Tanúsítási jelentés

Hung-TJ-005-2003

a JavaCard 32K CRISTAL intelligens kártya

biztonságos aláírás-létrehozó eszközről

/SchumbergerSema, France, Infineon Technologies AG, Germany/

/mikrochip:	**SLE66CX322P (GC A23 verzió),**
operációs rendszer:	**GEOS (SC_V3.0.0 verzió),**
aláírás-létrehozó alkalmazás:	**CRISTAL (AC_V1.0.0 verzió)/**

Tartalom

1. A Tanúsítási jelentés tárgya, feladata és hatóköre

Jelen Tanúsítási jelentés tárgya a JavaCard 32K CRISTAL intelligens kártya, melyet minősített aláírás létrehozásához kívánnak felhasználni, mint "biztonságos aláírás-létrehozó eszközt" (BALE).

A biztonságos aláírás-létrehozó eszközre vonatkozó követelményeket az elektronikus aláírásról szóló 2001. évi XXXV. törvény igen általánosan az alábbi módon fogalmazza meg 1. sz. mellékletében[1]:

1. *A biztonságos aláírás-létrehozó eszköznek megfelelő technikai és eljárási eszközökkel biztosítaniuk kell legalább a következőket:*
   a) *az aláírás készítéséhez használt aláírás-létrehozó adat aláírónként biztosan mindig különbözik, s titkossága kellően biztosított,*
   b) *az aktuálisan elérhető technológiával kellő bizonyossággal garantálható, hogy az aláírás készítéséhez használt aláírás-létrehozó adat nem rekonstruálható, megvalósítható annak a jogosulatlan felhasználókkal szembeni védelme, illetve az aláírás nem hamisítható.*

A fenti általános követelményeket kiegészíti a 2/2002. MeHVM irányelv[2] l. számú melléklete („elfogadott kriptográfiai algoritmusok"), mely meghatározza, hogy milyen aláíró algoritmusokat (mely paraméterekkel), kulcs létrehozási algoritmusokat, feltöltő módszereket, illetve lenyomat- (hash) függvényeket lehet minősített elektronikus aláíráshoz felhasználni.

Az EU Irányelvek fenti követelményeinek szakmai lebontásaként egy CEN Munkacsoport egyezmény született, mely a Közös szempontrendszer (Common Criteria, ISO/IEC 15408) által definiált védelmi profilok formájában határozta meg a biztonságos aláírás-létrehozó eszközökre vonatkozó részletes funkcionális és garanciális biztonsági követelményeket[3].

Funkcionalitás szempontjából három különböző BALE típus lett definiálva:

- 1-es típus: csak az aláírás-létrehozó / aláírás-ellenőrző adatpárok generálását támogatja, de nem állít elő elektronikus aláírást az általa előállított aláírás-létrehozó adattal[4],
- 2-es típus: biztosítja az elektronikus aláírás előállítását egy olyan aláírás-létrehozó adat felhasználásával, amelyet egy 1-es típusú BALE-től importál,

[1] Az idézett rész teljes mértékben megfelel (lévén szó szerinti fordítás) az Európai Parlament és Tanács 1999. december 13-án kelt, az elektronikus aláírásokra vonatkozó 1999/93/EK számú Irányelvének.

[2] „A minősített elektronikus aláírással kapcsolatos szolgáltatásokra és ezek szolgáltatóira vonatkozó biztonsági követelményekről."

[3] Bár az EU direktíva és a hazai elektronikus aláírás törvény magas szinten megfogalmazott követelményeit nem csak az említett védelmi profil követelményeinek való megfeleléssel lehet teljesíteni, az ebben a védelmi profilban megalapozott, megfogalmazott és megindokolt követelményrendszer biztosan helyes szakmai lebontása és részletezése az általános törvényi elvárásoknak.

[4] Szigorúan véve ez nem is BALE, csak azok a hitelesítés-szolgáltatók használhatják, melyek felvállalják az aláíró előfizetők számára történő kulcsgenerálás („aláírás-létrehozó eszközön az aláírás-létrehozó adat elhelyezése") szolgáltatását.

- 3-as típus: biztosítja mind az aláírás-létrehozó / aláírás-ellenőrző adatpárok generálását, mind az elektronikus aláírás előállítását az aláírás-létrehozó adattal.

A garanciális biztonság szempontjából egy szigorú és egy még szigorúbb változat készült:

- EAL4-es értékelés garancia szint,
- EAL4+ (emelt szintű) értékelési garancia szint

A JavaCard 32K CRISTAL intelligens kártya rendelkezik a fenti védelmi profilok közül a legerősebb funkcionalitású, egyúttal a szigorúbb garanciális követelményeket tartalmazó védelmi profilnak való megfelelőséget igazoló tanúsítvánnyal (Protection Profile – Secure Signature-Creation Device Type 3, version: 1.05, EAL4+, részletesen lásd 3. fejezet).

Jelen tanúsítási jelentés fő feladata annak megállapítása, hogy:

- a JavaCard 32K CRISTAL intelligens kártya alkalmas-e minősített aláírás-létrehozáshoz való felhasználásra,
- a Common Criteria adott védelmi profiljának való megfelelést igazoló tanúsítvány érvényessége, illetve a többi kielégítendő funkcionális és biztonsági követelmény teljesülése milyen korlátozásokat, feltételeket támaszt az intelligens kártya felhasználására.

Jelen tanúsítási jelentés ugyanakkor csak a 3-as típusú BALE-ként való felhasználással foglalkozik[5].

Jelen tanúsítási jelentésnek nem tárgya az érintett intelligens kártya mikrochip-je által támogatott egyéb funkcionalitás-halmaz, melyet a kártyán futó más alkalmazások elérhetnek, aktivizálhatnak (pl. a DES, Triple-DES és RSA titkosító algoritmusok).

A tanúsítási jelentés további szerkezete a következő:

- A JavaCard 32K CRISTAL intelligens kártya legfontosabb tulajdonságainak összefoglalása, beleértve az intelligens kártya hardver alapját képező mikrochip legfontosabb tulajdonságait is. (2. fejezet).
- A Common Criteria szerinti védelmi profilnak való megfelelőséget igazoló tanúsítvány eredményeinek összefoglalása, beleértve az intelligens kártya hardver alapját képező mikrochip korábbi értékelési és tanúsítási eredményeit is (3. fejezet).
- A megfelelőség viszonyítási alapját képező védelmi profil legfontosabb részeinek ismertetése (környezet, biztonsági célok, biztonsági követelmények, biztonsági funkciók) (4. fejezet).
- A megfelelőség tanúsításához figyelembe vett, mikrochip-re vonatkozó védelmi profil legfontosabb részeinek ismertetése (környezet, biztonsági célok, biztonsági követelmények, biztonsági funkciók) (5. fejezet).

[5] Mert a tanúsítási jelentés megrendelője csakis ilyen formában kívánja felhasználni az intelligens kártyát, attól függetlenül, hogy azt elvileg 2-es típusú BALE-ként is lehetne megszemélyesíteni és használni (igen eltérő feltétel rendszer mellett).

- A tanúsításhoz megkövetelt fejlesztői bizonyítékok (a mikrochip-re vonatkozó EAL5+, illetve az intelligens kártya egészére vonatkozó EAL4+ értékelési garancia szint elvárásai) (6. fejezet).
- A minősített aláírás-létrehozáshoz való alkalmasság megállapítása, valamint az alkalmazás feltételeinek és korlátainak a meghatározása (7. fejezet).
- A jelen tanúsítási jelentéshez figyelembe vett dokumentumok jegyzéke (8. fejezet).
- A felhasznált rövidítések jegyzéke (9. fejezet).

2. A JavaCard 32K CRISTAL legfontosabb biztonsági tulajdonságainak összefoglalása

A SchlumbergerSema Cyberflex nevű intelligens kártyája egy multiapplikációs Java Card. Megfelel mind a Java Card, mind a (Visa) Open Platform specifikációjának. A kártyán megvalósított virtuális gép különböző operációs rendszereket, s ezeken futó különböző alkalmazásokat támogat.

A JavaCard 32K CRISTAL intelligens kártya ennek a Cyberflex JavaCard-nak egy olyan speciális megvalósítása, mely az alábbi három fő komponensből áll:

- mikrochip (az Infineon SLE66CX322P típusú chip-je, mely valamennyi Cyberflex alapját képezi),
- operációs rendszer (a GEOS általános operációs rendszer, mely egyike a Cyberflex intelligens kártyákba ágyazható operációs rendszereknek),
- aláírás-létrehozó alkalmazás (a CRISTAL nevű alkalmazás, mely egy a Cyberflex intelligens kártyára tölthető, azon futtatható alkalmazás).

Jelen tanúsítási jelentés a Cyberflex ezen speciális megvalósítására vonatkozik, erre a továbbiakban JavaCard 32K CRISTAL intelligens kártyaként fogunk hivatkozni.

A JavaCard 32K CRISTAL intelligens kártya alábbi biztonsági tulajdonságait érintette az értékelés, majd az ezt követő (francia séma alapján végzett) tanúsítás:

- **az intelligens kártya öntesztelése**
  Minden munkaszakasz kezdetén a biztonsági funkciók tesztelik a RAM-ot az IC-t és ezek környezetét. Kérésre a biztonsági funkciók tesztelik az EEPROM-ot és a véletlen generátort is.
- **biztonsági események detektálása**
  Az intelligens kártya jelzi az alábbiakra vonatkozó hibákat: üzenet formátum, adat sértetlenség, környezeti feltételek elfogadható tartományból való kitérése, életciklus állapottal való összeférhetetlenség.
- **memória munkaterületek maradvány információ védelme**
  Az intelligens kártya törli munka memória területeit minden munkaszakasz kezdetén, illetve minden érzékeny adatra vonatkozó erőforrás kiosztás (allokáció) és erőforrás visszavétel (deallokáció) előtt.
- **tárolt adatok sértetlenségének ellenőrzése**
  Az intelligens kártya ellenőrzi a kriptográfiai kulcsok, hitelesítő adatok és az aláírandó adat reprezentáns sértetlenségét. Integritási hiba észlelése esetén hibajelzést ad, az érintett adatot elérhetetlenné teszi, s a folyamatban lévő műveletet megszakítja.
- **a műveletek és adatok megfigyelhetetlensége**
  Az intelligens kártya elrejti a külső megfigyelés elől az érzékeny adatokat továbbításuk és feldolgozásuk során.

- **az intelligens kártya menedzselése**
  Az intelligens kártya belső folyamatainak végrehajtása a kártya felhasználója által küldött megfelelő kezelő utasítások által irányítható. A kezelő utasítások üzenetei megfelelnek az ISO 7816 szabványban előírtaknak. Az intelligens kártya ellenőrzi mind az utasítás formátumát, mind az utasítás kód és megadott paramétereinek konzisztenciáját. Ellenőrzésre kerül az utasítások sorrendjének helyessége, illetve az adott életciklusban történő végrehajthatósága. Csak az ellenőrzésen sikeresen átesett utasítások hajtódnak végre.
- **kulcsok generálása**
  Az intelligens kártya 1024 bites RSA aláíró kulcspárt generál. (A kulcspár nyilvános összetevőjét szükség esetén képes előállítani a magánkulcs és a modulus alapján). Az intelligens kártya 112 bites triple DES munkaszakasz kulcsokat generál a VOP szabványnak megfelelő módon (a megbízható csatorna kiépítéséhez).
- **aláírás létrehozása**
  Az intelligens kártya a kívülről kapott vagy a kártyán tárolt adat lenyomatot (hash értéket) a PKCS #1 szabványnak megfelelően aláírja, 1024 bites RSA magánkulcsot használva. Az aláírás funkciót csak az előzetesen sikeresen hitelesített felhasználó aktivizálhatja.
- **adatok lenyomatolása**
  Az intelligens kártya a kívülről kapott vagy a kártyán lévő adatokra lenyomatot (hash értéket) készít, SHA-1 algoritmust használva. A kártya arra is képes, hogy befejezze a lenyomatolási folyamatot egy közbülső hash értékből kiindulva, az ehhez utólag fogadott adatokkal.
- **MAC kontrollösszeg képzése és ellenőrzése**
  Az intelligens kártya MAC kontrollösszeget képez, illetve ellenőriz, 112 bites triple DES kulcs felhasználásával.
- **megbízható csatorna kiépítése a külvilággal**
  Az intelligens kártya képes megbízható csatornát kiépíteni. A külső fél hitelességét egy olyan kölcsönös hitelesítési eljárással ellenőrzi, mely MAC-on alapuló kriptográfiai értéket használ. Egy belső számláló (3-ra) korlátozza a hitelesítési kísérleteket. Ez a funkció titkosítja és dekódolja a megbízható csatornán átküldött üzeneteket, illetve dekódolja a kívülről (a munkaszakasz kulcsok kialakításához) kapott kulcsokat 112 bites triple DES kulcsokat használva.
- **PIN kódok kezelése**
  Az intelligens kártya ellenőrzi a PIN kód kezelésével kapcsolatos valamennyi műveletet, köztük az aláíró hitelesítését, a PIN előállítását, ellenőrzését és módosítását.
- **hozzáférés ellenőrzés**
  Az intelligens kártya hozzáférés ellenőrzés funkciója ellenőrzi, hogy teljesülnek-e a hozzáférés feltételei a következő műveleteknél: az adminisztrátor általi kezdeti PIN kód létrehozás, illetve az aláíró általi PIN kód csere, nyilvános kulcs export és aláírás.

- **életciklus kontroll**
  Az intelligens kártya garantálja saját életciklusának megfelelő menedzselését. Folyamatosan ellenőrzi életciklus állapota sértetlenségét, megállapítja az aktuális fázist[6] és állapotot, illetve szükség esetén a következő állapotra vagy fázisra módosít. A fázisok módosítása visszafordíthatatlan folyamat.
- **biztonsági jellemzők meghatározhatósága**
  Az intelligens kártya az alábbi biztonsági jellemzők kezelését teszi lehetővé:

Jellemző (attribútum)	érték
Szerep	adminisztrátor / aláíró
Magán-nyilvános kulcspár kezelés	felhatalmazott / nem felhatalmazott
Nyilvános kulcs biztonságos importálásának engedélyezettsége	igen / nem
Magánkulcs működtetése (aláírás)	igen / nem
Aláírandó adat küldése egy felhatalmazott aláírás-létrehozó alkalmazástól	igen / nem

- **a mikrochip biztonsági tulajdonságainak menedzselése**
  Az intelligens kártya biztosítja mikrochip-je biztonsági tulajdonságainak menedzselését. Ez magában foglalja a chip állapotának vizsgálatát, biztonsági események generálását és tárolását, a chip védőburkának sérülése esetén a sérülés komolyságától függő intézkedések foganatosítását, a véletlen időgenerálás kontrollálását.
- **biztonságos állapotba való visszatérés**
  Az intelligens kártya garantálja, hogy a megelőző biztonságos állapotába kerüljön vissza, ha az alábbiak valamelyike bekövetkezik: korlátnál alacsonyabb áramerősség, korlátnál magasabb feszültség, órafrekvencia kiesése a megengedett (alsó és felső korlátok közötti) tartományból, integritás hiba.

A JavaCard 32K CRISTAL intelligens kártya alapját az Infineon SLE66CX322P típusú chip-je biztosítja.
Az SLE66CX322P egy teljes mikrochip, melynek hardver alkotó elemei az alábbiak:

- központi feldolgozó egység (CPU),
- memóri kezelő egység (MMU),
- memóriák:
  - RAM (256 bájt IRAM, 4 Kbájt XRAM)
  - ROM (136 Kbájt felhasználói, 8 Kbájt tesztelési, 32 Kbájt EEPROM)
- biztonsági logika,
- megszakító modul,
- busz rendszer,
- belső óra,
- megszakítás-vezérlésű I/O csatlakozás,
- véletlenszám generátor, kontrollösszeg képző modul,
- egy kriptográfiai műveleteket végző modul (ACE),

[6] Az intelligens kártyák életciklusainak modellezését, benne a jelen intelligens kártyára is érvényes 7 fázisos megközelítéssel, lásd az „Intelligens kártyák” című HunGuard tanulmányt.

- egy olyan DES algoritmus végrehajtását támogató kriptográfiai modul, melyet speciálisan úgy terveztek, hogy ellenálljon a DPA (differenciális áramfelvétel vizsgálat) és EMA (elektromágneses vizsgálat) támadásoknak.

Az SLE66CX322P mikrochip förmver alkotó elemei az alábbiak:

- erőforrás kezelő rendszer (RMS) rutinok az EEPROM programozására (a chip gyártó által elhelyezve, a normál felhasználói ROM egy zárolt területén tárolva),
- önteszt szoftver (STS) teszt és inicializáló rutinjai (védett teszt ROM-ban tárolva, csak a gyártási fázisokban elérhető módon).

Az SLE66CX322P mikrochip szoftver alkotó elemei az alábbiak:

- RSA2048 könyvtár, mely magas-szintű interfészt biztosít az RSA algoritmusok (kulcspár generálás, aláírás létrehozás, aláírás ellenőrzés, RSA modulus visszaszámítás) ACE hardver komponensen történő megvalósításához (a könyvtárt forrás kód formájában biztosítják a beágyazott szoftver fejlesztői számára),
- operációs rendszer (nem volt része a mikrochip alap értékelésének és tanúsításának),
- alkalmazások (nem volt része a mikrochip alap értékelésének és tanúsításának).

Az SLE66CX322P mikrochip-et nagy biztonságot igénylő alkalmazások széles skálájához tervezték. Támogatja a nagy sebességet igénylő hitelesítési, titkosítási és digitális aláírási folyamatokat. Számos (teljesen hardverben megvalósított, vagy szoftver úton felügyelt) biztonsági tulajdonsága garantálja a megfelelő műveleteket, illetve a tárolt adatok bizalmasságát és sértetlenségét. Ezek a tulajdonságok magukba foglalják a memóriavédelmet, az információ kiszivárgása elleni védelmet és azokat az érzékelőket, melyek csak speciális környezeti feltételek teljesülése esetén teszik lehetővé a műveletek végrehajtását.

Az SLE66CX322P mikrochip alábbi biztonsági tulajdonságait érintette az előzetes értékelés, az ezt követő (német séma alapján végzett) tanúsítás, melynek eredményeit a JavaCard 32K CRISTAL intelligens kártya értékelése és tanúsítása is mint kiindulási alapot vett figyelembe:

- **működési állapot ellenőrzés**
  Az SLE66CX322P helyes működése az RSA2048 könyvtárral csak bizonyos tartományon belül garantált. Az ezen tényt kihasználni igyekvő támadások megakadályozása érdekében szükség van annak észlelésére, hogy a környezeti körülmények elhagyták a garantált tartományt. Minden műveleti jelet megszűrnek a hibás működés elkerülése érdekében, egyúttal folyamatosan figyelemmel kísérik a működési állapotokat (a feszültséget, az óra jelet, a frekvenciát, a hőmérsékletet és az elektomágneses sugárzást érzékelő szenzorokkal).
- **életciklus fázis kezelés a teszt üzemmód lezárásával**
  A mikrochip korai életciklus fázisában, elindításkor a különböző fázis azonosítók függvényében választani lehet a felhasználói és a teszt üzemmód között. Ha a teszt üzemmód aktív, valamennyi művelet előtt hitelesítést kér a chip. Ez a teszt lezárás a biztonságot érvényre juttató és a felhasználói

szoftverek elkülönítését garantálja. A chip felhasználóhoz történő leszállítását követően a chip csak felhasználói üzemmódban használható.

- **kifürkészés elleni védelem**
  Számos biztonsági mechanizmus, köztük az álcázó topológiai tervezés próbál védekezni a felhasználói adatok és a tervezés kifürkészése ellen, mind a működtetés során, mind kikapcsolt állapotban.
- **Adatok titkosítása és álcázása**
  A mikrochip memóriatartalma titkosításra kerül, hogy védjen a tárolt, illetve a belül továbbított adatok elemzése ellen. Csak a kulcs tulajdonosának van lehetősége az adatok kiolvasására. A kiszivárgó információ értelmezésének megakadályozására az információ közé véletlen elemeket iktatnak. Ez különösen az áramfelvétel különbségére irányuló (DPA) támadás ellen hatékony.
- **Véletlenszám generálás**
  A véletlen adatok alapvető fontossággal bírnak mind a kriptográfiai, mind a fizikai biztonsági mechanizmusok támogatásában. A mikrochip-ben egy valódi, fizikai véletlen jelenségen alapuló véletlenszám generátor van. A generált véletlen adatokat mind a biztonságot érvényre juttató funkciók, mind a felhasználói szoftverek használhatják.
- **A biztonsági funkciók öntesztelése**
  A mikrochip-nek egy hardver-vezérelt öntesztje, mely elindítható a felhasználói szoftverekből, valamint közvetlenül elindul a „működési állapot ellenőrzés”, a „véletlenszám generálás” és „a fizikai támadások érzékelése és jelzése” biztonsági funkciók tesztelésére is. A tesztek érzékelnek minden szenzor megváltoztatására irányuló kísérletet is.
- **A fizikai támadások érzékelése és jelzése**
  A mikrochip teljes felülete egy aktív védőréteggel van biztosítva. A felületen keresztüli támadásokat azonnal érzékeli ez a biztonsági funkció, akár átlépik a védőréteg határait, akár csak érintkezésbe lépnek vele.
- **Memória kezelő egység**
  A mikrochip memória kezelő egysége lehetővé teszi a felhasználói szoftverek számára különböző hozzáférési jogosultságok meghatározását az egyes memória területekre nézve. A hozzáférés megsértése esetén a memória kezelő egység egy nem maszkolható megszakítást generál, így a megszakításokat kezelő rutin reagálhat a hozzáférés megsértésére. A memória kezelő egység beállítása és a memória területek kijelölése a felhasználói szoftverből történhet.
- **Kriptográfiai támogatás**
  A mikrochip hajtja végre a kriptográfiai műveleteket. Számos hardver gyorsítóval van ellátva a szabványos kriptográfiai algoritmusok támogatására, köztük egy DES hardver titkosító egység, valamint egy szoftver-hardver kombinációjú egység az RSA kriptográfia és az RSA kulcsgenerálás támogatására.

3. A Common Criteria szerinti értékelés és tanúsítás eredményeinek összefoglalása

A JavaCard 32K CRISTAL intelligens kártya megfelel a BSI-0006-2002 védelmi profilnak (Secure Signature-Creation Device Type 3, version: 1.05, EAL4+).

A tanúsítás a Common Criteria közös értékelési szempontrendszer szerint, a francia séma alapján történt.

Az értékelés (és tanúsítás) garanciális szintje EAL4+. Az emelt szintű garanciális szintet az alábbi kiegészítő komponensek adták:

- ADV_IMP.2 /Az értékelés tárgya biztonsági funkcióinak kivitelezése (csak EAL5-ös szinten elvárt)/,
- ALC_DVS.2 /A biztonsági intézkedések elégségessége (csak EAL6-os szinten elvárt)/,
- AVA_MSU.3 /A nem biztonságos állapotok vizsgálata és tesztelése (csak EAL6-os szinten elvárt)/,
- AVA_VLA4 /Nagymértékű ellenállás (csak EAL6-os szinten elvárt)/.

A tanúsítás alapját képező biztonsági értékelést a Serma Technologies laboratórium végezte.

A tanúsítás szponzora a SchlumbergerSema volt.

A JavaCard 32K CRISTAL értékelése egy olyan összetett értékelés volt, mert figyelembe vette a termék hardver platformját biztosító SLE66CX322P mikrochip korábbi értékelési és tanúsítási eredményeit is.
Az SLE66CX322P mikrochip tanúsítás jellemzői az alábbiak voltak:

A Common Criteria közös értékelési szempontrendszer szerint történt, a német séma alapján.

A tanúsítást a BSI végezte.

Az értékelés és tanúsítás a következő védelmi profilnak való megfelelést igazolta, tanúsította: Smartcard IC Platform Protection Profile (Registered and Certified by BSI, BSI-PP-0002).

Az értékelés (és tanúsítás) garanciális szintje EAL5+. Az emelt szintű garanciális szintet az alábbi kiegészítő komponensek adták:

- ALC_DVS.2 /A biztonsági intézkedések megfelelőségének igazolása (csak EAL6-os szinten elvárt)/
- AVA_MSU.3 /A nem biztonságos állapotok elemzése és vizsgálata (csak EAL6-os szinten elvárt)/
- AVA_VLA4 /Nagymértékű ellenállás(csak EAL6-os szinten elvárt)/.

Ennek a tanúsításnak a szponzora az Infineon Technologies AG volt.

4. A JavaCard 32K CRISTAL értékelési követelményei a Common Criteria megfelelő védelmi profilja szerint

Az alábbiakban áttekintjük annak a védelmi profilnak a legfontosabb elemeit (a környezetre vonatkozó állításokat, valamint a biztonsági célokat, követelményeket és funkciókat), melynek való megfelelőséget a JavaCard 32K CRISTAL intelligens kártya értékelését végző laboratórium[7] vizsgálta és igazolta.

4.1 A JavaCard 32K CRISTAL intelligens kártya biztonsági környezete

Az intelligens kártyának az alábbi értékeket kell megvédenie:
1. az aláírás-létrehozó adat bizalmassága,
2. az aláírás-ellenőrző adat sértetlensége, ha exportálásra kerülnek,
3. az aláírandó adat és annak reprezentánsa (részleges vagy teljes lenyomatolt képe) sértetlensége,
4. a hitelesítés során megadott PIN kód bizalmassága és hitelessége,
5. a PIN kód kártyán tárolt, transzformált változatának sértetlensége és bizalmassága,
6. az aláírás-létrehozó adatot felhasználó BALE aláírás-létrehozási funkciójának sértetlensége, helyes működése,
7. az elektronikus aláírások jogi hitelessége.

4.1.1 A biztonságra irányuló veszélyek

A fizikai környezet sebezhetőségének kihasználása
Egy támadó kölcsönhatásba lép az intelligens kártyával abból a célból, hogy kihasználja a fizikai környezet sebezhetőségét, és ezzel a biztonságot veszélyezteti.

A magánkulcs letárolása, lemásolása
Az aláírás-létrehozó adat intelligens kártyán kívüli tárolása vagy lemásolása veszélyt jelent az elektronikus aláírások jogi hitelességére.

Az aláírás-létrehozás adatok származtatása
Az aláírás-létrehozó adat titkosságára veszélyt jelent, ha egy támadó az aláírás-létrehozó adatot származtatni tudja nyilvánosan ismert adatokból, mint például az aláírás-létrehozó adathoz tartozó aláírás-ellenőrző adatból, vagy az aláírás-létrehozó adat felhasználásával előállított aláírásból, vagy más olyan adatból, amely a kommunikációk során az intelligens kártyán kívülre kerül.

Az aláírás-létrehozó adat kiszivárgása
Az aláírás-létrehozó adat kiszivárog a generálás, tárolás vagy aláírás készítésre való felhasználás során.

Az elektronikus aláírás hamisítása
A támadó meghamisítja az intelligens kártya által készített elektronikus aláírással aláírt adatokat úgy, hogy azt nem észleli az aláíró vagy egy harmadik fél.

[7] Serma Technologies

Az elektronikus aláírások letagadása
Az aláíró letagadja, hogy ő írta alá az adatokat a saját ellenőrzése alatt álló intelligens kártyában lévő aláírás-létrehozó adat felhasználásával, annak ellenére, hogy az aláírás sikeresen ellenőrzésre került az érvényes (nem visszavont) tanúsítványában található aláírás-ellenőrző adat segítségével.

Az aláírás-ellenőrző adatok hamisítása
Egy támadó meghamisítja az intelligens kártya által nyújtott aláírás-ellenőrző adatot.

Az aláírandó adat reprezentánsának meghamisítása
Egy támadó módosítja az aláírás-létrehozó alkalmazás által küldött aláírandó adat reprezentánst, s így az intelligens kártya ténylegesen a módosított értéket írja alá.

Visszaélés az intelligens kártya aláírás-létrehozó funkciójával
Egy támadó visszaél az intelligens kártya aláírás-létrehozó funkciójával abból a célból, hogy aláírt adatot hozzon létre olyan adatokhoz, amelyeket az aláíró nem akart aláírni.

4.1.2 Érvényre juttatandó biztonsági szabályok

Szakértő támadók
Az intelligens kártyát szándékosan támadhatják magas támadó képességgel rendelkező szakértők, akik részletes ismeretekkel rendelkeznek az intelligens kártya biztonsági alapelveiről, koncepcióiról. Az intelligens kártyának védeni kell az aláírás-létrehozó adatot az ilyen támadásokkal szemben (is).

Minősített tanúsítvány
A hitelesítés-szolgáltató megbízható tanúsítvány-létrehozó alkalmazást használ arra, hogy minősített tanúsítványt állítson elő a BALE által generált aláírás-ellenőrző adathoz. A minősített tanúsítvány tartalmazza a jogszabályokban[8] meghatározott elemeket, köztük az aláíró nevét és az aláíró kizárólagos ellenőrzése alatt álló intelligens kártyán implementált aláírás-létrehozó adatnak megfelelő aláírás-ellenőrző adatot[9]. A hitelesítés-szolgáltató a tanúsítvány vagy más nyilvánosan rendelkezésre álló információn keresztül biztosítja, hogy az intelligens kártyának az aláírással kapcsolatos használata nyilvánvaló legyen.

A rendszer teljes életciklusára kiterjedő biztonság
Az informatika biztonság szempontjait az intelligens kártya és az aláírás-létrehozó adat teljes életciklusában figyelembe kell venni.

Minősített elektronikus aláírás
Az aláíró egy aláírás-létrehozó rendszert használ az adatok minősített elektronikus aláírással való aláírására. Az aláírandó adatot az aláírás-létrehozó alkalmazás megjeleníti az aláíró számára. A minősített elektronikus aláírás egy minősített tanúsítványon alapul, és egy BALE hozza létre.

Az intelligens kártya, mint biztonságos aláírás-létrehozó eszköz
Az intelligens kártya az aláírás létrehozáshoz használt aláírás-létrehozó adatot az aláíró kizárólagos ellenőrzése alatt implementálja. Az aláírás létrehozásra szolgáló

[8] lásd a 2001. évi XXXV. elektronikus aláírási törvény 2. számú mellékletét
[9] Vagyis az aláíró magánkulcsának megfelelő nyilvános kulcsot.

aláírás-létrehozó adat gyakorlatilag csak egyszer fordulhat elő.

4.2 A JavaCard 32K CRISTAL intelligens kártya biztonsági céljai

Fizikai kisugárzás elleni védelem
Oly módon kell tervezni és felépíteni a rendszert, hogy az információ visszaállítását lehetővé tévő kisugárzásokat meghatározott korlátok közé szorítsa.

Aláírás-létrehozó / aláírás-ellenőrző adatpárok generálása
A JavaCard 32K CRISTAL intelligens kártyának biztosítania kell, hogy az aláírás-létrehozó / aláírás-ellenőrző adatpár generálását csak feljogosított felhasználók válthassák ki.

Az életciklus biztonsága
A fejlesztőnek a JavaCard 32K CRISTAL intelligens kártya fejlesztési fázisa során eszközöket, technikákat és biztonságos körülményeket kell biztosítania. Az intelligens kártyának támogatnia kell a hitelesítés-szolgáltatót és az aláírót abban, hogy az üzemeltetési fázis során észleljék és pótolják a hiányosságokat. Az intelligens kártyának biztonságos aláírás-létrehozó adat megsemmisítési technikákat kell nyújtania.

Az aláírás-létrehozó adatok titkossága
Az (aláírás előállítására szolgáló) aláírás-létrehozó adat titkosságát még magas támadási potenciállal rendelkező támadások ellen is biztosítani kell.

Az aláírás-ellenőrző és az aláírás-létrehozó adat közötti megfelelés
A JavaCard 32K CRISTAL intelligens kártyának biztosítania kell az aláírás-ellenőrző és az aláírás-létrehozó adat közötti megfelelést, amikor ezeket előállítja. Az intelligens kártyának igény esetén bizonyítania kell a megfelelést az általa tárolt aláírás-létrehozó adat és a számára elküldött aláírás-ellenőrző adat között.

Az aláírás-ellenőrző adat hitelességének biztosítása
A JavaCard 32K CRISTAL intelligens kártyának eszközöket kell nyújtania arra, hogy lehetővé váljon a tanúsítvány-létrehozó alkalmazás számára az intelligens kártya által exportált aláírás-ellenőrző adat hitelességének ellenőrzése.

A módosítás detektálása
A JavaCard 32K CRISTAL intelligens kártyának rendszer szintű tulajdonságokat kell biztosítania, amelyekkel a rendszer komponensek fizikai módosításait észlelni lehet, egyúttal ezeket a tulajdonságokat alkalmaznia kell a biztonság megszegésének korlátozására.

A fizikai módosítással szembeni ellenállás
A JavaCard 32K CRISTAL intelligens kártya akadályozza meg a speciális rendszer eszközök és komponensek fizikai módosításait, vagy álljon ellen ezeknek.

Az aláírás-létrehozó adatok egyedisége
A JavaCard 32K CRISTAL intelligens kártyának biztosítania kell a minősített elektronikus aláírásra szolgáló aláírás-létrehozó / aláírás ellenőrző adatpár kriptográfiai minőségét. Az aláírás előállításhoz használt aláírás-létrehozó adat „gyakorlatilag csak egyszer fordulhat elő", és ezt ne lehessen visszaállítani az aláírás-ellenőrző adatból. Ebben az összefüggésben a „gyakorlatilag egyszer fordulhat elő" kifejezés azt jelenti, hogy az azonos aláírás-létrehozó adatok valószínűsége elhanyagolhatóan kicsi.

Az aláírandó adat-reprezentáns sértetlenségének ellenőrzése
A JavaCard 32K CRISTAL intelligens kártyának ellenőriznie kell, hogy az aláírás-létrehozó alkalmazásból származó aláírandó adat-reprezentáns nem lett módosítva az aláírás-létrehozó alkalmazás és az intelligens kártya közötti átvitel során. Az intelligens kártyának biztosítania kell azt is, hogy önmaga sem módosítja az aláírandó adat-reprezentánst.

Az aláírás előállítási funkció csak a törvényes aláírónak áll rendelkezésre
A JavaCard 32K CRISTAL intelligens kártyának az aláírás előállítási funkciót csak a törvényes aláíró számára szabad biztosítania, és védenie kell az aláírás-létrehozó adatot a mások általi felhasználással szemben. Az intelligens kártyának ellen kell állnia a magas támadási potenciállal rendelkező támadásoknak.

Az elektronikus aláírás kriptográfiai biztonsága
A JavaCard 32K CRISTAL intelligens kártyának olyan elektronikus aláírást kell előállítania, amelyet az aláírás-létrehozó adat ismerete nélkül nem lehet meghamisítani erőteljes dekódolási technikák használatával sem. Az aláírás-létrehozó adatot ne lehessen visszaállítani az elektronikus aláírások felhasználásával. Az elektronikus aláírásoknak ellen kell állniuk az ilyen támadásoknak még akkor is, ha ezeket magas támadási potenciállal hajtják végre.

4.3 A JavaCard 32K CRISTAL intelligens kártya funkcionális biztonsági követelményei

Az alábbiakban felsoroljuk a védelmi profil funkcionális biztonsági követelményeit ***(vastag és dőlt betűvel megjelenítve***), majd alatta röviden kitérünk arra is, hogy a JavaCard 32K CRISTAL intelligens kártya hogyan felel meg az egyes követelményeknek.

Kriptográfiai kulcs generálás (FCS_CKM.1)
Az intelligens kártya képes 1024 bites RSA, valamint 112 bites triple DES kriptográfiai kulcsokat generálni. (Az RSA kulcsot digitális aláírás céljából, a triple DES kulcsot pedig a host oldallal kialakított megbízható csatorna védelmét ellátó munkaszakasz kulcsként.)

Kriptográfiai kulcs megsemmisítés (FCS_CKM.4)
Az intelligens kártya képes tárolt kulcsértékeinek fizikailag visszafordíthatatlan megsemmisítésére. (Az aláírás-létrehozó adatot /RSA magánkulcsot/ az aláíró külön kérésére, a munkaszakasz kulcsokat /triple DES kulcsot/ pedig a munkaszakasz

lezárása után automatikusan megsemmisíti).

Kriptográfiai eljárás (FCS_COP.1)
Az intelligens kártya képes az alábbi kriptográfiai algoritmusok szabványos végrehajtására:

- az RSA aláírás-létrehozó és aláírás-ellenőrző adatok egymásnak való megfelelésének ellenőrzése az 1024 bites RSA kulcsgenerálás során,
- Az RSA aláírás-ellenőrző adat visszaszámolása az aláírás-létrehozó és a nyilvános kitevő alapján,
- Az RSA aláíró algoritmus, 1024 bites kulcsmérettel és a PKCS #1 szabványnak megfelelően,
- Az aláírandó adatok lenyomatolása az SHA-1 hash függvénnyel.

Részleges hozzáférés ellenőrzés (FDP_ACC.1)
Az intelligens kártya képes a következő hozzáférés ellenőrzések érvényre juttatására:

- az aláírás-létrehozó adatot csak az aláíró generálhatja (inicializáláskor),
- az aláírás-ellenőrző adatot csak az aláíró exportálhatja (tanúsítvány generálása céljából, a minősített hitelesítés-szolgáltatóhoz),
- a hitelesítő adatot (PIN kód) csak az adminisztrátor hozhatja létre (a megszemélyesítés fázisában),

Biztonsági jellemzőkön alapuló hozzáférés ellenőrzés (FDP_ACF.1)
Az intelligens kártya az előbb felsorolt hozzáférés ellenőrzéseket az alábbi biztonsági jellemzőkre alapulva juttatja érvényre:

- az aláírás-létrehozó adat csak akkor generálható, ha:
  - a „szerep” biztonsági jellemző „aláíró” értékre,
  - a „magán-nyilvános kulcspár kezelés” biztonsági jellemző pedig „felhatalmazott” értékre van állítva[10]
- az aláírás-ellenőrző adat csak akkor exportálható, ha:
  - a „szerep” biztonsági jellemző „aláíró” értékre,
  - a „nyilvános kulcs biztonságos importálásának engedélyezettsége” biztonsági jellemző pedig „igen” értékre van állítva
- a hitelesítő adatot (PIN kód) csak akkor hozható létre, ha:
  - a „szerep” biztonsági jellemző „adminisztrátor” értékre van állítva.

Részleges maradvány információ védelem (FDP_RIP.1)
Az intelligens kártya biztosítja, hogy erőforrás visszavétel (deallokáció) után semmilyen korábbi információ tartalom ne legyen hozzáférhető az alábbi objektumokra nézve:

- aláírás-létrehozó adat (magánkulcs),
- hitelesítő adat (megadott PIN kód),
- hitelesítést ellenőrző adat (a PIN kód kártyán tárolt képe).

[10] Vagyis sem az adminisztrátor nem generálhat, sem az olyan aláíró, akit az adminisztrátor nem hatalmazott fel erre a megszemélyesítés fázisában.

A tárolt adatok sértetlenségének figyelése és beavatkozás (FDP_SDI.2)
Az intelligens kártya biztosítja az általa folyamatosan tárolt adatok közül az alábbiak sértetlenségének ellenőrzését:

- aláírás-létrehozó adat (magánkulcs),
- hitelesítést ellenőrző adat (a PIN kód kártyán tárolt képe),
- aláírás-ellenőrző adat nyilvános kulcs) /amennyiben az aláíró a kártyán tárolja/.

Az intelligens kártya biztosítja az általa átmenetileg tárolt adatok közül az alábbiak sértetlenségének ellenőrzését:

- aláírandó adatok.

Mindkét fenti adatcsoportra, integritás hiba észlelése esetén az intelligens kártya:

- megakadályozza a módosult adatok használatát, egyúttal
- értesíti az aláírót az integritás hibáról (hibaüzenet generálásával).

Alapszintű adat-csere bizalmasság (FDP_UCT.1)
Az intelligens kártya képes biztosítani a „megszemélyesítés" és a „hitelesítő adat cseréje" funkció során kapott, illetve az „aláírás-ellenőrző adat kiadása" funkció során küldött adatok (első PIN kód, csere PIN kód, nyilvános kulcs) védelmét jogosulatlan felfedés ellen (titkosítással).

Az adatcsere sértetlensége (FDP_UIT.1)
Az intelligens kártya képes biztosítani az „aláírás-ellenőrző adat kiadása" funkció során küldött adat (nyilvános kulcs) védelmét a módosításból és beszúrásból eredő hibáktól, továbbá a „megszemélyesítés" és a „hitelesítő adat cseréje" funkció során kapott adatok (első PIN kód, csere PIN kód) védelmét a módosításból, törlésből és beszúrásból eredő hibákból (MAC képzéssel).
A fentieken kívül, az intelligens kártya képes az általa fogadott aláírandó adatokra is észlelni a módosításból, törlésből és beszúrásból eredő hibákat (MAC képzéssel).

A hitelesítési hiba kezelése (FIA_AFL.1)
Az intelligens kártya képes detektálni, ha 3 egymást követő téves hitelesítési kísérlet történt. Ilyen esetben a kártya blokkolja a PIN kódot.

A felhasználói jellemzők meghatározása (FIA_ATD.1)
Az intelligens kártya képes kezelni az egyedi felhasználókhoz (aláíróhoz) tartozó biztonsági jellemzők következő listáját: PIN kód.

Az azonosítás időzítése (FIA_UID.1)
Az aláíró azonosítása előtt az intelligens kártya az alábbiakat engedi meg:

- egy megbízható útvonal létesítése a helyi felhasználó és az intelligens kártya között (az FTP_TRP.1-nek megfelelően),
- egy megbízható csatorna létesítése a megbízható aláírás-létrehozó alkalmazás és az intelligens kártya között (az FTP_ITC.1-nek megfelelően).

Az intelligens kártya bármilyen további, általa közvetített tevékenységet csak akkor engedélyez, ha az aláíró sikeresen azonosította magát.[11]

[11] Ez alapvetően az aláírás létrehozásával kapcsolatos tevékenységekre vonatkozik. Nem kifejezetten az aláírással kapcsolatos egyéb tevékenységek végrehajtása lehetséges az aláíró azonosítása előtt is.

A hitelesítés időzítése (FIA_UAU.1)
Az aláíró hitelesítése előtt az intelligens kártya az alábbiakat engedi meg:

- az aláíró azonosítása (a FIA_UID.1-nek megfelelően),
- egy megbízható útvonal létesítése a helyi felhasználó és az intelligens kártya között (az FTP_TRP.1-nek megfelelően),
- egy megbízható csatorna létesítése a megbízható aláírás-létrehozó alkalmazás és az intelligens kártya között (az FTP_ITC.1-nek megfelelően).

Az intelligens kártya bármilyen további, általa közvetített tevékenységet csak akkor engedélyez, ha az aláíró sikeresen hitelesítette magát[12].

A biztonsági funkciók viselkedésének kezelése (FMT_MOF.1)
Az intelligens kártya képes az aláírás-létrehozás funkció aktivizálását korlátozni, csak az aláíró számára elérhetővé téve azt.

A biztonsági jellemzők kezelése (FMT_MSA.1)
Az intelligens kártya képes:

- az „inicializálás” funkció „magán-nyilvános kulcspár kezelés” biztonsági jellemzőjének módosítási lehetőségét az adminisztrátorra korlátozni,
- az „aláírás-létrehozás” funkció „magánkulcs működtetése (aláírás)” biztonsági jellemzőjének módosítási lehetőségét az aláíróra korlátozni.

Biztonságos biztonsági jellemzők (FMT_MSA.2)
Az intelligens kártya biztosítja, hogy biztonsági jellemzőknek csak biztonságos értékek lesznek elfogadva.

Statikus jellemző inicializálás (FMT_MSA.3)
Az intelligens kártya az „inicializálás” és az „aláírás-létrehozás” biztonsági szabályokra korlátozó alapértékeket szolgáltat: az aláírás-létrehozó adat generálása után a „magánkulcs működtetése (aláírás)” biztonsági jellemzőt „nem” értékre állítja.
Az intelligens kártya lehetővé teszi az adminisztrátor számára, hogy a fenti korlátozó (default) alapértéket felülírja („igen”-re állítsa a megszemélyesítés folyamán).

A biztonsági funkciók adatainak kezelése (FMT_MTD.1)
Az intelligens kártya a hitelesítő adatok (PIN kód) módosításának lehetőségét az aláíróra korlátozza.

Biztonsági szerepkörök (FMT_SMR.1)
Az intelligens kártya képes az alábbi szerepek kezelésére: adminisztrátor, aláíró.
Az intelligens kártya képes összekapcsolni a felhasználókat az egyes szerepekkel.

Az absztrakt gép tesztelése (FPT_AMT.1)
Az intelligens kártya a kezdeti rendszer indítás során végrehajt egy olyan teszt-sorozatot, mely kimutatja, hogy helyesen működnek azok a biztonsági feltételek, melyeket az intelligens kártya alapját képező absztrakt gép (jelen esetben a mikrochip és annak könyvtára) biztosít.

[12] Ez alapvetően az aláírás létrehozásával kapcsolatos tevékenységekre vonatkozik. Nem kifejezetten az aláírással kapcsolatos egyéb tevékenységek végrehajtása lehetséges az aláíró hitelesítése előtt is.

Az intelligens kártya kisugárzása (FPT_EMSEC.1)
Az intelligens kártya, a tudomány jelenlegi szintje által meghatározott korlátok között, megakadályozza az aláírás-létrehozó adat (magánkulcs), valamint a hitelesítő adat (PIN kód) megismerését lehetővé tévő kisugárzódást[13].
Az intelligens kártya garantálja, hogy egyetlen felhasználó sem képes a külső interfészek kisugárzásából a magánkulcsot, illetve a PIN kódot megismerni.

A biztonságos állapot megőrzése hiba esetén (FPT_FLS.1)
Az intelligens kártya megőriz egy biztonságos állapotot, ha a következő típusú hibák lépnek fel:

- egy alsó korlátnál alacsonyabb áramerősség,
- egy felső korlátnál magasabb áramfeszültség,
- az órafrekvencia kilépése egy alulról és felülről is korlátozott tartományból,
- integritás hiba.

A fizikai támadások passzív észlelése (FPT_PHP.1)
Az intelligens kártya félreérthetetlen módon detektálja a biztonsági funkciók kompromittálódását okozható fizikai manipulálásokat.
Az intelligens kártya képes megállapítani, hogy a detektált fizikai manipulálás a biztonsági funkció elemeire, vagy az azt megalapozó eszközökre irányult.

A fizikai támadásokkal szembeni ellenálló képesség (FPT_PHP.3)
Az intelligens kártya ellenálló a mikrochip-re irányuló alábbi fizikai támadásokkal szemben:

- órafrekvencia,
- feszültség manipulálás,
- keresztülhatolás a védelmi rétegen,

olyan automatikus reagálással, ami megakadályozza a kártya biztonsági politikájának megsértését.

A biztonsági funkciók tesztelése (FPT_TST.1)
Az intelligens kártya a kezdeti rendszer indítás során, valamint érzékeny moduljai felhívásakor egy olyan teszt-sorozatot hajt végre, mely kimutatja, hogy biztonsági funkciói helyesen működnek.
Az intelligens kártya biztosítja, hogy az arra feljogosított felhasználók képesek legyenek a biztonsági funkció adatok sértetlenségének ellenőrzésére.
Az intelligens kártya biztosítja, hogy az arra feljogosított felhasználók képesek legyenek a kártya által tárolt végrehajtható kódok sértetlenségét ellenőrizni.

[13] Az intelligens kártyának meg kell akadályoznia az aláírás-létrehozó adat, illetve egyéb titkos adatok elleni olyan támadásokat, melyek az intelligens kártyán kívül megfigyelhető fizikai jelenségeken alapulnak. Ilyen megfigyelhető jelenségek lehetnek a kártya interfészeken, származhatnak a kártya külső működéséből, vagy kiválthatja egy támadó, aki megváltoztatja azt a fizikai környezetet, amely mellett a kártya működik. A mérhető fizikai jellemzők halmazát befolyásolja az a technológia, amelyet a kártya megvalósításakor alkalmaznak. A mérhető jellemzőkre példák az alábbiak: áramfelvétel, a belső állapotok közötti átmenetek időzítése, elektromágneses sugárzás a belső működés következtében, rádióhullámok vagy fény kibocsátása.
Az esetlegesen kisugárzásokat okozó technológiák heterogén természete miatt el kell végezni a tudomány jelenlegi szintjén álló olyan támadások felmérését, amelyek alkalmasak a kártya által alkalmazott technológiákhoz. Az ilyen támadásokra (nem kizárólagos) példák: az intelligens kártya elektromágneses sugárzásának kiértékelése, az egyszerű áramfelvétel vizsgálat (SPA), a differenciális áramfelvétel vizsgálat (DPA) és az időzítéssel kapcsolatos támadások.

Megbízható csatorna (FTP_ITC.1)

/A tanúsítvány-létrehozó alkalmazás, illetve az aláírás-létrehozó alkalmazás felé./

Az intelligens kártya biztonsági funkciói egy olyan kommunikációs csatornát biztosítanak a kártya és egy távoli megbízható IT termék között, mely logikailag különbözik a többi kommunikációs csatornától, egyúttal biztosítja végpontjainak garantált azonosítását és továbbított adatok illetéktelen felfedés és módosítás elleni védelmét.

A megbízható csatornán való kommunikációt a távoli megbízható IT termék is kezdeményezheti.

Az intelligens kártya ezen a biztonságos csatornán kezdeményez kommunikációt az alábbi esetekhez:

- aláírás-ellenőrző adat (nyilvános kulcs) kiadása (a tanúsítvány-létrehozó alkalmazás felé),
- aláírandó adat reprezentáns fogadása (az aláírás-létrehozó alkalmazástól).

Megbízható útvonal (FTP_TRP.1)

Az intelligens kártya biztonsági funkciói egy olyan kommunikációs útvonalat biztosítanak a kártya és a helyi felhasználók között, mely logikailag különbözik a többi kommunikációs útvonaltól, egyúttal biztosítja végpontjainak garantált azonosítását és a továbbított adatok illetéktelen felfedés és módosítás elleni védelmét.

A megbízható útvonalon való kommunikációt a helyi felhasználó kezdeményezheti.

Az intelligens kártya a kezdeti felhasználói hitelesítéshez megköveteli ennek a biztonságos útvonalnak a használatát.

5. Az SLE66CX322P mikrochip értékelési követelményei a Common Criteria szerint

Az alábbiakban áttekintjük annak a védelmi profilnak a legfontosabb elemeit (a környezetre vonatkozó állításokat, biztonsági célokat, követelményeket és funkciókat), melynek való megfelelőséget az SLE66CX322P mikrochip értékelését végző laboratórium[14] vizsgálta és igazolta.

5.1 A SLE66CX322P mikrochip biztonsági környezete

A mikrochip-nek az alábbi értékeket kell megvédenie:
A szabványos funkcionalitáshoz kapcsolódó elsődleges értékek:

1. a felhasználói adatok bizalmassága és sértetlensége,
2. az intelligens kártya beágyazott szoftverének bizalmassága és sértetlensége,
3. a mikrochip funkcióinak (beleértve a véletlenszám generátort is) sértetlensége, helyes működése,
4. a mikrochip által generált véletlen számok bizalmassága és sértetlensége.

Kiegészítő, másodlagos értékek[15]:

5. logikai tervezési adatok,
6. fizikai tervezési adatok,
7. a mikrochip-hez tartozó szoftver, inicializációs és elő-perszonalizációs adatok,
8. speciális fejlesztési segédeszközök,
9. a teszteléssel és a jellemzéssel kapcsolatos adatok,
10. a szoftver fejlesztést támogató anyagok,
11. fotómaszkok és a termék bármely formája[16].

5.1.1 A biztonságra irányuló veszélyek

Az alábbi 3 magas-szintű biztonsági probléma fogalmazható meg:

1. A felhasználói adatoknak és az intelligens kártya beágyazott szoftverének a manipulációja (mialatt ezeket végrehajtják/feldolgozzák, illetve a mikrochip memóriájában tárolják).
2. A felhasználói adatoknak és az intelligens kártya beágyazott szoftverének felfedése[17] (mialatt ezeket végrehajtják/feldolgozzák, illetve a mikrochip memóriájában tárolják).
3. A véletlen számok gyengesége.

[14] TÜV IT GmbH.
[15] Valamennyi másodlagos értéknek a bizalmasságát és a sértetlenségét kell védeni.
[16] A felhasználói adatok manipulációjának vagy felfedésének számos módja van:
(i) Egy támadó manipulálhatja az intelligens kártya beágyazott szoftverét vagy magát a mikrochip-et.
(ii) Egy támadó előidézheti a mikrochip hibás működését, vagy szabálytalanul használhatja a mikrochip által biztosított teszt lehetőségeket.
Az ilyen támadásokhoz általában terv információk megszerzése szükséges a chip-ről. Ezért a terv információk is védendő (másodlagos) értékek.
[17] Bár az intelligens kártya beágyazott szoftvere (amelyet általában ROM-ban tárolnak) sok esetben nem tartalmaz titkos adatot vagy algoritmust, mégis védeni kell a felfedéssel szemben, mert például a speciális kivitelezési részletek megismerése segítséget nyújthat a támadóknak. A legtöbb esetben a kritikus felhasználói adatokat EEPROM-ban tárolják.

A fenti 3 magas-szintű biztonsági problémát az alábbi veszélyek finomítják:

A működéssel járó információ kiszivárgás
Egy támadó kihasználhatja azokat az információkat, amelyek a mikrochip-ből kiszivárognak az intelligens kártya használata során, abból a célból, hogy bizalmas adatokat (felhasználói adatokat vagy biztonsági funkció adatokat) fedjen fel.
/Ehhez nem szükséges közvetlen érintkezés az intelligens kártya belső részeivel. Kiszivárgás történhet kisugárzás következtében, illetve az áramfelvétel, az I/O jellemzők, az órafrekvencia megváltozása, illetve a feldolgozási időszükséglet változásai által. Egy példa erre a differenciális áramellátás vizsgálat (DPA). Ez a kiszivárgás értelmezhető egy rejtett csatornán történő adásként is, bár az üzemelési paraméterek beméréséhez jobban kapcsolódik, amely származhat közvetlen (érintkezőn keresztüli) mérésekből, vagy pedig a kisugárzások méréséből./

Fizikai szondázás
Egy támadó fizikailag szondázhatja a mikrochip-et abból a célból, hogy:
- felhasználói adatokat fedjen fel,
- felfedje/rekonstruálja az intelligens kártya beágyazott szoftverét,
- kritikus üzemelési információkat fedjen fel, különös tekintettel a biztonsági funkciók adataira.

A fizikai szondázás közvetlen kölcsönhatást igényel az intelligens kártya integrált áramkörének belső részeivel. Olyan technikákat lehet felhasználni, amelyeket általában az IC hibavizsgálatoknál és IC visszafejtéseknél alkalmaznak. Mindenekelőtt a hardver biztonsági mechanizmusait és szerkezeti jellemzőit kell meghatározni. A szoftver tervek meghatározása, beleértve a felhasználói adatok kezelését is, ugyancsak előfeltétel lehet.

Hibás működés a környezeti túlterhelés miatt
Egy támadó a biztonsági funkciók vagy a beágyazott szoftver hibás működését válthatja ki környezeti túlterhelés alkalmazásával abból a célból, hogy:
- lebénítsa vagy módosítsa a mikrochip biztonsági jellemzőit vagy funkcióit,
- lebénítsa vagy módosítsa az intelligens kártya beágyazott szoftverének biztonsági funkcióit.

Ez elérhető azáltal, hogy az intelligens kártyát nem a normál üzemelési körülmények mellett működtetik. A támadás kiaknázásához a támadónak információkra van szüksége a funkcionális működésről is.

Fizikai manipuláció
Egy támadó fizikailag módosíthatja az intelligens kártyát abból a célból, hogy:
- módosítsa a mikrochip biztonsági sajátosságait vagy funkcióit,
- módosítsa az intelligens kártya beágyazott szoftverének biztonsági funkcióit,
- felhasználói adatokat módosítson.

A módosítás elérhető olyan technikák felhasználásával, amelyeket általában az IC hibavizsgálatoknál és IC visszafejtési kísérleteknél alkalmaznak. A módosítás a biztonsági funkciók lebénítását eredményezhetik. Mindezek előtt a hardver biztonsági mechanizmusait és szerkezeti jellemzőit kell meghatározni. A szoftver szerkezet értelmezése, beleértve a felhasználói adatok kezelését is, ugyancsak előfeltétel lehet. Az áramkörökön vagy adatokon végrehajtott változtatások lehetnek véglegesek vagy ideiglenesek. A „Hibás működés a környezeti túlterhelés miatt” veszéllyel ellentétben itt a támadónak jelentős ismereteket kell szereznie a mikrochip belső szerkezetéről is.

Mesterségesen előidézett információ kiszivárgás
Egy támadó kiaknázhatja azokat az információkat, amelyek a mikrochip-ből kiszivárognak az intelligens kártya használata során, abból a célból, hogy bizalmas adatokat (felhasználó adatokat vagy biztonsági funkció adatokat) fedjen fel, akkor is, ha az információ kiszivárgás nem a működés velejárója, hanem a támadó váltja ki.
Ez a veszély azokra a támadásokra vonatkozik, amelyeknél a "Hibás működés a környezeti túlterhelés miatt" és/vagy a "Fizikai manipuláció" veszélyeknél ismertetett módszereket alkalmazzák, hogy kiszivárgásokat váltsanak ki olyan kijelzésekből, amelyek normál körülmények között nem tartalmaznak érdemi titkos információt.

A funkcionalitás szabálytalan használata
Egy támadó használhatja a mikrochip azon funkcióit, amelyeket feltehetően nem használnak a mikrochip leszállítása után, abból a célból, hogy:

- felhasználói adatokat fedjen fel vagy manipuláljon,
- a mikrochip vagy egy beágyazott szoftver biztonsági tulajdonságait vagy funkcióit manipulálja (felderítse, kikerülje, lebénítsa vagy megváltoztassa),
- egy támadást tegyen lehetővé.

A véletlenszámok gyengesége
Egy támadó információt valószínűsíthet vagy nyerhet a mikrochip által előállított véletlenszámokról, például a rendelkezésre bocsátott véletlenszámok nem megfelelő entrópiája következtében.
Egy támadó információt gyűjthet az előállított véletlenszámokról, ami azért okozhat problémát, mert ezeket fel lehet használni kriptográfiai kulcsok előállítására is.
A véletlenszámok gyengesége esetén számítani lehet arra, hogy a támadó kihasználja a mikrochip által előállított véletlenszámok statisztikai tulajdonságait anélkül, hogy speciális ismeretei lennének a mikrochip véletlenszám generátoráról. A működési hiba vagy az idő előtti öregedés figyelembe vétele szintén segítséget nyújthat a véletlenszámokra vonatkozó információk megszerzésében.

5.1.2 Érvényre juttatandó biztonsági szabályok

Védelem a mikrochip fejlesztése és gyártása során
A mikrochip gyártójának biztosítania kell, hogy az intelligens kártya integrált áramkörének fejlesztése és gyártása biztonságos abban az értelemben, hogy sem továbbítanak véletlenül a mikrochip üzemeltetési fázisa számára. Például a terv információk és teszt adatok bizalmasságát és sértetlenségét garantálni kell; a mintákhoz, fejlesztési eszközökhöz és egyéb anyagokhoz való hozzáférést csak a feljogosított személyekre kell korlátozni; a selejtet meg kell semmisíteni stb. Ez nemcsak a mikrochip-re vonatkozik, hanem minden információra és anyagra, amelyet az intelligens kártya beágyazott szoftverének fejlesztőjével cserélnek, így elsősorban magára az intelligens kártya beágyazott szoftverére.
Ki kell alakítani a mikrochip-ek pontos azonosítását. Minden egyes mikrochip példánynak egyedi azonosítót kell kapnia.

Kiegészítő speciális biztonsági funkcionalitás
A mikrochip a beágyazott szoftver számára az alábbi kiegészítő biztonsági funkcionalitást biztosítja:

- terület alapú memória hozzáférés ellenőrzés,
- DES, triple DES, RSA.

5.2 A SLE66CX322P mikrochip biztonsági céljai

Az alábbi 3 magas-szintű biztonsági célkitűzés fogalmazható meg:

1. a felhasználói adatok és az intelligens kártya beágyazott szoftver sértetlenségének megőrzése (amikor ezeket végrehajtják/feldolgozzák, és amikor ezeket a mikrochip memóriájában tárolják),
2. a felhasználói adatok és az intelligens kártya beágyazott szoftver bizalmasságának[18] megőrzése (amikor ezeket végrehajtják/feldolgozzák, és amikor ezeket a mikrochip memóriájában tárolják).
3. véletlenszámok biztosítása.

A fenti 3 magas-szintű biztonsági célkitűzést az alábbi biztonsági célok finomítják:

A működéssel járó információ kiszivárgás elleni védelem
A mikrochip-nek védelmet kell biztosítania az intelligens kártya IC-ben tárolt és/vagy feldolgozott bizalmas adatok (felhasználói adatok és biztonsági funkció adatok) azon felfedései ellen, amelyet azzal érnek el, hogy:

- mérik és elemzik (például áram, óra vagy I/O vezetékeken) a jelek alakját és amplitúdóját,
- mérik és elemzik azt az időközt, amely eltelik a (például áram, óra vagy I/O vezetékeken) mért események között[19].

A fizikai szondázás elleni védelem
A mikrochip-nek védelmet kell nyújtania a felhasználói adatok felfedése, az intelligens kártya beágyazott szoftverének felfedése/rekonstruálása, illetve az egyéb kritikus üzemeltetési információk felfedése ellen. Ez magában foglalja a védelmet a következők ellen:

- galvanikus érintkezőkön keresztüli mérések, amelyek közvetlen fizikai szondázások a chipek felületén, de nem a kivezetéseken (szabványos feszültség és árammérő eszközök használatával),
- nem galvanikus, hanem más típusú fizikai, töltések közötti kölcsönhatásokat felhasználó mérések (amelyeket a szilárd-test fizikai kutatásoknál és az IC hiba vizsgálatoknál alkalmazott eszközökkel végeznek),

mely mérésekhez hozzájárul egy megelőző visszafejtés a szerkezet és annak tulajdonságainak, funkcióinak megértése érdekében[20].

[18] Bár az intelligens kártya beágyazott szoftvere (amelyet általában ROM-ban tárolnak) sok esetben nem tartalmaz titkos adatot vagy algoritmust, mégis védeni kell a felfedéssel szemben, mert például a speciális kivitelezési részletek megismerése segítséget nyújthat a támadóknak. A legtöbb esetben a kritikus felhasználói adatokat EEPROM-ban tárolják.
[19] Ez a biztonsági cél olyan mérésekre vonatkozik, amelyeket egy összetett jelfeldolgozás egészít ki, míg a „A fizikai szondázás elleni védelem" biztonsági cél azokról a közvetlen mérésekről szól, amelyeket a chip felszínén található elemeken végeznek.
[20] A mikrochip-et úgy kell tervezni és előállítani, hogy a biztonságot veszélyeztető fizikai támadásokhoz is felhasználható részletes szerkezeti és egyéb információt csak bonyolult berendezések felhasználásával, magas-szintű ismeretek, jártasságok birtokában, és jelentős időbefektetés árán lehessen szerezni.

Védelem a hibás működés ellen
A mikrochip-nek biztosítania kell a helyes működést.
A mikrochip-nek blokkolnia kell működését, ha a körülmények a normál üzemfeltételeken kívül esnek, melyek mellett a megbízható és biztonságos működés nem lett bizonyítva vagy tesztelve. Ez a hibák megelőzése érdekében szükséges. A környezeti feltételek magukban foglalhatnak áramellátást, órafrekvenciát, hőmérsékletet vagy külső energia mezőket[21].

A fizikai manipuláció elleni védelem
A mikrochip-nek védelmet kell biztosítania a chip (beleértve szoftverét és biztonsági funkció adatait), az intelligens kártya beágyazott szoftvere, valamint a felhasználói adatok manipulációja ellen. Ez magában foglalja következők elleni védelmet:
- visszafejtés (a szerkezet és annak tulajdonságainak és funkcióinak megértése),
- a hardver és bármely adat manipulációja,
- a memória tartalmak (felhasználói adatok) irányított manipulációja[22].

Védelem a mesterségesen előidézett információ kiszivárgás ellen
Az intelligens kártyát védeni kell a kártyán feldolgozott bizalmas adatok (felhasználói adatok vagy biztonsági funkció adatok) felfedése ellen („A működéssel járó információ kiszivárgás elleni védelem” biztonsági célnál ismertetett módszerek felhasználásával), még akkor is, ha az információ kiszivárgás nem a működés velejárója, hanem a támadó idézi elő azzal, hogy:
- hibás működést kényszerít ki (lásd a “Védelem a környezeti túlterhelés miatti hibás működés ellen” biztonsági célt) és/vagy
- fizikai manipulációt valósít meg (lásd a “Védelem a fizikai manipuláció ellen” biztonsági célt).

Ellenkező esetben azok a jelek, amelyek normál körülmények között nem tartalmaznak titkokról érdemi információt, információs csatornává válhatnak egy kiszivárgásos támadás számára.

Védelem a funkcionalitás szabálytalan használata ellen
A mikrochip-nek blokkolni kell azon funkcióit, melyeket a chip leszállítása után nem szabad használni, mert szabálytalanul fel lehetne használni arra, hogy:
- kritikus felhasználói adatokat fedjenek fel,
- az intelligens kártya beágyazott szoftverének kritikus felhasználói adatait manipulálják,
- az intelligens kártya szoftveresen kódolt beágyazott szoftverét manipulálják,
- a mikrochip biztonsági tulajdonságait vagy funkcióit megkerüljék, lebénítsák, megváltoztassák vagy felderítsék.

[21] A mikrochip hibás működését elő is lehet idézni a felületén található elemekkel való közvetlen kölcsönhatással. Ezt manipulációnak tekintjük (lásd „A fizikai manipuláció elleni védelem” biztonsági célt), feltéve, hogy ehhez részletes ismeretek szükségesek a mikrochip belső szerkezetéről, és a támadást irányított módon hajtják végre.
[22] A mikrochip-et úgy kell tervezni és előállítani, hogy a biztonságot veszélyeztető fizikai támadásokhoz is felhasználható részletes szerkezeti és egyéb információt csak bonyolult berendezések felhasználásával, magas-szintű ismeretek, jártasságok birtokában, és jelentős időbefektetés árán lehessen szerezni.

Mikrochip azonosítás
A mikrochip-nek eszközt kell nyújtania az inicializációs és elő-perszonalizációs adatok nem-felejtő memóriáiban való tárolására. Az inicializációs adatok (vagy ezek részei) a mikrochip azonosítására szolgálnak.

Véletlenszámok
A mikrochip-nek biztosítania kell a véletlenszám generálás kriptográfiai minőségét. A véletlen számoknak nem szabad például megjósolhatóknak lenniük, és megfelelő entrópiával kell rendelkezniük.
A mikrochip-nek biztosítania kell, hogy egy támadó számára semmilyen információ ne álljon rendelkezésre az előállított véletlenszámokról, hiszen ezeket például kriptográfiai kulcsok generálására is fel lehet használni.

Kiegészítő speciális biztonsági funkcionalitás
A mikrochip a beágyazott szoftver számára az alábbi kiegészítő biztonsági funkcionalitást biztosítja:

- terület alapú memória hozzáférés ellenőrzés,
- DES,
- triple DES,
- RSA.

5.3 A SLE66CX322P mikrochip funkcionális biztonsági követelményei

5.3.1 A környezeti túlterhelés miatti hibás működést megakadályozó követelmények

Korlátozott hibatűrés (FRU_FLT.2)
A biztonsági funkciók biztosítják a mikrochip helyes működését olyan üzemelési feltételek között, melyet normálisnak ítélnek (pontosabban nem észlelnek hibának a "Biztonságos állapot megőrzése hiba esetén"-nek megfelelően)[23].

A biztonságos állapot megőrzése hiba esetén (FPT_FLS.1)
A biztonsági funkciók megőriznek egy biztonságos állapotot, amikor olyan üzemelési feltételek lépnek fel, melyeket nem tolerál a "Korlátozott hibatűrés" követelmény, s mely esetekben ennélfogva hibás működés léphet fel[24].

Tartomány elkülönítés a biztonsági funkciók számára (FPT_SEP.1)
A biztonsági funkciók egy külön biztonsági tartományt tartanak fenn saját maguk végrehajtásához, mely megvédi ezen funkciókat a nem megbízható szoftverek kölcsönhatásától, illetve beavatkozásától[25].
A biztonsági funkciók szétválasztják a hatókörükbe tartozó szoftverek biztonsági tartományait.

5.3.2 Az információ kiszivárgást megakadályozó követelmények

A felhasználói adatok alapszintű belső átvitel védelme (FDP_ITT.1)
A mikrochip biztonsági funkciói megakadályozzák a felhasználói adatok felfedését a mikrochip fizikailag elkülönített részei (különböző memóriák, CPU és egyéb funkcionális egységek, pl. kriptográfiai co-processzor) közötti átvitel során.

A biztonsági funkciókhoz tartozó adatok alapszintű belső átvitel védelme (FPT_ITT.1)
A mikrochip biztonsági funkciói megakadályozzák saját adataik felfedését a mikrochip fizikailag elkülönített részei (különböző memóriák, CPU és egyéb funkcionális egységek, pl. kriptográfiai co-processzor) közötti átvitel során[26].

Részleges információ áramlás ellenőrzés (FDP_IFC.1)
A mikrochip biztonsági funkciói érvényre juttatják az „Adatfedolgozási politikát" minden bizalmas adatra vonatkozóan, amikor azokat a mikrochip vagy az intelligens kártya beágyazott szoftvere feldolgozza, illetve továbbítja.

[23] Ezek konkrét maghatározása csak a biztonsági funkciók nem nyilvános leírásában található meg.
[24] A konkrét hibatípusok listája csak a biztonsági funkciók nem nyilvános leírásában szerepelnek.
[25] A mikrochip azon részeit, melyek a "Korlátozott hibatűrés" és a "Biztonságos állapot megőrzése hiba esetén" követelmények teljesítését biztosítják, meg kell védeni az intelligens kártya beágyazott szoftverének zavaró hatásaival szemben.
[26] Ez a követelmény azonos a fenti FDP_ITT.1-gyel, csak biztonsági funkció adatokra vonatkozik felhasználói adatok helyett. Ezért úgy kell értelmezni, hogy mindkettő ugyanarra az Adatfeldolgozási politikára vonatkozik, amely az FDP_IFC.1 alatt van definiálva.

5.3.3 A fizikai manipulációt és szondázást megakadályozó követelmény

A fizikai támadásnak való ellenállás (FPT_PHP.3)
A mikrochip biztonsági funkciói ellenállnak a fizikai manipulációknak és fizikai szondázásnak[27] egy automatikus reagálás[28] útján úgy, hogy a mikrochip biztonsági politikája ne sérüljön[29].

5.3.4 A funkcionalitás szabálytalan használatát megakadályozó követelmények

Korlátozott képességek (FMT_LIM.1)
A mikrochip-et úgy tervezték, hogy képességei korlátozva legyenek[30], s így a "Korlátozott rendelkezésre állás"-sal együtt érvényre juttassa a következő politikát: *a mikrochip felhasználókhoz való leszállítása után a tesztelési lehetőségek felhasználása ne tegye lehetővé a felhasználói adatok felfedését és manipulációját, a biztonsági funkció adatok felfedését és manipulációját, a szoftver rekonstruálását, valamint semmilyen olyan lényeges információ megszerzését a biztonsági funkciók szerkezetéről, amely egyéb támadásokat tenne lehetővé.*

Korlátozott rendelkezésre állás (FMT_LIM.2)
A mikrochip-et úgy tervezték, hogy rendelkezésre állása korlátozva legyen[31], s így a "Korlátozott képességek"-kel együtt érvényre juttassa a következő politikát: *a mikrochip felhasználókhoz való leszállítása után a tesztelési lehetőségek felhasználása ne tegye lehetővé a felhasználói adatok felfedését és manipulációját, a biztonsági funkció adatok felfedését és manipulációját, a szoftver rekonstruálását, valamint semmilyen olyan lényeges információ megszerzését a biztonsági funkciók szerkezetéről, amely egyéb támadásokat tenne lehetővé.*

[27] Nem tárgya jelen jelentésnek, hogy konkrétan mely biztonsági funkciók, s milyen fizikai támadási forgatókönyvekre készültek fel.
[28] A mikrochip nincs mindig áramforrással ellátva, és ennél fogva nem képes észlelni, arra reagálni vagy jelezni, hogy manipuláció, szondázás érte. Szerkezeti jellemzői azonban megnehezítik a visszafejtést és manipulációkat. Ez "automatikus válasz"-nak tekinthető a manipulációra, szondázásra. A mikrochip emellett képes lehet aktívan is reagálni egy lehetséges fizikai támadásra.
[29] A mikrochip-nek megfelelő lépéseket kell végrehajtania abból a célból, hogy folyamatosan elhárítsa a fizikai manipulációkat és a fizikai szondázást. Az ilyen támadások (különösen a manipulációk) természete miatt a mikrochip semmi esetre sem tudja detektálni a támadásokat minden elemükre kiterjedően. Ezért egy állandó védelem szükséges ezekkel a támadásokkal szemben annak biztosítására, hogy a biztonsági politikát soha ne lehessen megsérteni. Így az "automatikus reagálás" itt a következőket jelenti
(i) fel van tételezve, hogy bármely időpontban felléphet egy támadás,
(ii) ellenintézkedések vannak biztosítva bármely időpontban.
[30] Bizonyos életciklus szakaszokban, pl. a gyártást követő részletes tesztelést követően.
[31] Például a rendelkezésre állás felhasználói hitelesítéshez (jelszavak) kötésével, vagy a későbbi életciklus fázisokra a rendelkezésre állás megszüntetésével (eltávolítás vagy lebénítás "kiégetés"-sel). A részletes technikai specifikáció szükségtelenül tárna fel részleteket (egy potenciális támadó számára is), így a követelmények meghatározásának hatókörén kívül esik.

5.3.5 Az azonosítást lehetővé tévő követelmény

Napló tárolás (FAU_SAS.1)
A biztonsági funkciók a mikrochip szállítása előtt a tesztelő személyzet számára biztosítják annak lehetőségét, hogy inicializációs és elő-perszonalizációs adatokat, illetve az intelligens kártya beágyazott szoftveréhez kiegészítéseket tároljanak a napló bejegyzésekben.

5.3.6 A véletlenszámok kriptográfiai minőségét biztosító követelmény

A véletlenszámok minőségi mértéke (FCS_RND.1)
A mikrochip biztonsági funkciói egy olyan mechanizmust biztosítanak a véletlenszámok generálásához, mely kielégít egy meghatározott minőségi mértéket[32].

5.3.7 Kiegészítő biztonsági funkcionális követelmények

Az alábbi követelményeket a megfelelő védelmi profil elvárásain túl teljesíti a mikrochip.

A mikrochip részleges biztonsági tesztelése (FPT_TST.2)
A mikrochip a kezdeti rendszer indítás során, valamint egy felhatalmazott felhasználó kérésére egy olyan önteszt-sorozatot hajt végre, mely kimutatja, hogy 1.-es, 2-es, 5-ös és 6-os biztonsági funkciói helyesen működnek[33].

Részleges hozzáférés ellenőrzés (FDP_ACC.1)
A mikrochip képes a „Memória hozzáférés ellenőrzés politika”[34] érvényre juttatására:

- valamennyi szoftverre,
- valamennyi adatra (beleértve a memóriában tárolt kódokat is), és
- valamennyi a „Memória hozzáférés ellenőrzés politika” által meghatározott műveletre.

Biztonsági jellemzőkön alapuló hozzáférés ellenőrzés (FDP_ACF.1)
A mikrochip képes a „Memória hozzáférés ellenőrzés politika érvényre juttatására az alább felsorolt memória területekre alapulóan:

- memória terület, ahonnan egy szoftver elindítható, és/vagy
- memória terület, ahová a hozzáférés megadható, és/vagy
- a végrehajtható művelet

A mikrochip képes a következő szabályok érvényre juttatására, annak meghatározása érdekében, hogy egy adott szoftver, egy adott adaton, egy adott műveletet végrehajthat-e: a megfelelő „engedélyt vezérlő információ” elemzése a hozzáférés előtt, alatt vagy után, oly módon, hogy a visszautasított hozzáféréseket a műveletet végrehajtani próbáló ne használhassa.

[32] Nem tárgya jelen jelentésnek, hogy konkrétan milyen ez a minőségi mérték.
[33] Az érintett biztonsági mechanizmusok leírását a (nem publikált) funkció specifikáció tartalmazza.
[34] Memória hozzáférés ellenőrzés politika:
A mikrochip képes ellenőrizni az egyes memória területein lévő szoftverek által az „olvasás”, „írás”, „törlés” és „végrehajtás” műveletek elérhetőségét az adatokon, a memória területeken tárolt kódokat is beleértve.
A mikrochip egy speciális jellemzővel ellátott szoftverre korlátozza az alkalmazandó szabályok meghatározását, módosítását, és végleges elfogadását.

Statikus jellemző inicializálás (FMT_MSA.3)
A mikrochip képes a „Memória hozzáférés ellenőrzés politika” érvényre juttatása érdekében a biztonsági jellemzők számára „jól meghatározott” alapértékeket biztosítani.
A mikrochip lehetővé teszi valamennyi szoftver részére, hogy a „Memória hozzáférés ellenőrzés politika” érvényre juttatásával a szükséges hozzáféréseket végrehajthassa.

A biztonsági jellemzők kezelése (FMT_MSA.1)
A mikrochip a „Memória hozzáférés ellenőrzés politika” érvényre juttatása érdekében egy speciális jellemzővel ellátott szoftverre korlátozza annak képességét, hogy az „engedélyt vezérlő információ” biztonsági jellemzőket módosítsa, törölje, vagy alapértékét felülírja.

Kriptográfiai eljárás (FCS_COP.1)
A mikrochip képes az alábbi kriptográfiai algoritmusok szabványos végrehajtására:

- 56 bites DES titkosító/dekódoló algoritmus,
- 112 bites triple DES titkosító/dekódoló algoritmus,
- RSA titkosító/dekódoló algoritmus az alábbi kulcsméretek mellett: 512, 520, 528, …, 1016, 1024 bit, illetve 1280 és 2048 bit.

Kriptográfiai kulcs generálás (FCS_CKM.1)
A mikrochip képes RSA kulcspár generálása az alábbi kulcsméretek mellett: 512, 520, 528, …, 1016, 1024 bit, illetve 1280 és 2048 bit.

6. A JAVACARD 32K CRISTAL követelményeknek való megfelelését ellenőrző független értékelés garancia szintje

Az intelligens kártya egészére vonatkozó, fejlesztőktől független ellenőrző vizsgálat garancia szintje az ISO 14508 /Common Criteria/ emelt **EAL 4**-es /módszeresen tervezett, vizsgált és átnézett rendszer/ volt.

Az alábbi táblázat összefoglalja az értékelés garanciaosztályait és garanciaösszetevőit az értékelésnél alkalmazott emelt EAL 4-es szinten.

Garanciaosztályok	**Garanciaösszetevők a JavaCard 32K CRISTAL intelligens kártya értékelésénél /EAL4+/**
A konfiguráció menedzselése	ACM_AUT.1 A konfiguráció menedzselés részleges automatizálása
	ACM_CAP.4 A szoftver telepítést támogató és elfogadó eljárások
	ACM_SCP.2 A problémakövető konfiguráció menedzselés lefedettsége
Kiszállítás és üzemeltetés	ADO_DEL.2 A módosítások észlelése
	ADO_IGS.1 A hardver-telepítés, szoftver-telepítés, beindítás eljárásai
Fejlesztés	ADV_FSP.2 Teljesen meghatározott külső interfészek
	ADV_HLD.2 Felső-szintű tervezést érvényesítő biztonság
	ADV_IMP.2 Az értékelés tárgya biztonsági funkcióinak kivitelezése /csak EAL5-től megkövetelt/
	ADV_LLD.1 Az alsó-szintű tervezés leírása
	ADV_RCR.1 A kölcsönös megfelelés informális szemléltetése
	ADV_SPM.1 Az értékelés tárgya biztonsági szabályzatának informális modellje
Útmutató dokumentumok	AGD_ADM.1 Az adminisztrátori útmutató
	AGD_USR.1 A felhasználói útmutató
Az életciklus támogatása	**ALC_DVS.2 A biztonsági intézkedések elégségessége /csak EAL6-tól megkövetelt /**
	ALC_LCD.1 A fejlesztő által meghatározott életciklus-modell
	ALC_TAT.1 A jól meghatározott fejlesztőeszközök
Tesztelés	ATE_COV.2 A lefedettség elemzése
	ATE_DPT.1 A felső-szintű terv(ezés) vizsgálata
	ATE_FUN.1 Funkcionális tesztelés
	ATE_IND.2 Független tesztelés – mintán
A sebezhetőség felmérése	**AVA_MSU.3 A nem biztonságos állapotok elemzése és vizsgálata /csak EAL6-tól megkövetelt /**
	AVA_SOF.1 Az értékelés tárgya biztonsági funkciónak erősségértékelése
	AVA_VLA.4 Keményen ellentálló /csak EAL6-tól megkövetelt /

A fenti értékelés felhasználta az intelligens kártya mikrochip-jének korábbi értékelési és tanúsítási eredményeit. Ez még magasabb, emelt EAL 5-ös /félformálisan tervezett és vizsgált rendszer/ értékelés garancia szintű volt.
A mikrochip-re azért vártak el magasabb szintű független garanciákat (mint az intelligens kártya egészére), mert a biztonsági szempontból legkritikusabb tevékenységek ezen eszközben valósulnak meg (köztük a véletlenszámok generálása, az erre épülő kulcspár előállítása, a titkos és magánkulcsok tárolása, a legtöbb kriptográfiai funkció és mechanizmus megvalósítása), s ezért úgy tervezték, hogy ellenálljon még az erős támadási potenciállal rendelkező támadóknak is, még védtelen környezetben is.

Ez az igen magas, a fejlesztőktől függetlenül garantált biztonság már formális (félformális) bizonyítékokat is szolgáltat a termék sebezhetőségének felméréséhez, illetve biztosítja az értékelők számára a termékkel kapcsolatos valamennyi fejlesztői információhoz való hozzáférést (beleértve az alacsony szintű terveket és forráskódokat is).

Az alábbi garanciaösszetevőket tartalmazza tételesen:

Garanciaosztályok	Garanciaösszetevők a JavaCard 32K CRISTAL intelligens kártya értékelésénél /EAL5+/
A konfiguráció menedzselése	ACM_AUT.1 A konfiguráció menedzselés részleges automatizálása
	ACM_CAP.4 A szoftver-telepítést támogató és elfogadó eljárások
	ACM_SCP.3 A fejlesztőeszközök konfiguráció menedzselés lefedettsége
Kiszállítás és üzemeltetés	ADO_DEL.2 A módosítások észlelése
	ADO_IGS.1 Hardver-telepítés, szoftver-telepítés, beindítás eljárásai
Fejlesztés	ADV_FSP.3 Félformális funkcionális előírás
	ADV_HLD.3 A félformális felső-szintű tervezés
	ADV_IMP.2 Az értékelés tárgya biztonsági funkcióinak kivitelezése
	ADV_INT.1 Modularitás
	ADV_LLD.1 Az alsó-szintű tervezés leírása
	ADV_RCR.2 A kölcsönös megfelelés félformális szemléltetése
	ADV_SPM.3 Az értékelés tárgya biztonsági szabályzatának formális modellje
Útmutató dokumentumok	AGD_ADM.1 Az adminisztrátori útmutató
	AGD_USR.1 A használói útmutató
Az életciklus támogatása	**ALC_DVS.2 A biztonsági intézkedések elégségessége /csak EAL6-tól megkövetelt /**
	ALC_LCD.2 A szabványosított életciklus-modell
	ALC_TAT.2 Megfelelés a kivitelezési szabványoknak
Tesztelés	ATE_COV.2 A lefedettség elemzése
	ATE_DPT.2 Az alsó-szintű terv(ezés) vizsgálata
	ATE_FUN.1 Funkcionális tesztelés
	ATE_IND.2 Független tesztelés - mintán
A sebezhetőség felmérése	AVA_CCA.1 A rejtett csatorna elemzése
	AVA_MSU.3 A nem biztonságos állapotok elemzése és vizsgálata /csak EAL6-tól megkövetelt /
	AVA_SOF.1 A értékelés tárgya biztonsági funkcióinak erősségértékelése
	AVA_VLA.4 Keményen ellentálló /csak EAL6-tól megkövetelt /

7. A Tanúsítási jelentés eredménye, érvényességi feltételei

7.1 A Tanúsítási jelentés eredménye

A JAVACARD 32K CRISTAL intelligens kártya
/SchumbergerSema, France,
Infineon Technologies AG, Germany/

tanúsítás tárgyát képező verziója

/mikrochip:	SLE66CX322P (GC A23 verzió),
operációs rendszer:	GEOS (SC_V3.0.0 verzió),
aláírás-létrehozó alkalmazás:	CRISTAL (AC_V1.0.0 verzió)/

a tanúsítás érvényességi feltételeinek[35] együttes teljesülése esetén

ALKALMAS

minősített aláírások létrehozására,
mint
3-as típusú biztonságos aláírás-létrehozó eszköz.

[35] Lásd a 7.2 "Az eredmények érvényességi feltételei" alfejezet 1.-7. feltételeit.

7.2 Az eredmények érvényességi feltételei

A JavaCard 32K CRISTAL intelligens kártya adott alkalmazását úgy fejlesztették, hogy (a sokkal általánosabb kriptográfiai funkcionalitást is támogató mikrochip-je, illetve több felhasználói alkalmazás futtatására alkalmas platformja szolgáltatásait kihasználva) pontosan megfeleljen a viszonyítási alapként tekintett védelmi profil követelményeinek.
Ez jelentősen leegyszerűsíti a feltételek meghatározását. Nem szükséges például külön elemezni és áttekinteni a mikrochip tanúsítványának érvényességi feltételeit, hiszen azt a későbbi értékelő/tanúsító szervezetek figyelembe vették (teljesítettnek nyilvánították, vagy saját feltételeik közé is beépítették).

Az alábbiakban összefoglaljuk azokat a feltételeket, melyek **együttes** betartása feltétele a tanúsítvány érvényességének.

7.2.1 A tanúsítás viszonyítási alapját képező védelmi profilból adódó érvényességi feltételek

1. **Az adminisztrátor kövesse az adminisztrátori útmutatót**
   Az adminisztrátornak be kell tartania a JavaCard 32K CRISTAL intelligens kártya inicializálásához, megszemélyesítéséhez és adminisztrálásához biztosított adminisztrátori útmutató[36] valamennyi előírását[37].

2. **Megbízható tanúsítvány-létrehozó alkalmazást kell használni**
   Csak minősített hitelesítés-szolgáltató által működtetett tanúsítvány-létrehozó alkalmazást szabad használni a nyilvános kulcs tanúsítványba foglalásához. Az ilyen tanúsítvány kellő biztonsággal megvédi a minősített tanúsítványban szereplő felhasználói név és aláírás-ellenőrző adat hitelességét a minősített hitelesítés-szolgáltató aláírásával.

3. **Az aláíró kövesse a felhasználói útmutató előírásait**
   Az aláírónak követnie kell a JavaCard 32K CRISTAL intelligens kártya által biztosított felhasználói útmutató[38] valamennyi előírását[39].
   /Különösen fontos az alábbiak betartása:
   A felhasználónak (aláírónak) titokban kell tartania saját PIN kódját./

4. **Megbízható aláírás-létrehozó alkalmazást használjanak**
   Az aláíró csak megbízható aláírás-létrehozó alkalmazást használhat.
   Az aláírás-létrehozó alkalmazás állítja elő és küldi át az aláíró által alá írni kívánt adatokat (vagy annak reprezentánsát, részlegesen vagy teljesen lenyomatolt képét) a JavaCard 32K CRISTAL intelligens kártyára, az aláíráshoz megfelelő formában.

[36] Administration manual: RUBIS (MRD06GI003072 v.1.3)
[37] Az alábbiakban azért nem részletezzük ezen előírásokat, mert egy nem nyilvános dokumentum tartalmazza azokat /Administration manual: RUBIS/
[38] User manual: RUBIS (MRD06GI003073 v.1.4)
[39] Az alábbiakban azért nem részletezzük ezen előírásokat, mert egy nem nyilvános dokumentum tartalmazza azokat /User manual: RUBIS/

7.2.2 A hazai jogszabályokból adódó érvényességi feltételek

Nincsenek járulékos követelmények.

Ennek egyik oka, hogy a JavaCard 32K CRISTAL intelligens kártya minden kategóriában támogat egy a 2/2002. (IV. 26.) MeHVM irányelv l. számú mellékletében felsorolt „elfogadott kriptográfiai algoritmust”:

- aláíró algoritmus: **RSA (1024 bites kulcsmérettel)**
- kulcs létrehozási algoritmus: **valódi véletlen**
- feltöltő módszer: **PKCS #1 (emsa-pkcs-v1_5)**
- lenyomat- (hash) függvény: **SHA-1**

A másik ok az, hogy a JavaCard 32K CRISTAL intelligens kártya (pontosabban annak CRISTAL alkalmazása) csak a fenti elfogadott kriptográfiai algoritmusok meghívását teszi lehetővé, nincs szükség tehát a kiválasztható sokféle algoritmus közül megtiltani néhány nem elfogadott algoritmussal való felhívását.

7.2.3 Egyéb érvényességi feltételek

5. A megbízható csatorna kialakításában közreműködő kulcsokat a host oldalon is védeni kell

Az intelligens kártya és a host oldal közötti kölcsönös hitelesítés egy közös titok ismeretén alapul. Ezt a titkot (statikus kulcsot) a host oldalon is kellő biztonsággal meg kell védeni az illetéktelen felfedés ellen.

6. Megfelelő hosszú PIN kódot használjanak

A JavaCard 32K CRISTAL intelligens kártya **legfeljebb 8 hosszú PIN kód**ot támogat, megadott értékét bájtos alakban kezeli. 3 egymást követő sikertelen hitelesítési kísérlet (téves PIN kód megadás) után a kártya alkalmazás blokkolja valamennyi felhasználói funkcióját. Ahhoz, hogy magas fokú védelem legyen biztosítva **minimálisan 4 jegyű, véletlenszerű PIN kódot kell használni**. A szakirodalom szerint erősen ajánlott a véletlen próbálgatáson alapuló illetéktelen hitelesítési kísérletek sikere ellen annak valószínűségét az 1/1000000-od valószínűség közelébe leszorítani, mely a PIN kód jelkészletétől függő módon az alábbi alsó hosszúság korlátot jelenti a PIN kódra: számjegyek alkalmazása esetén: 6; hexadecimális karakterek alkalmazása esetén: 5; általános klaviatúra használata esetén (kis és nagy betűk, számjegyek): 4 karakter.

7. Pontosan a tanúsított verziót használják

A tanúsítvány csak a jelenlegi hardver és förmver verzióra érvényes[40] /mikrochip: SLE66CX322P (GC A23 verzió), operációs rendszer: GEOS (SC_V3.0.0 verzió), aláírás-létrehozó alkalmazás: CRISTAL (AC_V1.0.0 verzió)/.

[40] A tanúsítás érvényes marad, ha a CRISTAL alkalmazás mellé más alkalmazásokat töltenek az intelligens kártyára.

8. A tanúsításhoz figyelembe vett dokumentumok

8.1 Termékmegfelelőségi követelményeket tartalmazó dokumentumok

Az elektronikus aláírásról szóló 2001. évi XXXV. törvény

2/2002. (IV. 26.) MeHVM irányelv a minősített elektronikus aláírással kapcsolatos szolgáltatásokra és ezek szolgáltatóira vonatkozó biztonsági követelményekről

CEN/ISSS ESign Workshop – Expert Group F: Protection Profile – Secure Signature-Creation Device Type 3, version: 1.05, EAL4+

Smartcard IC Platform Protection Profile (BSI-PP-0002)

8.2 A tanúsítási jelentéshez figyelembe vett egyéb dokumentumok

Kérelem /a tanúsítás elvégzésére/

Kérdőív a tanúsítás kérelmezéséhez

Certification Report BSI-PP-0006-2002: Protection Profile – Secure Signature-Creation Device Type 3, version: 1.05, EAL4+

SSI: Rapport de certification 2002/07: JavaCard 32K CRISTAL (référence M256LCAC2)

SchlumbergerSema: JavaCard 32K, Common Criteria/ISO 15408 Security Target (Public version, EAL4+)

BSI: Certification Report BSI-DSZ-CC-0169-2002: Smart Card IC (Security Controller) SLE66CX322P with RSA 2048 6 m148a23

Infineon Technologies AG: SLE66CX322P with RSA2048 / m1484 Security Target (version 1.0.5)

Administration manual: RUBIS (MRD06GI003072 v.1.3)

User manual: RUBIS (MRD06GI003073 v.1.4)

9. Rövidítések

ACE	Advenced Crypto Engine
BSI	Bundesamt für Sicherheit in der Informationstechnik
CEN	European Comittee for Standardization
CPU	Central Processing Unit
DES	Data Encryption Standard /FIPS PUB 46-3, FIPS PUB 74, FIPS PUB 81/
DPA	Differencial Power Attack
DTBS	Data to be Signed /aláírandó adat/
EAL	Evaluation Assurance Level
EEPROM	Electrically Erasable Programmable Read Only Memory
EMA	Electro Magnetic Analysis
EU	Európa Unió
IC	Integrated Circuit
IEC	International Electrotechnical Comission
I/O	Input/Output
IRAM	Internal Random Access Memory
ISO	International Organization for Standardization
IT	Information Technology
MAC	Message Authentication Code
MMU	Memory Management Unit
PIN	Personal Identification Number
PKCS	Public Key Cryptographic Standards
PKCS #1	RSA Cryptography Standard
PP	Protection Profile
RAM	Random Access Memory
RMS	Resource Management System
ROM	Read Only Memory
RSA	Rivest-Shamir-Adleman (public key cryptosystem) /ANSI X9.31/
SHA-1	Secure Hash Algorithm /FIPS PUB 180-1/
SSI	la Securité des Sstemes d'Information
SSCD	Secure Signature Creation Device (lásd BALE)
SSCD-PP	Secure Signature Creation Device – Protection Profile
STS	Self Test Software
Triple-DES	/FIPS PUB 46-3, ANSI X9.52/
VOP	Visa Open Platform
XRAM	eXtended Random Access Memory
BALE	Biztonságos aláírás-létrehozó eszköz