bd546816
```

Az értékelt konfiguráció elemei:

Operációs rendszerek:
- XP SP3,
- Windows7,
- Vista SP2

Fejlesztő környezet: .NET Framework 4.0

Minősített elektronikus aláírás létrehozásához biztonságos aláírás-létrehozó eszközök:
- Gemalto TPC IM CC v3 (middleware: Classic Client Toolbox)
- Giesecke StarCert v2.2 (middleware: SmartSign CSP for StarCert v1.0.9.15)

Fokozott biztonságú elektronikus aláírás létrehozásához aláírás létrehozó eszköz:
- eToken Pro 64K v4.2 (middleware: Aladdin eToken PKI Client v5.0.0.65)

9 Az értékelés eredményei

XadesMagic elektronikus aláírás alkalmazás fejlesztő készlet minősített elektronikus aláíráshoz termék értékelése az E-Magic elektronikus aláírás alkalmazással együtt történt. Az E-Magic alkalmazás a XadesMagic fejlesztői könyvtár szolgáltatásaira épülve végez elektronikus aláírást és ellenőrzést.

Az E-Magic + XadesMagic értékelés az informatikai termékek technológia szempontú biztonsági értékelésére kidolgozott MIBÉTS (Magyar Informatikai Biztonsági Értékelési és Tanúsítási Séma) módszertant használta.

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 felel meg.

Az értékelés fő következtetése az alábbi:

Az E-Magic (elektronikus aláírás alkalmazás) v2.0.0 + XadesMagic (elektronikus aláírás alkalmazás fejlesztő készlet minősített elektronikus aláíráshoz) v2.0.0 megfelel biztonsági előirányzatának, kielégíti az abban megfogalmazott funkcionális és garanciális biztonsági követelményeket.

9.1 A biztonsági előirányzat értékelése

Ez az alfejezet az E-Magic + XadesMagic biztonsági előirányzata értékelési eredményeit foglalja össze.

Az értékelés alapja az alábbi dokumentum:

Biztonsági előirányzat	XM_biztonsagi_eloiranyzat_v20	2.0

Garancia-osztály	Garancia-összetevő	Az értékelés eredménye
Biztonsági előirányzat	ASE_INT.1 Bevezetés	A követelményeknek **megfelelt**.
	ASE_CCL.1 Megfelelőségi nyilatkozatok	A követelményeknek **megfelelt**.
	ASE_SPD.1 Biztonsági probléma meghatározás	A követelményeknek **megfelelt**.
	ASE_OBJ.1 Biztonsági célok	A követelményeknek **megfelelt**.
	ASE_ECD.1 Kiterjesztett biztonsági követelmények	A követelményeknek **megfelelt**.
	ASE_REQ.1 Biztonsági követelmények	A követelményeknek **megfelelt**.
	ASE_TSS.1 Az értékelés tárgya összefoglaló előírása	A követelményeknek **megfelelt**.

9.2 A fejlesztés értékelése

Ez az alfejezet az E-Magic + XadesMagic tervezési dokumentációit értékeli a biztonsági funkcióik megfelelő leírása és magyarázata szempontjából.

Az értékelés alapját az alábbi fejlesztői bizonyítékok képezték:

Biztonsági előirányzat	XM_biztonsagi_eloiranyzat_v20.doc	2.0
Biztonsági szerkezet leírás	XM_biztonsagi_szerkezet_v20.doc	2.0
Funkcionális specifikáció	XM_funkcionalis_specifikacio_v20.doc	2.0
TOE terv	XM_TOE_terv_v20.doc	2.0
Felhasználói dokumentáció	EMagicFelhasznaloiDokumentacio_v20.doc	2.0

Garancia-osztály	Garancia-összetevő	Az értékelés eredménye
Fejlesztés	ADV_ARC.1 A biztonsági szerkezet leírás	A követelményeknek **megfelelt**.
	ADV_FSP.3 A funkcionális specifikáció teljes összegzéssel	A követelményeknek **megfelelt**.
	ADV_TDS.2 Szerkezeti terv	A követelményeknek **megfelelt**.

9.3 Az útmutatók értékelése

Ez az alfejezet az E-Magic + XadesMagic útmutató dokumentációját értékeli.

Az értékelés alapját az alábbi fejlesztői bizonyítékok képezték:

Biztonsági előirányzat	XM_biztonsagi_eloiranyzat_v20.doc	2.0
Funkcionális specifikáció	XM_funkcionalis_specifikacio_v20.doc	2.0
TOE terv	XM_TOE_terv_v20.doc	2.0
Felhasználói dokumentáció	EMagicFelhasznaloiDokumentacio_v20.doc	2.0
Felhasználói leírás fejlesztőknek	Doc-O-Matic_20101119 a fejlesztő készlet leírása	2.0.0.2

Garancia-osztály	Garancia-összetevő	Az értékelés eredménye
Útmutató dokumentumok	AGD_PRE.1 Az előkészítő eljárások	A követelményeknek **megfelelt**.
	AGD_USR.1 Az üzemeltetési felhasználói útmutató	A követelményeknek **megfelelt**.

9.4 Az életciklus támogatás értékelése

Ez az alfejezet az E-Magic + XadesMagic fejlesztése során a fejlesztői környezetben betartott biztonsági intézkedéseket értékeli.

Az értékelés alapját az alábbi fejlesztői bizonyítékok képezték:

Biztonsági előirányzat	XM_biztonsagi_eloiranyzat_v20.doc	2.0
A tesztelésre alkalmas E-Magic + XadesMagic	E-Magic: SDA.E-Magic.exe XadesMagic: 4 dll	2.0.0.3 2.0.0.2
Konfiguráció lista	XM_konfiguracio_lista_v20.doc	2.0
A konfiguráció kezelés dokumentációja	XM_konfiguracio_kezeles_v20.doc	2.0
A fejlesztés biztonság dokumentációja	XM_fejlesztes_biztonsag_v20.doc	2.0
Az életciklus meghatározás dokumentációja	XM_eletciklus_meghatarozas_v20.doc	2.0

Garancia-osztály	Garancia-összetevő	Az értékelés eredménye
Életciklus támogatás	ALC_CMC.3 Engedélyezéssel kapcsolatos intézkedések	A követelményeknek **megfelelt**.
	ALC_CMS.3 A megvalósítási reprezentáció CM lefedettsége	A követelményeknek **megfelelt**.
	ALC_DEL.1 A szállítási eljárások	A követelményeknek **megfelelt**.
	ALC_DVS.1 A biztonsági intézkedések azonosítása	A követelményeknek **megfelelt**.
	ALC_LCD.1 A fejlesztő által meghatározott életciklus modell	A követelményeknek **megfelelt**.

9.5 A tesztelés értékelése

Ez az alfejezet azt vizsgálja és értékeli, hogy az E-Magic + XadesMagic a tervdokumentációkban megadottaknak megfelelően működik-e, valamint összhangban van-e a biztonsági előirányzatában megfogalmazott funkcionális biztonsági követelményeivel.

Az értékelés alapját az alábbi fejlesztői és értékelői bizonyítékok képezték:

Biztonsági előirányzat	XM_biztonsagi_eloiranyzat_v20.doc	2.0
Biztonsági szerkezet leírás	XM_biztonsagi_szerkezet_v20.doc	2.0
Funkcionális specifikáció	XM_funkcionalis_specifikacio_v20.doc	2.0
TOE terv	XM_TOE_terv_v20.doc	2.0
Felhasználói dokumentáció (E-Magic)	EMagicFelhasznaloiDokumentacio_v20.doc	2.0
A konfiguráció kezelés dokumentációja	XM_konfiguracio_kezeles_v20.doc	2.0
A tesztelésre alkalmas E-Magic + XadesMagic	E-Magic: SDA.E-Magic.exe XadesMagic: 4 dll	2.0.0.3 2.0.0.2
Tesztelési dokumentáció	XM-TestCollection_v20 alkönyvtár	2.0
Teszt lefedettség elemzés	XM_teszt_lefedettseg_v20.doc	2.0
Teszt mélység elemzés	XM_teszt_melyseg_v20.doc	2.0

Garancia-osztály	Garancia-összetevő	Az értékelés eredménye
Tesztelés	ATE_FUN.1 A funkcionális tesztelés	A követelményeknek **megfelelt**.
	ATE_COV.2 A teszt lefedettség elemzés	A követelményeknek **megfelelt**.
	ATE_DPT.1 Az alap terv tesztelése	A követelményeknek **megfelelt**.
	ATE_IND.2 A független tesztelés	A követelményeknek **megfelelt**.

9.6 A sebezhetőség értékelése

Ez az alfejezet az E-Magic + XadesMagic-ben lévő hibák, gyengeségek meglétét és a velük való visszaélések lehetőségét kívánja meghatározni vagy kizárni. Mindez a fejlesztő és az értékelő elemzésén alapul, valamint értékelői tesztelés egészíti ki.

Az értékelés alapját az összes fejlesztői bizonyíték képeztek (lásd 14.2)

Garancia-osztály	Garancia-összetevő	Az értékelés eredménye
A sebezhetőség felmérése	AVA_VAN.2 A sebezhetőség vizsgálat	A követelményeknek **megfelelt**.

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 v2.0.0 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.

A fent leírt külön vizsgálatnak a következtetése az alábbi:

A XadesMagic v2.0.0 fejlesztő készlet (A 4. 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.**

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

11.1 A XadesMagic v2.0.0 megfelelése a funkcionális követelményeknek

Funkcionális követelmény	Teljesülés	Teljesülés módja
F_SCA_1	**megfelel**	**megvalósít**
F_SDP_1	**megfelel**	**kezel, tárol**
F_SDP_2	**megfelel**	**kezel, tárol**
F_SDP_3	**megfelel**	**kezel, tárol**
F_SAV_1	**megfelel**	**kezel, tárol**
F_SAV_2	**megfelel**	**kezel, tárol**
F_SAV_3	**megfelel**	**támogat**
F_SIC_1	**nem vonatkozik rá a követelmény**	**-**
F_SIC_2	**nem vonatkozik rá a követelmény**	**-**
F_DTBSF_1	**megfelel**	**megvalósít**

Funkcionális követelmény	Teljesülés	Teljesülés módja
F_DTBSF_2	**megfelel**	**megvalósít**
F_DHC_1	**megfelel**	**megvalósít**
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**	**megvalósít**
F_I/O-1	**nem vonatkozik rá a követelmény**	**-**
F_I/O-2	**megfelel**	**megvalósít**
F_I/O-3	**megfelel**	**megvalósít**
F_ISV-1	**megfelel**	**megvalósít**
F_ISV-2	**megfelel**	**megvalósít**
F_ISV-3	**megfelel**	**megvalósít**
F_USV-1	**megfelel**	**megvalósít**
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	**nem vonatkozik rá a követelmény**	**-**
F_human_5	**nem vonatkozik rá a követelmény**	**-**
F_human_6	**nem vonatkozik rá a követelmény**	**-**
F_human_7	**megfelel**	**megvalósít, támogat**
F_machine_1	**megfelel**	**megvalósít, támogat**
F_machine_2	**megfelel**	**megvalósít, támogat**

Funkcionális követelmény	Teljesülés	Teljesülés módja
F_general_1	**nem vonatkozik rá a követelmény**	**-**
F_protocol	**megfelel**	**megvalósít**
F_format	**megfelel**	**megvalósít**
F_principles	**nem vonatkozik rá a követelmény**	**-**

11.2 A XadesMagic v2.0.0 megfelelése a biztonsági követelményeknek

Biztonsági követelmény	Teljesülés	Teljesülés módja
S_SCA_1	**feltétellel megfelel** **OE.TOE/SCDev_Communications**	**részben megvalósít**
S_SCA_2	**feltétellel megfelel** **OE.Signatory_Authentication_Data_Protection**	**részben megvalósít** + **külső környezeti elvárás**
S_SCA_3	**megfelel**	**megvalósít**
S_SCA_4	**megfelel**	**megvalósít**
S_SCA_5	**megfelel**	**támogat**
S_SCA_6	**megfelel**	**támogat**
S_SCA_7	**nem vonatkozik rá a követelmény**	**-**
S_SCA_8	**nem vonatkozik rá a követelmény**	**-**
S_SCA_9	**feltétellel megfelel** **OE.Host_Platform**	**részben megvalósít** + **külső környezeti elvárás**
S_SCA_10	**megfelel**	**megvalósít**
S_SCA_11	**megfelel**	**megvalósít**
S_SCA_12	**megfelel**	**megvalósít**
S_SDP_1	**megfelel**	**megvalósít**
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	**megfelel**	**támogat**
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**	**megvalósít**
S_SDP_11	**megfelel**	**megvalósít**

Biztonsági követelmény	Teljesülés	Teljesülés módja
S_SDP_12	**nem vonatkozik rá a követelmény**	**-**
S_SAV_1	**megfelel**	**megvalósít**
S_SAV_2	**megfelel**	**megvalósít**
S_SAV_3	**megfelel**	**megvalósít**
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	**nem vonatkozik rá a követelmény**	**-**
S_SIC_3	**nem vonatkozik rá a követelmény**	**-**
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** **OE.Signatory_Authentication_Data_Protection**	**részben megvalósít** + **külső környezeti elvárás**
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**	**-**

Biztonsági követelmény	Teljesülés	Teljesülés módja
S_SAC_12	**nem vonatkozik rá a követelmény**	**-**
S_DTBSF_1	**megfelel**	**megvalósít**
S_DHC_1	**megfelel**	**megvalósít**
S_DHC_2	**nem vonatkozik rá a követelmény**	**-**
S_DHC_3	**megfelel**	**megvalósít**
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** **OE.Host_Platform**	**részben megvalósít** **+** **külső környezeti elvárás**
S_I/O_2	**feltétellel megfelel** **OE.Host_Platform**	**részben megvalósít** **+** **külső környezeti elvárás**
S_I/O_3	**nem vonatkozik rá a követelmény**	**-**
S_VER_1	**feltétellel megfelel** **OE.Host_Platform**	**részben megvalósít** **+** **külső környezeti elvárás**

11.3 A tanúsított termékek listájába javasolt szöveg

Jelenleg Magyarországon 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 és minősített 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, RSA algoritmus támogatással.*
- *Aláírás létrehozáshoz lenyomat készítése SHA-1, ,SHA-224, SHA-256, SHA-384, SHA-512, algoritmusokkal.*
- *Időbélyeg kérése és ellenőrzése.*
- *Visszavonási információ kérése és ellenőrzése (CRL, OCSP).*

Ennek alapján a XadesMagic v2.0.0 fejlesztői készlet segítségével olyan alkalmazások fejleszthetők, melyek a nyilvános kulcsú technológia alapján bizalmasságot, sértetlenséget, hitelesítést és letagadhatatlanságot biztosító szolgáltatásokat képesek nyújtani."

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

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 fejlesztőkészletet, vagy az erre épülő aláíró alkalmazásokat használja, azaz a XadesMagic szolgáltatásait igénybe veszi.

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.

13.2 Rövidítések

Az alábbiakban meghatározzuk a jelen értékelési jelentésben használt betűszavak jelentését.

API	**A**pplication **P**rogramming **I**nterface
BALE	**B**iztonságos **a**láírás **l**étrehozó **e**szköz
CC	**C**ommon **C**riteria (Közös szempontok)
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)
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 TS	**ETSI T**echnical **S**pecification
MIBÉTS	**M**agyar **I**nformatikai **B**iztonsági **É**rtékelési és **T**anúsítási **S**éma
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)
SSCD	**S**ecure **S**ignature-**C**reation **Dev**ice (biztonságos aláírás-létrehozó eszköz)
TOE	**T**arget **o**f **E**valuation (az értékelés tárgya)

XML E**x**tensible **M**arkup **L**anguage

XAdES **X**ML **Ad**vanced **E**lectronic **S**ignature (XML formátumú elektronikus aláírás)

14 Felhasznált dokumentumok

14.1 A tanúsításhoz felhasznált kiinduló dokumentumok

- Kérdőív a tanúsítás kérelmezéséhez
- XadesMagic v2.0.0 Biztonsági előirányzat v1.0
- XadesMagic v2.0.0 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:

fejlesztői bizonyíték	Cím	verzió
Megvalósítás		
futtatható saját szoftver elemek	E-Magic: • SDA.E-Magic.exe (v2.0.0.3)	2.0.0.3
	XadesMagic: • SDA.XadesMagic.dll • SDA.Cryptography.dll (v2.0.0.2) • SDA.Cryptography.Framework.dll (v2.0.0.2) • SDA.TimestampProtocol.dll (v2.0.0.2)	2.0.0.2 2.0.0.2 2.0.0.2 2.0.0.2
forráskódok	Lásd konfiguráció lista 3.6 alfejezete	2.0.0.2
harmadik fél által fejlesztett szoftver komponensek	Microsoft .NET Framework	4.0
	NetronGraphLib.dll	2.0.0.2
	BasicShapes.dll	2.0.0.2
	Nini.dll	0.9.0.0
	ICSharpCode.SharpZipLib.dll	0.83.1.0
	SandBar.dll	1.0.13.1
	SandDock.dll	1.0.5.1
	Security.Cryptography.dll	1.6.622.0

Fejlesztői dokumentációk		
Biztonsági előirányzat	XM_biztonsagi_eloiranyzat_v20.doc	2.0
Felhasználói dokumentáció (E-Magic)	EMagicFelhasznaloiDokumentacio_v20.doc	2.0
Fejlesztői dokumentáció (XadesMagic)	Doc-O-Matic_20101119 alkönyvtár	2.0
Biztonsági szerkezet leírás	XM_biztonsagi_szerkezet_v20.doc	2.0
Funkcionális specifikáció	XM_funkcionalis_specifikacio_v20.doc	2.0
TOE terv	XM_TOE_terv_v20.doc	2.0
Konfiguráció lista	XM_konfiguracio_lista_v20.doc	2.0
A konfiguráció kezelés dokumentációja	XM_konfiguracio_kezeles_v20.doc	2.0
A fejlesztés biztonság dokumentációja	XM_fejlesztes_biztonsag_v20.doc	2.0
Az életciklus meghatározás dokumentációja	XM_eletciklus_meghatarozas_v20.doc	2.0
A tesztelésre alkalmas E-Magic + XadesMagic	E-Magic: SDA.E-Magic.exe XadesMagic: 4 dll	2.0.0.3 2.0.0.2
Tesztelési dokumentáció	XM-TestCollection_v20 alkönyvtár	2.0
Teszt lefedettség elemzés	XM_teszt_lefedettseg_v20.doc	2.0
Teszt mélység elemzés	XM_teszt_melyseg_v20.doc	2.0

14.3 Az értékeléshez felhasznált módszertani anyagok

Az értékelés az alábbi dokumentumokban leírt módszertant és eljárásrendet követte:

- Common Criteria for Information Technology Security Evaluation, Part 1: Introduction and general model. Version 3.1, Revision 1, September 2006.
- [Common Criteria for Information Technology Security Evaluation, Part 2: Security functional requirements. Version 3.1, Revision 2, September 2007.
- Common Criteria for Information Technology Security Evaluation, Part 3: Security Assurance Requirements. Version 3.1, Revision 2, September 2007.
- Common Methodology for Information Technology Security Evaluation, Evaluation Methodology. Version 3.1, Revision 2, September 2007.
- KIB (Közigazgatási Informatikai Bizottság) 28. számú ajánlás „Termékekre vonatkozó értékelési módszertan”

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
- Protection Profile - Electronic Signature Creation Application (DCSSI-PP-2008/05)
- Protection Profile - Electronic Signature Verification Module (DCSSI-PP-2008/06)
- ETSI TS 102 176-1 v2.0.0 Electronic Signatures and Infrastructures (ESI) Algorithms and Parameters for Secure Electronic Signatures Part 1: Hash functions and asymmetric algorithms
- Egységes MELASZ formátum elektronikus aláírásokra v2.0 (MMM-001: 2008, v2.0)
- RFC 2560: PKIX - Online Certificate Status Protocol – OCSP
- RFC 3161 PKIX - Time-Stamp Protocol
- RFC 5280 PKIX - Certificate and Certificate Revocation List (CRL) Profile
- SHS Secure Hash Standard /FIPS PUB 180-3/
- PKCS#1 RSA Cryptography Standard v2.1, June 2002