Tanúsítási jelentés

Hung-TJ-017-2004

a
Signed Document eXpert (SDX) Professional 1.0

elektronikus aláíró alkalmazásról

/E-Group Magyarország Rt./

Tartalom

1. Az SDX Professional legfontosabb tulajdonságainak összefoglalása

A tanúsított termék az E_Group magyarország Rt. által fejlesztett és forgalmazott Signed Document eXpert Professional 1.0 elektronikus aláírás alkalmazás (a továbbiakban SDX Professional aláíró alkalmazás vagy SDX Professional).

1.1 Architektúra

Az SDX Professional aláíró alkalmazás elektronikusan aláírt dokumentumok létrehozását és elektronikusan aláírt dokumentumok hitelességének (aláírásának) ellenőrzését támogatja.
Mindezt szabványos formában (XAdES, XML Advanced Electronic Signatures, ETSI TS 101 903) végzi.
Az SDX Professional teljes mértékben a Windows operációs rendszer erőforrásaira, eszközeire támaszkodik. A Crypto API függvényeit használja, amely Windows-os vagy más gyártó CSP-jét használja, ezek pedig magát a biztonságos aláírás-létrehozó eszközt (intelligens kártyát) megszólító, vele kommunikáló driver-eket hívnak meg. Az aláírás létrehozása során a megfelelő XML struktúrák legenerálódnak, majd az aláírandó XML elemre Microsoft Crypto API-n keresztül elkészül a digitális aláírás.

1.2 Tulajdonságok

Az SDX Professional lehetővé teszi, hogy az elektronikus aláírás létrehozásával, ellenőrzésével kapcsolatos feladatok hatékonyan elvégezhetők legyenek az alkalmazási környezetek széles körében. Az elektronikus aláíráshoz kapcsolódó feladatokat képes megoldani állomány szinten, levelező alkalmazásokban, browser-alapú alkalmazásokban, dokumentum kezelő és archiváló rendszerek környezetében, illetve egyedi és tömeges aláírás létrehozás/ellenőrzés esetén is. Az SDX Professional szabványos interfészeken keresztül kapcsolódik a hitelesítés-szolgáltatókhoz (CRL lekérdezés) és szabványos függvényhívásokon keresztül éri el az aláíráshoz kapcsolódó alacsony szintű funkciókat (MS Crypto API).
Az SDX Professional alapvetően két folyamatot kezel:

- Elektronikusan aláírt (hitelesített) dokumentumok létrehozása: Az aláíró a hitelesítés szolgáltatótól kapott tanúsítvány segítségével hitelesíti, aláírja a dokumentumot. Az eredmény egy elektronikusan aláírt dokumentum.
- Elektronikusan aláírt (hitelesített) dokumentumok hiteleségének ellenőrzése: Bármely aláíró által létrehozott, (megfelelő formátumú) hitelesített dokumentumról eldönti, hogy valóban hiteles-e. Az ellenőrzés eredménye egy "hiteles" vagy "nem hiteles" válasz.

Mindkét fenti folyamat alapja az aláírás létrehozására és ellenőrzésére vonatkozó előírásokat definiáló Elektronikus Aláírási Szabályzat (EASZ). Az SDX Professional EASZ független, ami azt jelenti, hogy az aláírásra és annak ellenőrzésére vonatokozó követelmények szabványos módon, formalizált nyelven (XML) leírhatók és az SDX Professional rendszerében szereplő eszközök ezen formális szabályzat alapján hozzák létre, illetve ellenőrzik a hiteles dokumentumokat. A formalizált szabályzatokat elérhetővé kell tenni az aláíró és ellenőrző fél számára, és aláíráskor a használt szabályzat autentikus módon hozzákapcsolódik az aláírt dokumentumhoz. Ennek a megoldásnak a hatására ugyanazokkal az eszközökkel különböző felhasználási célra lehet dokumentumokat hitelesíteni a megfelelő EASZ kiválasztásával.

Az SDX Professional önálló alkalmazás, egyben egy nagyobb termékcsalád (DSA) része. Jelen tanúsítás kizárólag az SDX Professional alkalmazásra vonatkozik.

Az SDX Professional jellemző tulajdonságai:

- XML Advanced Electronic Signatures szabvány szerinti hiteles dokumentum formátum.
- Az alkalmazás és az alkalmazási környezet integritásvédelmének biztosítása digitális aláírással és annak ellenőrzésével.
- Windows (Explorer) integráció.
- Szabványos, X.509 tanúsítványok kezelése.
- Egymásba ágyazott, többszörös elektronikus aláírás kezelésének támogatása.
- Az RFC 3161 szabvány szerinti időbélyeg szolgáltatás támogatása.
- Felhasználó azonosítás támogatása időbélyeg szolgáltatás használatához.
- Tanúsítvány érvényességi állapotának teljes körű ellenőrzése.
- BALE kezelése.
- Szabványos XML elektronikus aláírási szabályzat kezelése.
- Elektronikus Aláírási Szabályzat végrehajtás (dokumentum formátum, tanúsítvány tartalom ellenőrzés, zárt hálózati működés, preferált időbélyeg szerver)

1.3 A tanúsítás tárgya és hatóköre

Jelen tanúsítási jelentés tárgya maga az SDX Professional aláíró alkalmazás.

A tanúsítás során feltételeztük, hogy az SDX Professional aláíró alkalmazás alapját képező Windows operációs rendszer, valamint az ennek részét képező CSP modul biztonságosan és helyesen működnek. Az SDX Professional alapvetően a következő operációs rendszer komponensre épül:

- a Microsoft Crypto API függvényei.

2. Az SDX Professional aláíró alkalmazás megfelelése a funkcionális és biztonsági követelményeknek

Az alábbiakban áttekintjük azokat a (CEN/ISSS CWA 14170 és CEN/ISSS CWA 14171 követelményrendszereiből fakadó) funkcionális és biztonsági követelményeket, melyek minősített aláírások létrehozására és ellenőrzésére szolgáló alkalmazásokra vonatkoznak.
Valamennyi követelménynél rövid magyarázattal kiegészítve megadjuk, hogy az SDX Professional aláíró alkalmazás megfelel-e az adott követelménynek.

Minthogy az SDX Professional aláíró alkalmazást minősített aláírásra kívánják felhasználni, megfelelő tanúsítási végeredmény csak akkor adható, ha az alkalmazás valamennyi rá vonatkozó követelményeknek megfelel.

2.1 A funkcionális követelményeknek való megfelelés

F_SCA_1: Minden aláírás-létrehozó rendszer tartalmazzon egy (teljes) aláírás-ellenőrző rendszert is.
Magyarázat: Az SDX Professional aláíró alkalmazás minden általa aláírt dokumentum esetén automatikus aláírás-ellenőrzést végez.
Konklúzió: **megfelel**

F_SDP_1: Minden aláírói dokumentumnak közvetett módon tartalmaznia kell egy tartalom-formátumot, amely meghatározza azokat a részleteket, ahogyan a dokumentumot az ellenőrző számára meg kell jeleníteni, vagy ahogyan fel kell használni.
Magyarázat: Az SDX Professional az ETSI TS 101 903 szabványnak megfelelően a <SignedDataObjectProperties> struktúrában tárolja és kezeli a dokumentum tartalom formátumát.
Konklúzió: **megfelel**

F_SDP_2: Amennyiben az aláírói dokumentum szemantikája nem függ annak megjelenítésétől, akkor vagy az aláírói dokumentumban vagy egy aláírás tulajdonságban meg kell adni a tartalom egyértelműséghez szükséges információkat.
Magyarázat: Az SDX Professional aláíró alkalmazás az ETSI TS 101 903 szabványnak megfelelően a <SignedDataObjectProperties> struktúrában tárolja és kezeli a dokumentum tartalom formátumát.
Konklúzió: **megfelel**

F_SDP_3: Amennyiben az aláírói dokumentum szemantikája függ annak megjelenítésétől, akkor az aláírónak elegendő információval kell ellátnia az aláírás ellenőrzőjét a dokumentum pontos megjelenítéséhez.
Magyarázat: Az SDX Professional aláíró alkalmazás az ETSI TS 101 903 szabványnak megfelelően a <SignedDataObjectProperties> struktúrában tárolja és kezeli a dokumentum tartalom formátumát.
Konklúzió: **megfelel**

F_SDP_4: Az ellenőrzési folyamatok helyesen értelmezzék a F_SDP_1 által megkövetelt információt, illetve ezek alapján egyértelműen és helyesen jelenítsék azt meg az ellenőrző számára.

Magyarázat: Az SDX Professional aláíró alkalmazás az ETSI TS 101 903 szabványnak megfelelően a <SignedDataObjectProperties> struktúrában tárolja és kezeli a dokumentum tartalom formátumát. A tartalom formátumnak megfelelő megjelenítőt (mint külső alkalmazást) meghívja.

Konklúzió: **megfelel**

F_SAV_1: Mind az aláíró, mind az ellenőrző számára meg kell jeleníteni az aláírási tulajdonságokat, különös tekintettel a következőkre:

- az aláíró tanúsítványa,
- az aláíró dokumentumának tartalom-formátuma (ha szerepel),
- az aláírási szabályzat (ha szerepel),
- a kötelezettségvállalás típusa (ha szerepel).

Magyarázat: Az SDX Professional aláíró alkalmazás valamennyi fenti aláírási tulajdonságot képes megjeleníteni.

Konklúzió: **megfelel**

F_SAV_2: Lehetőséget kell biztosítani az aláíró/ellenőrző számára ahhoz, hogy az aláíráshoz csatolandó/csatolt tanúsítványt átvizsgálja.

Magyarázat: Az SDX Professional aláíró alkalmazás lehetőséget biztosít a csatolandó/csatolt tanúsítvány megjelenítésére.

Konklúzió: **megfelel**

F_SIC_1: Egy aláírás létrehozása előtt meg kell győződni arról, hogy az aláíró valóban létre kíván-e hozni egy minősített elektronikus aláírást.

Magyarázat: Az SDX Professional aláíró alkalmazás az aláírások létrehozását és ellenőrzését csak az aláíró szándékának kifejezett kinyilvánítására valósítja meg.

Konklúzió: **megfelel**

F_SIC_2: Az aláíró/ellenőrző számára vezérlő funkciók szükségesek, melyen keresztül irányíthatja az aláírási/ellenőrzési folyamatot és az aláírás-alkalmazás tevékenységét.

Magyarázat: Az SDX Professional aláíró alkalmazás biztosítja az aláíró/ellenőrző számára szükséges vezérlő funkciókat.

Konklúzió: **megfelel**

F_SIC_3: Egy elektronikus aláírás létrehozása előtt a biztonságos aláírás-létrehozó eszköznek és az aláírás-létrehozó alkalmazásnak is meg kell győződnie arról, hogy az aláíró a biztonságos aláírás-létrehozó eszköz tulajdonosa (vagy jogosult használója).

Magyarázat: Az SDX Professional aláíró alkalmazás csak azt követően hozza létre az elektronikus aláírást, miután az aláírás-létrehozást kiváltani próbáló felhasználó helyesen megadta a BALE PIN kódját.

Konklúzió: **megfelel**

F_DTBSF_1: Ki kell alakítani a szabványos formattált aláírandó adatot az aláíró dokumentumából, az aláírási tulajdonságok felhasználásával.

Magyarázat: Az SDX Professional kialakítja a szabványos formattált aláírandó adatot az aláíró dokumentumából, az aláírási tulajdonságokból.

Konklúzió: **megfelel**

F_DTBSF_2: Ha az aláírandó adatnak tartalmaznia kell az aláírói dokumentum lenyomatát, és ha ez még nem létezik, akkor a DTBSF összetevőnek kezdeményezni kell a lenyomatolási eljárást a formattált aláírandó adat kialakítása előtt.
Magyarázat: Az SDX Professional elvégzi ezt a feladatot.
Konklúzió: **megfelel**

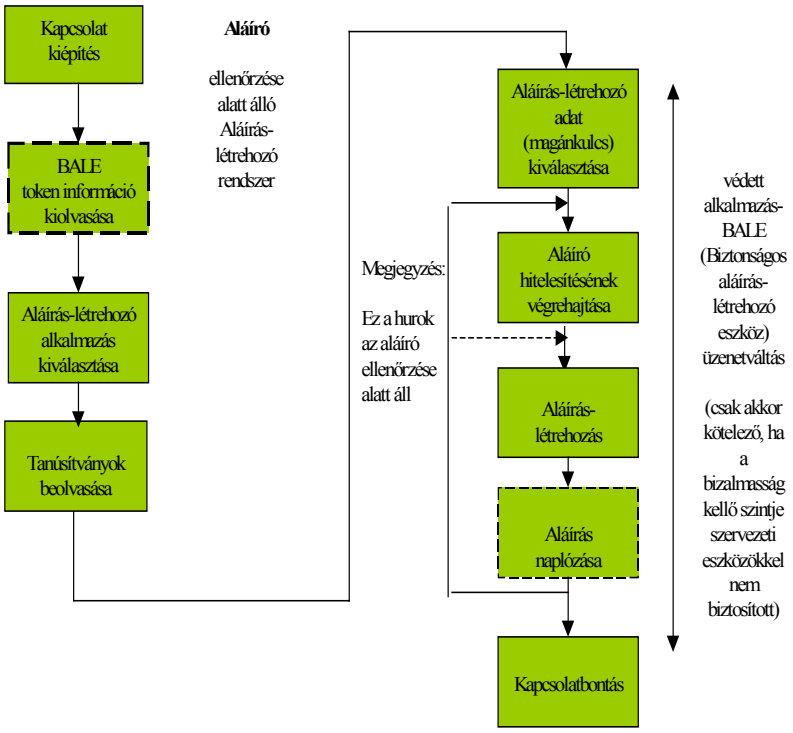
F_DHC_1: Az aláírás-létrehozó folyamat kiváltása utáni első lépésként végre kell hajtani a lenyomatolást.
Magyarázat: Ezt az SDX Professional felhívására a CSP (Cryptographic Service Provider) elvégzi.
Konklúzió: **megfelel**

F_DHC_2: Második lépéseként végre kell hajtani a lenyomat formattálását (feltöltését).
Magyarázat: Ezt az SDX Professional felhívására a CSP elvégzi.
Konklúzió: **megfelel**

F_SSC_1: Egy aláíró ellenőrzése alatti aláírás-létrehozó rendszer és a biztonságos aláírás-létrehozó eszköz között végre kell hajtani a 1. ábrán jelölt minden szükséges kommunikációt.
Magyarázat: Az SDX Professional minden szükséges kommunikációt végrehajt.
Konklúzió: **megfelel**

F_SSC_2: Egy szolgáltató ellenőrzése alatti aláírás-létrehozó rendszer és a biztonságos aláírás-létrehozó eszköz között végre kell hajtani a 2. ábrán[1] jelölt minden szükséges kommunikációt.
Magyarázat: Az SDX Professional aláíró alkalmazást nem külső szolgáltató ellenőrzése alá tervezték.
Konklúzió: **nem vonatkozik rá a követelmény**

[1] Mivel a követelmény nem vonatkozik az értékelés tárgyára, ezért az ábrát mellőzzük



1. ábra: Az aláíró ellenőrzése alatt álló aláírás-létrehozó rendszer esetén megvalósítandó együttműködési sorozat az aláírás-létrehozó rendszer és a biztonságos aláírás-létrehozó eszköz között

F_SSC_3: Az aláírás-létrehozó alkalmazásnak legalább egy fizikai interfésszel kell rendelkeznie, amely alkalmas a biztonságos aláírás-létrehozó eszközzel való kommunikációra.

Magyarázat: Az SDX Professional aláíró alkalmazás fizikai interfészen keresztül kommunikál az aláírást végző intelligens kártyával.

Konklúzió: **megfelel**

F_SSC_4: A biztonságos aláírás-létrehozó eszköz funkcionalitása megvalósítható egy olyan platformon (pl. intelligens kártya), amely egy vagy több biztonságos aláírás-létrehozó eszköz funkciót hordoz és, ezen felül esetleg más alkalmazásokat is. Ilyen több-alkalmazásos platform esetén az aláírás-létrehozó alkalmazásnak ki kell választania az egyiket.

Magyarázat: Az SDX Professional elvileg támogat több-alkalmazásos platformot is, de ilyenkor az aktivizálandó magánkulcshoz tartozó tanúsítványt be kell hozzá előzetesen állítani.

Konklúzió: **megfelel**

F_SSC_5: Egy biztonságos aláírás-létrehozó eszköz hordozhat több tanúsítványt is. Ebben az esetben ki kell tudni választani az egyiket.
Magyarázat: Az SDX Professional támogatja a több tanúsítványból történő választást.
Konklúzió: **megfelel**

F_SSC_6: Ha egy biztonságos aláírás-létrehozó eszköz egynél több aláírás-létrehozó adatot (magánkulcsot) tartalmaz, akkor a megfelelőt ki kell tudni választani az aláíró szándéka szerint.
Magyarázat: Az SDX Professional támogatja a több magánkulcsból történő választást.
Konklúzió: **megfelel**

F_SSC_7: A biztonságos aláírás-létrehozó eszköz és az aláírás-létrehozó alkalmazás közötti kommunikátor (SSC) összetevőnek át kell vennie az aláírót hitelesítő adatot az aláírót hitelesítő összetevőtől egy megbízható útvonalon keresztül, és el kell küldenie egy megfelelő parancs (utasítás) kíséretében a biztonságos aláírás-létrehozó eszköznek összehasonlításra.
Magyarázat: BALE alkalmazása esetén az SDX Professional (pontosabban az általa meghívott CSP) támogatja a PIN kód védett továbbítását.
Konklúzió: **megfelel**

F_SSC_8: Az aláírás létrehozó folyamat utolsó lépéseként ki kell számíttatni (a biztonságos aláírás-létrehozó eszköz által megvalósítva) magát az aláírást.
Magyarázat: Ezt a feladatot az SDX Professional (az alapját képező CSP-vel és BALE-vel) megoldja.
Konklúzió: **megfelel**

F_SSC_9: A befejezett aláírásokat naplózni kell.
Magyarázat: A rendszer mind a sikeres, mind a sikertelen aláírásokat naplózza.
Konklúzió: **megfelel**

F_SSA_1 Ha az aláírás-létrehozás egy - szolgáltató ellenőrzése alatt álló – aláírás-létrehozó rendszeren történik meg, akkor az aláírónak képesnek kell lennie annak megállapítására, hogy feltételezhet-e ugyanolyan szintű bizalmasságot, mint amit a saját ellenőrzése alatt álló aláírás-létrehozó rendszer esetén elérhet.
Magyarázat: Az SDX Professional aláíró alkalmazás nem áll egy külső szolgáltató ellenőrzése alatt.
Konklúzió: **nem vonatkozik rá a követelmény**

F_SDC_1: Lehetővé kell tenni az aláíró számára az aláírói dokumentum létrehozását vagy kiválasztását.
Magyarázat: Az SDX Professional lehetővé teszi az aláírói dokumentum létrehozását és kiválasztását is.
Konklúzió: **megfelel**

F_SDOC_1: Össze kell kapcsolni a biztonságos aláírás-létrehozó eszköz kimeneti adatát (az elektronikus aláírást) a formattált aláírt adattal, a szabvány formátumnak megfelelően.
Magyarázat: Az SDX Professional aláíró alkalmazás a szabványos XadES XML formátumot támogatja.
Konklúzió: **megfelel**

F_SLC_1: Minden létrehozott/ellenőrzött aláírásra egy napló bejegyzés tárolandó.
Magyarázat: A rendszer mind a sikeres, mind a sikertelen aláírásokat naplózza.
Konklúzió: **megfelel**

F_SCPC_1: A hitelesítés-szolgáltatóval való kapcsolat felvételén keresztül képesnek kell lennie az alábbiakra:

- az aláírói tanúsítványok megszerzése,
- az aláírói tanúsítványok állapotának lekérése.

Magyarázat: Az SDX Professional aláíró alkalmazás támogatja mind az aláíró tanúsítványának, mind a tanúsítvány visszavonási listának a megszerzését. (Az OCSP-t az SDX Professional aláíró alkalmazás nem támogatja.)
Konklúzió: **megfelel**

F_I/O_1: Ha aláírás-létrehozásnál a biztonságos aláírás-létrehozó eszköz nem tartalmaz minden szükséges tanúsítványt az aláírási folyamathoz (mert csak a tanúsítvány azonosítókat tartalmazza), vagy ha aláírás-ellenőrzésnél az aláírótól nem érkezett meg a szükséges tanúsítvány (csak annak azonosítója), akkor az aláírás-alkalmazásnak képesnek kell lennie arra, hogy ezeket a tanúsítványokat megszerezze (lekérdezze a hitelesítés-szolgáltatótól).
Magyarázat: Az SDX Professional aláíró alkalmazás támogatja ilyen esetekben is a tanúsítvány megszerzését.
Konklúzió: **megfelel**

F_I/O-2: Az aláírás-alkalmazásnak képesnek kell lennie arra, hogy a megszerzett tanúsítványok hitelességét ellenőrizze.
Magyarázat: A tanúsítványok hitelességét a hitelesítés-szolgáltató garantálja, a rendszer pedig mindig ellenőrzi.
Konklúzió: **megfelel**

F_I/O_3: Ha az aláírói dokumentumot, vagy annak egy részét, vagy az aláírási tulajdonságokat egy input/output interfészen keresztül adják meg, az aláírás-létrehozó alkalmazásnak biztosítania kell, hogy egyetlen rejtett rész se játszhasson szerepet, és hogy egyetlen aláírandó adat összetevőt se cserélhessenek ki.
Magyarázat Az SDX Professional aláíró alkalmazás biztosítja a fenti elvárást.
Konklúzió: **megfelel**

F_ISV_1: Az érvényesítő adatokat az ellenőrzőnek be kell gyűjtenie, és az aláírási szabályzat minden követelményét teljesítenie kell.
Magyarázat Az SDX Professional aláíró alkalmazás biztosítja a fenti elvárást.
Konklúzió: **megfelel**

F_ISV_2: Ha szükség lehet utólagos ellenőrzésre, az érvényesítő adatoknak tartalmazniuk kell annak bizonyítékát, hogy a felhasznált tanúsítvány lánc érvényes volt az aláírás létrehozásának időpontjában.
Magyarázat: Az XadES formátum megfelelő aláírási szabályzat esetén támogatja az utólagos ellenőrizhetőséget.
Konklúzió: **megfelel**

F_USV_1: A kezdeti ellenőrzés során begyűjtött érvényesítő adatok ellenőrzésénél az aláírási szabályzat minden követelményét teljesíteni kell.
Magyarázat: Az SDX Professional képes az aláírási szabályzat végrehajtására .
Konklúzió: **megfelel**

Ember által történő ellenőrzés esetén:

F_human_1: Az aláírás-ellenőrző rendszernek eszközt kell biztosítania a felhasználó számára, amelyen keresztül az kommunikálni tud a rendszerrel. Ha az aláírt adatokhoz egynél több aláírás van hozzárendelve, akkor ennek a kommunikációnak azzal kell kezdődnie, hogy kijelzésre kerül az aláírások száma, amelyek feltehetően léteznek, és fel kell kínálni, hogy melyik legyen az ellenőrizendő.
Magyarázat: Az SDX Professional aláíró alkalmazás támogatja a fenti elvárást.
Konklúzió: **megfelel**

F_human_2: Az aláírás-ellenőrző rendszernek interaktív eszközt kell biztosítania a felhasználó számára, hogy megnézhesse az aláírási szabályzat teljes egészét, vagy legalább az alkalmazási területre és feltételekre vonatkozó részeket.
Magyarázat: Az SDX Professional aláíró alkalmazás támogatja a fenti elvárást.
Konklúzió: **megfelel**

F_human_3: A felhasználói felületnek megfelelő módon meg kell jelenítenie az aláíró dokumentumot, hogy az aláírást ellenőrző személy képes legyen az aláírói dokumentum tartalmának kellő meghatározására. Teljesíteni kell az “Ami megjelenik, azt írták alá.” követelményt. Ha valamilyen okból az aláírói dokumentum nem jeleníthető meg pontosan a megfelelő módon, akkor ezt a felhasználói interfésznek világosan jeleznie kell.
Magyarázat: Az SDX Professional aláíró alkalmazás támogatja a fenti elvárást.
Konklúzió: **megfelel**

F_human_4: Az aláíró azonosítójának, vagyis az állítólagos aláíró nevének vagy felvett nevének megjeleníthetőnek kell lenni. Az adott nevet az aláíró tanúsítványában szereplő, “megkülönböztető név” információjából kell venni. Ha az aláíró nem bocsátotta rendelkezésre a tanúsítványt, a hitelesítés-szolgáltató nevét kell megjeleníteni ehelyett, és ha ez a név elfogadható, akkor az adott tanúsítványt a hálózati interfész felhasználásával be kell szerezni. Az említett névnek csak a tanúsítványt kibocsátó hitelesítés-szolgáltató számára van jelentése, ezért a hitelesítés-szolgáltató nevét az aláíró nevével együtt ki kell jelezni.
A kezdeti aláírás-ellenőrzési folyamat kimenő állapota az alábbiak egyike legyen:

- „érvényes” állapot (sikeres ellenőrzés),
- „érvénytelen” állapot (sikertelen ellenőrzés),
- „befejezetlen ellenőrzés” állapot (befejezetlen ellenőrzés)

Magyarázat: Az SDX Professional aláíró alkalmazás kezdeti aláírás-ellenőrzési folyamatának kimenő állapota vagy "érvényes” (sikeres ellenőrzés), vagy "érvénytelen” (sikertelen ellenőrzés).
Konklúzió: **megfelel**

F_human_5: „Befejezetlen ellenőrzés” állapot esetén az aláírás-ellenőrző alkalmazásnak javasolnia kell a felhasználó számára, hogy szerezze be azt az információt, ami az aláírást érvényessé teszi hosszú távra.
Magyarázat: Az SDX Professional aláíró alkalmazás kezdeti aláírás-ellenőrzési folyamatának kimenő állapota vagy "érvényes” (sikeres ellenőrzés), vagy "érvénytelen” (sikertelen ellenőrzés), tehát sosem befejezetlen ellenőrzés".
Konklúzió: **nem vonatkozik rá a követelmény**

F_human_6: A felhasználói interfészekre teljesüljenek az F_principles egyszerűségre és hibamentességre vonatkozó speciális elvárásai.
Magyarázat: Az SDX Professional aláíró alkalmazás teljesíti a fenti elvárást.
Konklúzió: **megfelel**

Gépi (automatikus) ellenőrzés esetén:

F_machine_1: Az 1-es típusú API-k alkalmasnak kell lenniük az elektronikus aláírásban tárolt információk kinyerésére és az elektronikus aláírás formátumának meghatározására.
Magyarázat: Az SDX Professionalt nem automatikus ellenőrzésre tervezték.
Konklúzió: **nem vonatkozik rá a követelmény**

F_machine_2: A 2-es típusú API-k az elektronikus aláírások hitelesítését és/vagy ellenőrzését kell lehetővé tenniük, illetve be kell szerezniük az aláírói információkat, az output állapotot és az érvényesítő adatokat.

- Az automatizált feldolgozás esetében alkalmazói program interfészek (API-k) használhatók. Bár az ilyen interfészek kialakításának többféle módja van, ezeket két csoportba lehet sorolni:
- az 1-es típusú API-k arra szolgálnak, hogy az elektronikus aláírásban tárolt adatokat kigyűjtsék.
- A 2-es típusú API-k az elektronikus aláírás ellenőrzésére és az érvényesítő adatok beszerzésére szolgálnak.

Magyarázat: Az SDX Professionalt nem automatikus ellenőrzésre tervezték.
Konklúzió: **nem vonatkozik rá a követelmény**

F_general_1: A rendszer által megvalósított aláírás-ellenőrzési folyamatnak meg kell felelnie egy ember számára olvasható formájú leírásnak, feltételezve, hogy az aláírási szabályzat minden feldolgozási szabálya világosan meghatározott.
Magyarázat: Az SDX Professional teljesíti a fenti elvárást.
Konklúzió: **megfelel**

F_protocol: Mind az aláírás-létrehozó, mind az aláírás-ellenőrzési alkalmazásnak szabványos protokollt kell használnia a megbízható szolgáltatóval (szolgáltatókkal) történő kommunikáció során.

- tanúsítvány visszavonási állapot megszerzésekor;
- időbélyeg kérelem és válasz esetén;
- egyéb esetekben (pl. központi archiválási, időjelzési, naplózási szolgáltatások igénybe vétele esetén).

Magyarázat: Az SDX Professional teljesíti a fenti elvárást.
Konklúzió: **megfelel**

F_format: Mind az aláírás-létrehozó, mind az aláírás-ellenőrzési alkalmazásnak képesnek kell lennie szabványos formátumok kezelésére az alábbi területeken:

- szabványos aláírási formátumok;
- szabványos tanúsítvány formátumok.

Magyarázat: Az SDX Professional teljesíti a fenti elvárást.
Konklúzió: **megfelel**

F_principles: A felhasználói (aláírói, aláírás-ellenőrzői) felületek tervezésekor a következő elveket kell figyelembe venni:

- alkalmasnak kell lennie a feladatra;
- konzisztensnek kell lennie;
- felhasználóbarátnak (könnyen érthető, egyszerűen használható) kell lennie;
- ellenőrizhetőnek kell lennie;
- hibatűrőnek kell lennie;
- lehetővé kell tennie az egyedi beállításokat;
- egyenlőségen alapuló hozzáférést kell biztosítania;
- megfelelő állapotjelzéseket és hibaüzeneteket küldjön a felhasználónak

Az aláírókkal és ellenőrzőkkel párbeszédet folytató rendszer teljesítse az alábbiakat:

- félreérthetetlen felhasználói útmutatót kell szolgáltatnia arra nézve, hogy hogyan kell a rendszert installálni, konfigurálni és használni;
- ön-leírónak kell lennie abban az értelemben, hogy minden párbeszéd-lépésnek azonnal érthetőnek kell lennie vagy a rendszertől kapott visszajelzéseken keresztül, vagy úgy, hogy az ellenőrző kérésére a rendszer magyarázatot ad;
- meg kell felelnie a felhasználók szokásos elvárásainak, azaz tudásuknak, képzettségüknek, tapasztalatuknak és az általánosan elfogadott konvencióknak;
- adaptálhatónak kell lennie, azaz támogatnia kell a felhasználók egyéni igényeit és preferenciáit;
- hibatűrőnek kell lennie úgy, hogy a nyilvánvaló input hibák ellenére az eredményt el lehessen érni minimális javításokkal.
- tájékoztató hiba üzeneteket kell küldenie, a felhasználó továbbhaladása érdekében;
- visszajelzéseket kell szolgáltatnia, mely megerősíti a felhasználó által végrehajtott tevékenység helyességét (vagy helytelenségét);
- a hibaüzenetek legyenek kellően informatívak, adjanak eligazítást a hiba okáról, a szükséges teendőkről (pl. a “Hibakód: 213” hibaüzenet nem igazán segítőkész);
- szabatos és minden részletre kiterjedő terminológia helyett hétköznapi kifejezéseket kell használni (a technikai kifejezéseket ugyanis a legtöbb felhasználó nem érti, és nem is kell értenie);
- alkalmaznia kell a színek használatára vonatkozó konvenciókat (pl. piros = hiba, zöld = továbbhaladás/siker);
- minden időpontban képesnek kell lennie arra, hogy az éppen végrehajtás alatt álló műveletet félbeszakítsa és vagy visszatérjen a főmenübe, vagy teljesen kilépjen a rendszerből;
- a felhasználói egyének számára biztosítania kell a magántitok jelleget (pl. azáltal, hogy az információkat nem teszi mások számára hozzáférhetővé a felhasználói interfészen keresztül).

A műveletek helyes időzítésével elegendő időt kell biztosítani minden felhasználónak a folyamatok befejezéséhez (figyelembe véve azt a tényt is, hogy az emberek olvasási és reagálási képességei különbözők).

Magyarázat: Az SDX Professional aláíró alkalmazás megfelel a fenti elvárásoknak.

Konklúzió*:* **megfelel**

2.2 A biztonsági követelményeknek való megfelelés

A biztonsági követelményeknek való megfelelés értékelésénél felhasználtuk a fejlesztők által készített, s az "SDX Professional 1.0 - Funkcionális specifikáció" című dokumentációban szereplő indoklásokat. Azokban az esetekben, ahol a fejlesztői indoklást teljes egészében elfogadhatónak ítéltük, a "Magyarázat" rovatba a következő szöveget írjuk: "A megfelelésre vonatkozó fejlesztői indoklás elfogadva."

2.2.1 Követelmények az aláírás-létrehozó alkalmazás (SCA) egészére

Az aláírás-létrehozó alkalmazás és a biztonságos aláírás-létrehozó eszköz közötti megbízható útvonalra vonatkozó követelmények:

Bizt_köv1: Az aláírás-létrehozó alkalmazásnak meg kell őriznie a következők sértetlenségét:

- aláírandó adat (DTBS), formattált aláírandó adat (DTBSF), aláírandó adat reprezentáns (DTBSR) és minden egyéb, az aláíró által szolgáltatott információ,
- Az aláírás-létrehozó alkalmazás és a biztonságos aláírás-létrehozó eszköz között áramló valamennyi protokoll adat.

Magyarázat: "A megfelelésre vonatkozó fejlesztői indoklás elfogadva."
Konklúzió*:* **megfelel**

Bizt_köv2: Az aláírás-létrehozó alkalmazásnak meg kell őriznie az aláírandó adat komponensek, a formattált aláírandó adat és az aláírót hitelesítő adatok bizalmasságát.
Magyarázat: "A megfelelésre vonatkozó fejlesztői indoklás elfogadva."
Konklúzió: **megfelel**

Bizt_köv3: … Bizt_köv6:
Magyarázat: A 3.-6. követelmények csak a nyilvános aláíró alkalmazásokra vonatkoznak (melyek egy szolgáltató ellenőrzése alatt állnak). Az SDX Professional aláíró alkalmazás nem ilyen.
Konklúzió: **nem vonatkoznak rá a követelmények**

Bizt_köv7: Az aláírás-létrehozó alkalmazásnak biztosítania kell, hogy az aláírónak bemutatott aláírandó adat ugyanaz, mint amit az aláíró kiválasztott.
Magyarázat: "A megfelelésre vonatkozó fejlesztői indoklás elfogadva."
Konklúzió: **megfelel**

Bizt_köv8: Az aláírás-létrehozó alkalmazásnak biztosítania kell, hogy a formattált aláírandó adat és aláírandó adat reprezentáns előállításához felhasznált aláírandó adat komponensek ugyanazok, mint amelyeket az aláírónak bemutattak a bemutatási eljárás során, és amelyeket a felhasználó kiválasztott.
Magyarázat: "A megfelelésre vonatkozó fejlesztői indoklás elfogadva."
Konklúzió: **megfelel**

Osztott architektúrájú aláírás-létrehozó alkalmazásokra vonatkozó követelmények

Bizt_köv9: … Bizt_köv10:
Magyarázat: Az SDX Professional aláíró alkalmazás nem osztott architektúrájú alkalmazás.
Konklúzió: **nem vonatkoznak rájuk a követelmények**

A nem megbízható folyamatokból és kommunikációs portokból adódó követelmény

Bizt_köv11: Meg kell gátolni, hogy az aláírási folyamatba beavatkozhassanak olyan nem megbízható rendszer és alkalmazási folyamatok, perifériák és kommunikációs csatornák, amelyek nem szükségesek az aláírás-létrehozás alkalmazás működéséhez.
Magyarázat: "A megfelelésre vonatkozó fejlesztői indoklás elfogadva."
Konklúzió: **megfelel**

Az aláírandó adatra vonatkozó követelmények

Bizt_köv12: Az aláírandó adatnak tartalmaznia kell egy aláírói dokumentumot. (Egy "üres" dokumentumhoz ne lehessen aláírást előállítani).
Magyarázat: "A megfelelésre vonatkozó fejlesztői indoklás elfogadva."
Konklúzió: **megfelel**

Bizt_köv13: Az aláírandó adatnak tartalmaznia kell az aláírónak azt a tanúsítvány-azonosítóját, amely az elektronikus aláírás létrehozásánál a biztonságos aláírás-létrehozó eszköz által felhasznált aláírás-létrehozó adathoz kapcsolódik, s amely az aláíró szándékának megfelel.
Magyarázat: "A megfelelésre vonatkozó fejlesztői indoklás elfogadva."
Konklúzió: **megfelel**

Bizt_köv14: Az aláírandó adatnak tartalmaznia kell egy hivatkozást az aláírási szabályzatra.
Magyarázat: "A megfelelésre vonatkozó fejlesztői indoklás elfogadva."
Konklúzió: **megfelel**

Bizt_köv15: Az aláírandó adatnak tartalmaznia kell a kötelezettségvállalás típus tulajdonságot, ha az aláírási szabályzat egynél több kötelezettségvállalás típust határoz meg.
Magyarázat: "A megfelelésre vonatkozó fejlesztői indoklás elfogadva."
Konklúzió: **megfelel**

Bizt_köv16: Ha az alkalmazás vagy az érvényben lévő biztonsági szabályzat egynél több aláírói dokumentum tartalom formátumot enged meg, az aláírandó adatnak tartalmaznia kell az aláírói dokumentum tartalom formátumot.
Magyarázat: "A megfelelésre vonatkozó fejlesztői indoklás elfogadva."
Konklúzió: **megfelel**

2.2.2. Követelmények az aláíró dokumentumát megjelenítő összetevőre (SDP)

Bizt_köv17: Az aláíró dokumentumát megjelenítő összetevőnek lehetővé kell tennie az aláírói dokumentum tartalom-formátumának csatolását vagy közvetett módon az aláírási szabályzat részeként, vagy pedig egy közvetlen aláírás tulajdonságként.
Magyarázat: "A megfelelésre vonatkozó fejlesztői indoklás elfogadva."
Konklúzió: **megfelel**

Bizt_köv18: Az aláíró dokumentumát megjelenítő összetevőnek figyelmeztetnie kell az aláírót, ha a dokumentum nem felel meg a tartalom formátummal meghatározott szintaxisnak, és lehetővé kell tennie az aláíró számára, hogy félbeszakítsa az aláírási folyamatot.
Magyarázat: "A megfelelésre vonatkozó fejlesztői indoklás elfogadva."
Konklúzió: **megfelel**

Bizt_köv19: A használati útmutatóban jelezni kell, hogy milyen tartalom formátum helyes kezelésére alkalmas az aláíró dokumentumát megjelenítő összetevő.
Magyarázat: "A megfelelésre vonatkozó fejlesztői indoklás elfogadva."
Konklúzió: **megfelel**

Bizt_köv20: A használati útmutatóban jelezni kell, hogy milyen lehetséges következménnyel jár, ha az aláíró tévesen választja ki a tartalom formátumot.
Magyarázat: "A megfelelésre vonatkozó fejlesztői indoklás elfogadva."
Konklúzió: **megfelel**

Bizt_köv21: Az aláíró dokumentumát megjelenítő összetevőnek figyelmeztetnie kell az aláírót, ha olyan aláírói dokumentumot kíván aláírni, amelynek tartalom formátumát nem támogatja.
Magyarázat: "A megfelelésre vonatkozó fejlesztői indoklás elfogadva."
Magyarázat kiegészítés: Az SDX nem csak figyelmeztet, hanem megtagadja az aláírás elkészítését, vagyis egy szigorúbb követelménynek tesz eleget.
Konklúzió: **megfelel**

Bizt_köv22: Az aláíró dokumentumát megjelenítő összetevőnek biztosítania kell, hogy az aláírónak megmutatott aláírói dokumentum ugyanaz, mint amit az aláírási folyamat fog használni, és ugyanaz, mint amit az aláíró választott ki aláírásra.
Magyarázat: "A megfelelésre vonatkozó fejlesztői indoklás elfogadva."
Konklúzió: **megfelel**

Bizt_köv23: A megjelenítő folyamatnak tájékoztatnia kell az aláírót, hogy egyéb aláírt adatok vannak beágyazva az aláírói dokumentumba (az aláíró dokumentumát megjelenítő összetevőnek kapcsolódnia kell egy aláírás ellenőrző rendszerrel az ilyen aláírások ellenőrzésére).
Magyarázat: "A megfelelésre vonatkozó fejlesztői indoklás elfogadva."
Konklúzió: **megfelel**

Bizt_köv24: Az aláíró dokumentumát megjelenítő összetevőnek nem szabad lehetővé tennie az aláíró számára, hogy az aláírói dokumentum bármely részét megváltoztassa.
Magyarázat: "A megfelelésre vonatkozó fejlesztői indoklás elfogadva."
Konklúzió: **megfelel**

Bizt_köv25: Az aláíró dokumentumát megjelenítő összetevőnek figyelmeztetnie kell az aláírót, ha nem képes az aláírói dokumentum minden részének a helyes, tartalom formátumnak megfelelő megjelenítésére.
Magyarázat: "A megfelelésre vonatkozó fejlesztői indoklás elfogadva."
Konklúzió: **megfelel**

Az aláíró dokumentumára vonatkozó egyértelműségi követelmény:

Bizt_köv26: Az aláírás-létrehozó alkalmazásnak lehetővé kell tennie egy tartalom formátum tulajdonság csatolását az aláírandó adatokhoz annak biztosítására, hogy az aláíró dokumentumának megjelenítése egyértelmű legyen. Vagyis pontosan úgy lehessen azt a későbbiekben megjeleníteni, mint ahogyan az aláírónak a megjelenítési folyamat során.
Magyarázat: "A megfelelésre vonatkozó fejlesztői indoklás elfogadva."
Konklúzió: **megfelel**

A nem megjelenítés-érzékeny aláírói dokumentumokra vonatkozó követelmény:

Bizt_köv27: Az aláírás-létrehozó alkalmazásnak lehetővé kell tennie egy tartalom formátum tulajdonság csatolását az aláírandó adatokhoz annak biztosítására, hogy az aláíró dokumentum szemantikáját csak egyféleképpen lehessen értelmezni.
Magyarázat: "A megfelelésre vonatkozó fejlesztői indoklás elfogadva."
Konklúzió: **megfelel**

A rejtett szövegre és aktív kódra vonatkozó követelmény:

Bizt_köv28: Az aláírás-létrehozó alkalmazásnak figyelmeztetnie kell az aláírót a rejtett szövegek, makrók vagy aktív kódok jelenlétére. Amennyiben az aláírási szabályzat nem engedélyezi az ilyen aláírói dokumentumok aláírását, akkor az aláírás-létrehozó alkalmazásnak érvényre kell juttatnia ezt a tiltást.
Magyarázat: "A megfelelésre vonatkozó fejlesztői indoklás elfogadva."
Konklúzió: **megfelel**

2.2.3. Követelmények az aláírás tulajdonságokat megjelenítő összetevőre (SAV)

Bizt_köv29: Az aláírás tulajdonság megjelenítési folyamatának lehetővé kell tennie az aláíró számára az aláírás tulajdonságok megtekintését.
Magyarázat: "A megfelelésre vonatkozó fejlesztői indoklás elfogadva."
Konklúzió: **megfelel**

Bizt_köv30: Az aláírás tulajdonságokat megjelenítő folyamatnak biztosítania kell, hogy az aláírónak megjelenített aláírás tulajdonság ugyanaz, mint ami az aláírás folyamatában aláírásra kerül majd, és amit az aláíró kiválasztott az aláíráshoz.
Magyarázat: "A megfelelésre vonatkozó fejlesztői indoklás elfogadva."
Konklúzió: **megfelel**

Bizt_köv31: Az aláírás tulajdonságok sértetlenségét és hitelességét meg kell védeni.
Magyarázat: "A megfelelésre vonatkozó fejlesztői indoklás elfogadva."
Konklúzió: **megfelel**

Bizt_köv32: Az aláírót figyelmeztetni kell az aláírás tulajdonságokban jelenlévő bármilyen rejtett szövegről, makróról vagy aktív kódról. Amennyiben az aláírási szabályzat nem engedélyezi az ilyen aláírói dokumentumok aláírását, akkor az aláírás-létrehozó alkalmazásnak érvényre kell juttatnia ezt a tiltást.
Magyarázat: "A megfelelésre vonatkozó fejlesztői indoklás elfogadva."
Konklúzió: **megfelel**

Bizt_köv33: Az aláírás tulajdonság megjelenítő folyamatnak figyelmeztetnie kell az aláírót bármely, az aláírás tulajdonságokba beágyazott rejtett vagy aktív komponens (pl. word processzor makró) jelenlétére. Amennyiben az aláírási szabályzat nem engedélyezi az ilyen aláírói dokumentumok aláírását, akkor az aláírás-létrehozó alkalmazásnak érvényre kell juttatnia ezt a tiltást.
Magyarázat: "A megfelelésre vonatkozó fejlesztői indoklás elfogadva."
Konklúzió: **megfelel**

Bizt_köv34: Az aláírás tulajdonság megjelenítő összetevőnek lehetővé kell tennie az aláíró számára, hogy átvizsgálja a kiválasztott, aláírandó adatokhoz csatolandó tanúsítvány fő összetevőit.
Magyarázat: "A megfelelésre vonatkozó fejlesztői indoklás elfogadva."
Konklúzió: **megfelel**

2.2.4. Követelmények az aláíróval kölcsönható összetevőre (SIC)

Az aláírás kiváltására vonatkozó követelmények

Bizt_köv35: Az aláírási folyamat megkezdése előtt az aláíróval kölcsönható összetevőnek egy olyan nem nyilvánvaló, az aláírás-létrehozó alkalmazással folytatott, aláírás kiváltási cselekvést kell elvárnia az aláírótól, amely véletlenül valószínűleg nem következne be.
Magyarázat: "A megfelelésre vonatkozó fejlesztői indoklás elfogadva."
Konklúzió: **megfelel**

Az inaktivitási időkorlátra vonatkozó biztonsági követelmények

Bizt_köv36: Az aláírás-létrehozó alkalmazásnak egy korlátot kell megadnia arra az időtartamra, ami az aláírót hitelesítő adatok megadásától az aláírás kiváltásáig eltelhet.
Magyarázat: A követelményt nem az SDX Professional aláíró alkalmazásnak, hanem a CSP összetevőnek kell teljesítenie.
Konklúzió: ***nem vonatkozik rá a követelmény***

Bizt_köv37: Ha az időkorlát letelik, az egész aláírási folyamatot félbe kell szakítani, az aláírótól az aláírási folyamat újraindítását követelve meg, hitelesítő adatainak újra megadását is beleértve. Az újraindítás szükségességéről tájékoztatni kell az aláírót.
Magyarázat: A követelményt nem az SDX Professional aláíró alkalmazásnak, hanem a CSP összetevőnek kell teljesítenie.
Konklúzió: ***nem vonatkozik rá a követelmény***

2.2.5. Követelmények az aláírót hitelesítő összetevőre (SAC)

A tudáson alapuló aláírót hitelesítő adatokra vonatkozó követelmények

Bizt_köv38: Az aláírás-létrehozó alkalmazásnak eszközt kell biztosítania a felhasználó számára ahhoz, hogy az megadhassa az aláírót hitelesítő adatot ezen keresztül a biztonságos aláírás-létrehozó eszköz számára.
Magyarázat: A követelményt nem az SDX Professional aláíró alkalmazásnak, hanem a CSP összetevőnek kell teljesítenie.
Konklúzió: ***nem vonatkozik rá a követelmény***

Bizt_köv39: Az aláírás-létrehozó alkalmazásnak meg kell őriznie az aláírót hitelesítő adatok bizalmasságát, és biztonságosan törölnie kell azokat, amint azokra nincs már szükség.
Magyarázat: A követelményt nem az SDX Professional aláíró alkalmazásnak, hanem a CSP összetevőnek kell teljesítenie.
Konklúzió: ***nem vonatkozik rá a követelmény***

Bizt_köv40: Ha az aláírni szándékozó egy korlátot meghaladó számban helytelen hitelesítő adatot ad meg, akkor az újrapróbálkozást le kell tiltani, egyúttal hibajelzést kell adni az aláíró részére, ha az aláíró hitelesítési módszert már nem blokkolta korábban a biztonságos aláírás-létrehozó eszköz. Az aláírni szándékozó részére egy megfelelő üzenetet kell küldeni.
Magyarázat: A követelményt nem az SDX Professional aláíró alkalmazásnak, hanem a CSP összetevőnek kell teljesítenie.
Konklúzió: ***nem vonatkozik rá a követelmény***

Bizt_köv41: Ha az aláírni szándékozó ismételten helytelen hitelesítő adatot ad meg (pl. három egymást követő alkalommal), a biztonságos aláírás-létrehozó eszköznek félbe kell szakítania az aláíró hitelesítését, és erről informálnia kell az aláírás-létrehozó alkalmazást, amelynek az aláíró részére egy megfelelő üzenetet kell küldeni.
Magyarázat: A követelményt nem az SDX Professional aláíró alkalmazásnak, hanem a CSP összetevőnek kell teljesítenie.
Konklúzió: ***nem vonatkozik rá a követelmény***

Bizt_köv42: Egy megbízható útvonalat kell biztosítani a PIN/jelszó továbbítására a PIN pad (vagy billentyűzet) és a biztonságos aláírás-létrehozó eszköz között az aláírás-létrehozó alkalmazáson keresztül.
Magyarázat: A követelményt nem az SDX Professional aláíró alkalmazásnak, hanem a CSP összetevőnek kell teljesítenie.
Konklúzió: ***nem vonatkozik rá a követelmény***

Bizt_köv43: Biztosítani kell egy olyan funkciót, amellyel a tudáson alapuló hitelesítő adatok lecserélhetőek (hacsak ez nincs tiltva egy aláírás-létrehozó alkalmazás típus esetében az alkalmazás szolgáltatójának biztonsági szabályzatában).
Magyarázat: A követelményt nem az SDX Professional aláíró alkalmazásnak, hanem a CSP összetevőnek kell teljesítenie.
Konklúzió: ***nem vonatkozik rá a követelmény***

Bizt_köv44: A megadott PIN kódot (vagy jelszót) nem szabad kijelezni, bár egy számjegy vagy karakter begépelését vissza kell jelezni egy megfelelő jellel (pl. egy csillag karakterrel), amely nem fedi fel magát a PIN-t (vagy a jelszót).
Magyarázat: A követelményt nem az SDX Professional aláíró alkalmazásnak, hanem a CSP összetevőnek kell teljesítenie.
Konklúzió: ***nem vonatkozik rá a követelmény***

Bizt_köv45: Az aláírás-létrehozó alkalmazásnak meg kell követelnie az új PIN kód (jelszó) kétszeri megadását, és ellenőriznie kell ezek azonosságát, mielőtt az új PIN kódot (jelszót) továbbítaná a biztonságos aláírás-létrehozó eszköznek.
Magyarázat: A követelményt nem az SDX Professional aláíró alkalmazásnak, hanem a CSP összetevőnek kell teljesítenie.
Konklúzió: ***nem vonatkozik rá a követelmény***

A biometrikus, aláírót hitelesítő adatokra vonatkozó biztonsági követelmények

Bizt_köv46: Megbízható útvonalat kell biztosítani a biometrikus adatok továbbítására a biometrikus érzékelő egység és a biztonságos aláírás-létrehozó eszköz közé
Magyarázat: A követelményt /ha egyáltalán kezel biometrikus adatokat a rendszer/ nem az SDX Professional aláíró alkalmazásnak, hanem a CSP összetevőnek kell teljesítenie.
Konklúzió: ***nem vonatkozik rá a követelmény***

Bizt_köv47:
Magyarázat: A követelményt /ha egyáltalán kezel biometrikus adatokat a rendszer/ nem az SDX Professional aláíró alkalmazásnak, hanem a CSP összetevőnek kell teljesítenie.
Konklúzió: ***nem vonatkozik rá a követelmény***

2.2.6. Követelmények az aláírandó adat formattáló összetevőre (DTBSF)

Bizt_köv48: Az aláírás-létrehozó alkalmazásnak azt a helyes aláírandó adat formátumot kell előállítania, amelyet az aláíró által kiválasztott aláírási szabályzat határoz meg.
Magyarázat: "A megfelelésre vonatkozó fejlesztői indoklás elfogadva."
Konklúzió: **megfelel**

2.2.7. Követelmények az adat lenyomat készítő összetevőre (DHC)

Bizt_köv49: Az aláírás-létrehozó alkalmazásnak biztosítania kell egy “elfogadott” lenyomatoló algoritmus használatát lenyomatolásra.
Magyarázat: „A lenyomatoló algoritmust a CSP összetevő biztosítja, az SDX alkalmazás az EASZ-ban meghatározott lenyomatoló algoritmust választja ki a CSP meghívásakor. Ezen keresztül biztosítja az „elfogadott” algoritmus használatát.
Konklúzió: **megfelel**

Bizt_köv50: Az aláírás-létrehozó alkalmazásnak biztosítania kell az "emsa-pkcs1-v1_5" elektronikus aláírás input formátum (feltöltési módszer) kizárólagos használatát.

Magyarázat: „Az input formátum feltöltést a CSP összetevő biztosítja, az SDX alkalmazás az EASZ-ban meghatározott formátumot választja ki a CSP meghívásakor. Ezen keresztül biztosítja az „emsa-pkcs1-v1_5" aláírás formátum használatát.

Konklúzió: **megfelel**

Bizt_köv51: Az aláírás-létrehozó alkalmazásnak biztosítania kell a helyes aláírandó adatreprezentáns előállítását az elektronikus aláíráshoz.

Magyarázat: „Az adat reprezentáns előállítását a CSP összetevő biztosítja, az SDX alkalmazás az EASZ-ban meghatározott módon választja ki a CSP meghívásakor. Ezen keresztül biztosítja a megfelelő adatreprezentáns előállítását.

Konklúzió: **megfelel**

2.2.8. Követelmények a biztonságos aláírás-létrehozó eszköz és az aláírás-létrehozó alkalmazás közötti kommunikáció összetevőre (SSC)

Bizt_köv52: Az aláírás-létrehozó rendszernek támogatnia kell a fizikai interfész minden fontos részletét egy meghatározott tartományon belül, vagy egy meghatározott jellegzetességgel, az általa támogatott biztonságos aláírás-létrehozó eszköz típusok megfelelő működésének biztosítása érdekében.

Magyarázat: A követelményt nem az SDX Professional aláíró alkalmazásnak, hanem a CSP összetevőnek kell teljesítenie.

Konklúzió: ***nem vonatkozik rá a követelmény***

Bizt_köv53: Amennyiben vezeték nélküli összeköttetést használnak az aláírás-létrehozó alkalmazás és a biztonságos aláírás-létrehozó eszköz között, az SSC összetevőnek megfelelő eszközöket kell biztosítania a lehallgatás és a zavarás megakadályozása érdekében.

Magyarázat: A követelményt /ha egyáltalán alkalmaznak a rendszerben vezeték nélküli összeköttetést/ nem az SDX Professional aláíró alkalmazásnak, hanem a CSP összetevőnek kell teljesítenie.

Konklúzió: ***nem vonatkozik rá a követelmény***

Bizt_köv54: Az SSC összetevőnek biztosítania kell a biztonságos aláírás-létrehozó eszköz helyes funkcionalitásának kiválasztását, amennyiben a biztonságos aláírás-létrehozó eszköz ilyen kiválasztást tesz szükségessé (mert pl. több alkalmazást támogat párhuzamosan). Biztosítania kell az aláíró választása szerinti, az aláírás tulajdonságoknak megfelelő aláírás-létrehozó adat (magánkulcs) használatát, amennyiben több magánkulcs van a biztonságos aláírás-létrehozó eszközön tárolva.

Magyarázat: A követelményt nem az SDX Professional aláíró alkalmazásnak, hanem a CSP összetevőnek kell teljesítenie.

Konklúzió: ***nem vonatkozik rá a követelmény***

Bizt_köv55: Az SSC-t védeni kell a jogosulatlan módosításokkal szemben.

Magyarázat: A követelményt nem az SDX Professional aláíró alkalmazásnak, hanem a CSP összetevőnek kell teljesítenie.

Konklúzió: ***nem vonatkozik rá a követelmény***

2.2.9. Követelmények az SSCD/SCA hitelesítő összetevőre (SSA)

Bizt_köv56: Az SSA-nak támogatnia kell az aláírás-létrehozó alkalmazás és a biztonságos aláírás-létrehozó eszköz között az entitások hitelesítését, hogy megbízható jelzést adhasson az aláírónak egy sikeres hitelesítésről, és védenie kell az ezt követő kommunikációt egy biztonságos üzenetközvetítéssel.
Magyarázat: A követelményt nem az SDX Professional aláíró alkalmazásnak, hanem a CSP összetevőnek kell teljesítenie.
Konklúzió: ***nem vonatkozik rá a követelmény***

2.2.10. Követelmények az Input/Output interfészre (I/O)

Bizt_köv57: Intézkedéseket kell tenni annak biztosítására, hogy vírusok ne ronthassák el az SCA összetevőket, és hogy az esetlegesen vírussal fertőzött SCA összetevők megfelelően helyre legyenek állítva.
Magyarázat: "A megfelelésre vonatkozó fejlesztői indoklás elfogadva."
Konklúzió: **megfelel**

Bizt_köv58: Az SCA-nak védenie kell funkcionális összetevőinek sértetlenségét, és meg kell akadályozni, hogy behatolók elrontsák ezeket.
Magyarázat: "A megfelelésre vonatkozó fejlesztői indoklás elfogadva."
Konklúzió: **megfelel**

Bizt_köv59: Intézkedéseket kell tenni az aláírás-létrehozó alkalmazásban arra, hogy importált aláírás-létrehozó alkalmazás komponenseket csak egy biztonságos letöltés felhasználásával lehessen installálni.
Magyarázat: "A megfelelésre vonatkozó fejlesztői indoklás elfogadva."
Konklúzió: **megfelel**

2.2.11. Követelmények az aláírás-rendszer védelmére (biztonságos terület)

Bizt_köv60: Az aláírás-rendszer összes, az aláírás-létrehozás vagy aláírás-ellenőrzés folyamattal kölcsönhatásba lépő összetevőjét egy **biztonságos területen** kell megvalósítani.
Magyarázat: Az SDX alkalmazás az alkalmazási környezet komponenseinek integritását ellenőrizni tudja, beállítható komponens lista alapján. Mivel az SDX alkalmazás szoftver, ezért a futtató környezetnek biztosítania kell, hogy magát az SDX alkalmazást (teljes egészében) ne lehessen lecserélni
Konklúzió: **megfelel.**

3. Az SDX Professional aláíró alkalmazás megfelelése a követelményeknek

3.1 Az SDX Professional aláíró alkalmazás megfelelése a funkcionális követelményeknek

Funkcionális követelmény	Teljesülés
F_SCA_1	**megfelel**
F_SDP_1	**megfelel**
F_SDP_2	**megfelel**
F_SDP_3	**megfelel**
F_SDP_4	**megfelel**
F_SAV_1	**megfelel**
F_SAV_2	**megfelel**
F_SIC_1	**megfelel**
F_SIC_2	**megfelel**
F_SIC_3	**megfelel**
F_DTBSF_1	**megfelel**
F_DTBSF_2	**megfelel**
F_DHC_1	**megfelel**
F_DHC_2	**megfelel**
F_SSC_1	**megfelel**
F_SSC_2	**megfelel**
F_SSC_3	**megfelel**
F_SSC_4	**megfelel**
F_SSC_5	**megfelel**
F_SSC_6	**megfelel**
F_SSC_7	**megfelel**
F_SSC_8	**megfelel**
F_SSC_9	**megfelel**
F_SSA_1	nem vonatkozik rá a követelmény
F_SDC_1	**megfelel**
F_SDOC_1	**megfelel**
F_SLC_1	**megfelel**
F_SCPC_1	**megfelel**
F_I/O_1	**megfelel**
F_I/O_2	**megfelel**
F_I/O_3	**megfelel**
F_ISV_1	**megfelel**
F_ISV_2	**megfelel**
F_USV_1	**megfelel**
F_human_1	**megfelel**
F_human_2	**megfelel**
F_human_3	**megfelel**
F_human_4	**megfelel**
F_human_5	nem vonatkozik rá a követelmény
F_human_6	**megfelel**
F_machine_1	nem vonatkozik rá a követelmény
F_machine_2	nem vonatkozik rá a követelmény
F_general_1	**megfelel**
F_protocol	**megfelel**
F_format	**megfelel**
F_principles	**megfelel**

3.2 Az SDX Professional aláíró alkalmazás megfelelése a biztonsági követelményeknek

Biztonsági követelmény	Teljesülés
Bizt_köv1	**megfelel**
Bizt_köv2	**megfelel**
Bizt_köv3	nem vonatkozik rá a követelmény
Bizt_köv4	nem vonatkozik rá a követelmény
Bizt_köv5	nem vonatkozik rá a követelmény
Bizt_köv6	nem vonatkozik rá a követelmény
Bizt_köv7	**megfelel**
Bizt_köv8	**megfelel**
Bizt_köv9	nem vonatkozik rá a követelmény
Bizt_köv10	nem vonatkozik rá a követelmény
Bizt_köv11	**megfelel**
Bizt_köv12	**megfelel**
Bizt_köv13	**megfelel**
Bizt_köv14	**megfelel**
Bizt_köv15	nem vonatkozik rá a követelmény
Bizt_köv16	**megfelel**
Bizt_köv17	**megfelel**
Bizt_köv18	nem vonatkozik rá a követelmény
Bizt_köv19	**megfelel**
Bizt_köv20	**megfelel**
Bizt_köv21	**megfelel**
Bizt_köv22	**megfelel**
Bizt_köv23	**megfelel**
Bizt_köv24	**megfelel**
Bizt_köv25	nem vonatkozik rá a követelmény
Bizt_köv26	**megfelel**
Bizt_köv27	**megfelel**
Bizt_köv28	**megfelel**
Bizt_köv29	**megfelel**
Bizt_köv30	**megfelel**
Bizt_köv31	**megfelel**
Bizt_köv32	nem vonatkozik rá a követelmény
Bizt_köv33	nem vonatkozik rá a követelmény
Bizt_köv34	**megfelel**
Bizt_köv35	**megfelel**
Bizt_köv36	nem vonatkozik rá a követelmény
Bizt_köv37	nem vonatkozik rá a követelmény
Bizt_köv38	nem vonatkozik rá a követelmény
Bizt_köv39	nem vonatkozik rá a követelmény
Bizt_köv40	nem vonatkozik rá a követelmény
Bizt_köv41	nem vonatkozik rá a követelmény
Bizt_köv42	nem vonatkozik rá a követelmény
Bizt_köv43	nem vonatkozik rá a követelmény
Bizt_köv44	nem vonatkozik rá a követelmény
Bizt_köv45	nem vonatkozik rá a követelmény
Bizt_köv46	nem vonatkozik rá a követelmény
Bizt_köv47	nem vonatkozik rá a követelmény
Bizt_köv48	**megfelel**
Bizt_köv49	**megfelel**
Bizt_köv50	**megfelel**
Bizt_köv51	**megfelel**
Bizt_köv52	nem vonatkozik rá a követelmény
Bizt_köv53	nem vonatkozik rá a követelmény

Bizt_köv54	nem vonatkozik rá a követelmény
Bizt_köv55	nem vonatkozik rá a követelmény
Bizt_köv56	nem vonatkozik rá a követelmény
Bizt_köv57	**megfelel**
Bizt_köv58	**megfelel**
Bizt_köv59	**megfelel**
Bizt_köv60	Védett környezetben: **megfelel** (lásd 2. számú feltétel)

4. A Tanúsítási jelentés eredménye, érvényességi feltételei

4.1 Eredmények

A 4.2 alfejezetben megfogalmazott feltétel teljesülése esetén az SDX Professional aláíró alkalmazás alkalmas minősített elektronikus aláírások létrehozására és ellenőrzésére (a feltételek nem a megvalósított aláíró alkalmazásra, hanem annak telepítésére, környezetére, illetve az alkalmazható Elektronikus Aláírási Szabályzatra vonatkoznak).

4.2 Érvényességi feltételek

Az alábbiakban összefoglaljuk azokat a kötelezően betartandó, a jelen tanúsítvány érvényességére kiható feltételeket, melyek hozzájárulnak az SDX Professional aláíró alkalmazás által kezelt aláírások biztonságához.

1. számú feltétel
Az SDX Professional aláíró alkalmazást olyan biztonságos aláírás-létrehozó eszköz felhasználása mellett alkalmazzák, mely szerepel a Nemzeti Hírközlési Hatóság BALE nyilvántartásában.
A feltételek nem a megvalósított aláíró alkalmazásra, hanem annak telepítésére, környezetére, illetve az alkalmazható Elektronikus Aláírási Szabályzatra vonatkoznak.
Érintett biztonsági követelmények: Bizt_köv38,
Bizt_köv42,
Bizt_köv52,
Bizt_köv54,
Bizt_köv55,
Bizt_köv56

2. számú feltétel
Az SDX Professional aláíró alkalmazás működtetési környezetében technikai és eljárásrendi intézkedéseket kell tenni annak biztosítására, hogy az aláíró alkalmazást, valamint valamennyi az aláírás-létrehozás, aláírás-ellenőrzés folyamatokkal kölcsönhatásba lépő összetevőjét egy **biztonságos területen** valósítsák meg.
/Az SDX alkalmazás az alkalmazási környezet komponenseinek integritását ellenőrizni tudja, egy beállítható komponens lista alapján. Mivel az SDX alkalmazás egy szoftver, ezért a futtató környezetnek biztosítania kell, hogy magát az SDX alkalmazást (teljes egészében) ne lehessen lecserélni./
Érintett biztonsági követelmény: Bizt_köv60

3. számú feltétel
Az SDX Professional aláíró alkalmazást olyan Elektronikus Aláírási Szabályzattal együtt kell használni, amely az elektronikus aláírás során használt algoritmusokra és input formátumokra az alábbi követelményeket fogalmazza meg:

- aláíró algoritmus: **RSA** (legalább **1024** kulcsméret mellett).
- lenyomatoló algoritmus: **SHA-1**.
- aláírás formátum: **emsa-pkcs1-v1_5**,

Érintett biztonsági követelmények: Bizt_köv49,
Bizt_köv50,
Bizt_köv51

5. A követelményeknek való megfelelést ellenőrző független vizsgálat garancia szintje

A jelen tanúsítási jelentéshez figyelembe vett, a fejlesztőktől független ellenőrző vizsgálat garancia szintje az ISO 14508 /Common Criteria/ **EAL 3**-as szintjéhez hasonló volt. /Az EAL3 a fejlesztőktől függetlenül garantált biztonság közepes szintjét biztosítja./

A fejlesztőktől független ellenőrző vizsgálat összefoglalásaként egy értékelési jelentés készült.
Jelen tanúsítási jelentés alapvetően a fejlesztői bizonyítékokra, valamint az értékelési jelentésben megfogalmazott és dokumentált eredményekre épül.

Az értékelés az alábbi garanciaosztályokra terjedt ki:
- konfiguráció menedzselés
- kiszállítás és működtetés
- fejlesztés
- útmutató dokumentumok
- életciklus támogatás
- tesztek
- sebezhetőség felmérése

Az értékelés során a fejlesztőktől független minta tesztelésre is sor került.

6. A tanúsításhoz figyelembe vett dokumentumok

6.1 Termékmegfelelőségi követelményeket tartalmazó dokumentumok

Az elektronikus aláírásról szóló 2001. évi XXXV. törvény

CEN/ISSS/E-Sign; Area G1, 14170 munkacsoport egyezmény: Security Requirements for Signature Creation Systems

CEN/ISSS/E-Sign; Area G2, 14171 munkacsoport egyezmény: Procedures for Electronic Signature Verification

CEN/ISSS/E-Sign; Area V, 14172-4 munkacsoport egyezmény: EESSI Conformity Assessment Guidance - Part 4: Signature Creation Application and Procedures for Electronic Signature Verification

6.2 A tanúsítási jelentéshez figyelembe vett egyéb dokumentumok

6.2.1 A tanúsításhoz figyelembe vett, fejlesztői dokumentumok

Kérelem a tanúsítás elvégzésére
Kérdőív a tanúsítás kérelmezéséhez
SDX Professional 1.0 - Konfigurációmenedzsment eljárások - 2003.11.14,
Alkalmazások tervezése, fejlesztése - Minőségirányítási eljárás - 2002.05.07,
SDX Professional 1.0 - Funkcionális specifikáció - 2003.11.14,
SDX Professional 1.0 - Magas szintű terv - 2003.11.14.
SDX Professional 1.0 - Felhasználói kézikönyv - 2004.01.08,
SDX Professional 1.0 - Telepítési útmutató - 2003.11.14.
E-Group Magyarország Rt. Informatikai szabályzat v1.0
Alkalmazások tesztelése - Minőségirányítási eljárás - 2002.05.07,
SDX Professional Functional Tests - 2003.08.14 - 08.18,
SDX Professional 1.0 - A vizsgálat kiterjedtsége - 2003.08.14,
SDX Professional 1.0 - A vizsgálat mélysége - 2003.08.14.
SDX Professional 1.0 - Sebezhetőség vizsgálat - 2003.12.04

6.2.2 A tanúsításhoz figyelembe vett, fejlesztőktől független dokumentumok

Értékelési jelentés a Signed Document eXpert (SDX) professional 1.0 elektronikus aláíró alkalmazásról (készítette: HunGuard Kft.)

7. Rövidítések

API	Application Programming Interface
CRL	Certificate Revocation List
CSP	Cryptographic Service Provider
DHC	Data Hashing Component
DLL	Dynamic Link Library
DTBS	Data To Be Signed
DTBSF	DTBS Formatter
EAL	Evaluation Assurance Level
OCSP	Online Certificate Status Protocol
PKI	Public Key Infrastucture
PIN	Personal Identification Number
SAC	Signer's Authentication Component
SAV	Signature Attribute Viewer
SCA	Signature Creation Application
SDC	Signer's Document Composer
SDOC	Signed Data Object Composer
SDP	Signer's Document Presenter
SDX	Signed Document eXpert
SIC	Signer's Interaction Component
SLC	Signature Logging Component
SSA	SSCD/SCA Communicator Authenticator
SSC	SSCD/SCA Communicator
SSCD	Secure Signature Creation Device
TJ	Tanúsítási jelentés