Tanúsítási jelentés

Hung-TJ-006-2003

a CosmopolIC
intelligens kártya

biztonságos intelligens kártya platformról

/Oberthur Card Systems, France,
Philips Semiconductors GmbH, Germany/

/mikrochip:	**P8WE5033V0G,**
nyílt platform:	**COSMOPOLIC (2.1 V4),**
aláírás-létrehozó alkalmazás:	**- (nem tárgya a tanúsításnak)/**

Tartalom

1. A Tanúsítási jelentés tárgya, feladata és hatóköre

Jelen Tanúsítási jelentés tárgya a CosmopolIC intelligens kártya, melyet különböző alkalmazások támogatására (köztük fokozott biztonságú és minősített elektronikus aláírások létrehozásához) kívánnak felhasználni.

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 lenyomatoló (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.

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[3],
- 2-es típus: biztosítja az elektronikus aláírás előállítását egy olyan aláírás-létrehozó adat felhasználásával, amelyet egy 1-es típusú BALE-től importál,
- 3-as típus: biztosítja mind az aláírás-létrehozó / aláírás-ellenőrző adatpárok generálását, mind az elektronikus aláírás előállítását az aláírás-létrehozó adattal.

[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] 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.

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

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

A CosmopolIC intelligens kártyát nem értékelték a fenti védelmi profilok szerint.

Ugyanakkor a CosmopolIC intelligens kártyát és az alapját képező mikrochip-et sokkal általánosabb és szélesebb hatókörű követelményrendszerek szerint értékelték, tanúsították. Ezek alapján az intelligens kártya az alkalmazások igen széles skáláját támogatja, biztonságos futtatási környezetet és kriptográfiai támogatást biztosítva számukra. Az alkalmazások köre túlmutat a hagyományos debit/credit kártyák, elektronikus pénztárcák és hűség kártyák körén, számos erős kriptográfiai alapot igénylő alkalmazásra is kiterjed, köztük a nyilvános kulcsú kriptográfia alkalmazásának alábbi klasszikus területeire:

- titkosítás,
- hitelesítés,
- elektronikus (digitális) aláírás.

A CosmopolIC intelligens kártya az alábbi tanúsítási eredményekkel rendelkezik:

Az intelligens kártya alapját képező chip-et (Philips P8WE5033) értékelték az alábbi védelmi profil szerint:

- BSI-PP-0002-2001: Smart Card IC Platform Protection Profile (EAL5+)

Az intelligens kártya platformját (chip + BIOS + Virtuális gép + API + OS + rezidens alkalmazás) értékelték az alábbi biztonsági előirányzat szerint:

- CosmopolIC 2.1 v4 JavaCard Open Platform Security Target (EAL4+)

Jelen tanúsítási jelentés fő feladata annak megállapítása, hogy:

- A CosmopolIC különböző biztonsági követelményrendszereknek való megfelelését igazoló tanúsítványok milyen pozitív állításokat fogalmaznak meg az intelligens kártya biztonsági tulajdonságaira, megbízható felhasználhatóságára,
- a fent említett tanúsítványok érvényessége milyen feltételeket támaszt az intelligens kártya felhasználására, azaz különböző appletek fejlesztésére és alkalmazására vonatkozóan.

A tanúsítási jelentés további szerkezete a következő:

- A CosmopolIC intelligens kártya legfontosabb tulajdonságainak összefoglalása, beleértve az intelligens kártya hardver alapját képező mikrochip legfontosabb tulajdonságait is. (2. fejezet).
- A CosmopolIC intelligens kártya értékelési és tanúsítási eredményeinek összefoglalása (3. fejezet).
- A CosmopolIC intelligens kártya megfelelőségének viszonyítási alapját képező biztonsági előirányzat (Security Target) 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).
- A tanúsításhoz megkövetelt fejlesztői bizonyítékok (a mikrochip-re vonatkozó EAL5+, illetve az intelligens kártya egészére vonatkozó EAL4+ értékelési garancia szint elvárásai) (6. fejezet).
- Az alkalmazások fejlesztésére és felhasználására vonatkozó feltételek megadása (7. fejezet).
- A jelen tanúsítási jelentéshez figyelembe vett dokumentumok jegyzéke (8. fejezet).
- A felhasznált rövidítések jegyzéke (9. fejezet).

2. A CosmopolIC legfontosabb biztonsági tulajdonságainak összefoglalása

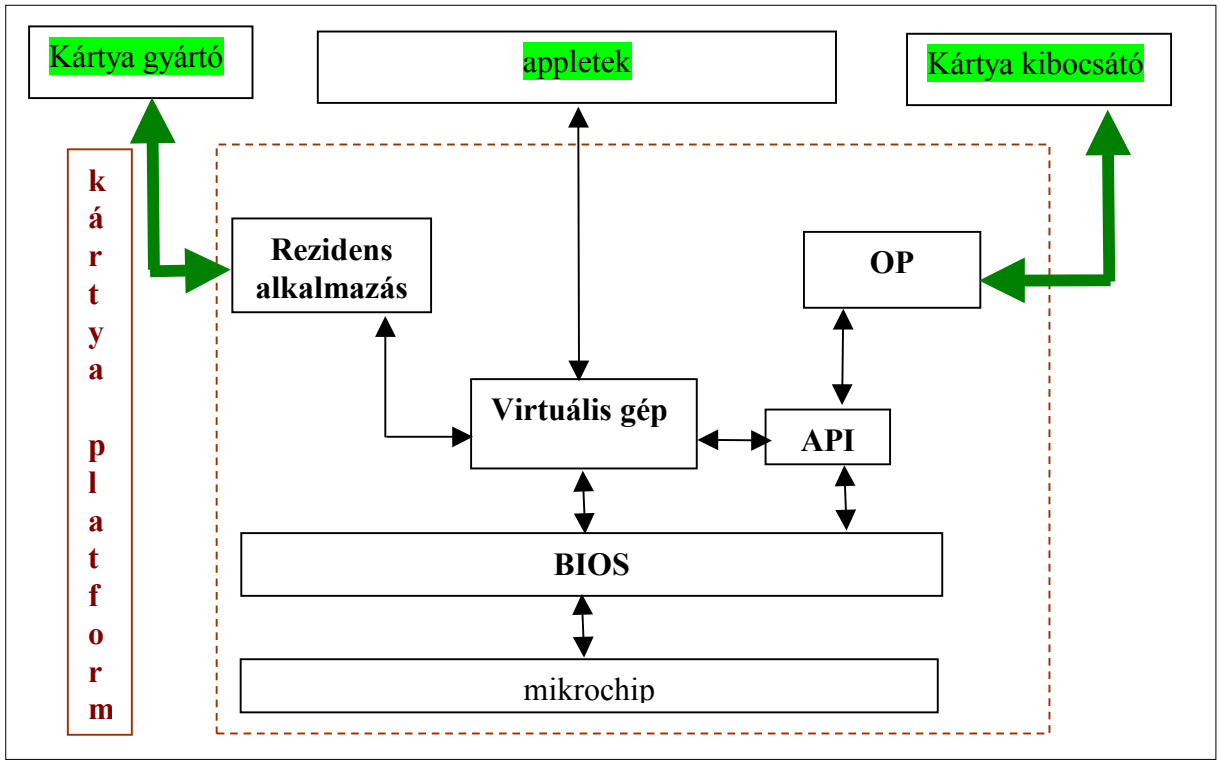
2.1 A CosmopolIC intelligens kártya fő komponensei

Az Oberthur Card Systems CosmopolIC 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 CosmopolIC intelligens kártya az alábbi komponensekből áll:

- **mikrochip** (a Philips P8WE5033V0G típusú chip-je),
- **BIOS** (a hardver komponens és az alkalmazások közötti interfész)
- **virtuális gép** (az utólag telepített /letöltött/ alkalmazások számára egységes /operációs rendszertől független/ felületet biztosító, az alkalmazások futtatását végző komponens),
- **API** (jelen esetben a JavaCard 2.1.1 alkalmazás interfész),
- **nyílt platform alkalmazás** (jelen esetben az Open Platform OP 2.0.1, Configuration 1b /benne az alkalmazásokat az intelligens kártyára telepítő, onnan törlő, illetve a külvilággal való kommunikáció biztonságát felügyelő „**Kártyamenedzser**”/
- **rezidens alkalmazás** (parancs irányító)

A fenti komponensek nem tartalmazzák az intelligens kártyára tölthető, azon futtatható alkalmazásokat (ezért használjuk a későbbiekben a CosmopolIC intelligens kártyára a „biztonságos intelligens kártya platform” megnevezést).



A **mikrochip** képezi a CosmopolIC intelligens kártya alapját. Hardver és förmver alkotóelemeit, illetve főbb biztonsági tulajdonságait a 2.4 alfejezet részletesen tárgyalja.

A **BIOS** interfészt biztosít a hardver komponens (mikrochip) és a natív komponensek (virtuális gép és API) között. A következőket valósítja meg:

- APDU (az intelligens kártyával való adatcsere alapegység csomagja) kezelés,
- időzítés kezelés,
- kivétel kezelés,
- tranzakció kezelés,
- EEPROM hozzáférés,
- kriptográfiai modulok (RSA kulcsgenerátor, DES, RSA, SHA-1)

A (JavaCard 2.1.1-nek megfelelő) **virtuális gép** a következőket valósítja meg:

- értelmezi a JavaCard appletek bájt kódját,
- támogatja a logikai csatornákat, lehetővé téve különböző appletek kiválasztását (egy időben) különböző csatornákon (amiből 4-et kezel az intelligens kártya),
- támogatja a ROM-ba töltött appletek végrehajtását,
- aktivizálódik, amint egy applet kiválasztásra kerül.

A (JavaCard 2.1.1-nek megfelelő) **API** támogatja az alábbiakat:

- kulcsgenerálás,
- üzenet aláírás és titkosítás,
- egyedi API OCSystem,
- egyedi API FileSystem.

A **nyílt platform alkalmazás (OP):**

- a Kártyamenedzser-ből, API OPsystem-ből és biztonsági tartományokból áll,
- Java nyelven íródott, bájt kódját a ROM tárolja,
- akkor aktivizálódik, amikor a kártya kibocsátó kiválasztja a Kártyamenedzsert.

/Az API Opsystem-et az appletek bármikor meghívhatják./

A rezidens alkalmazás egy olyan natív kód alkalmazás, mely:

- fogadja a kártya parancsokat,
- az alkalmazásokhoz és modul függvényekhez irányítja őket.

2.2 Az intelligens kártya életciklus változásai

A Kártyamenedzser felelős a kártya és annak tartalma általános biztonságáért és adminisztrálásáért. Ennél fogva a Kártyamenedzser életciklusa tekinthető az egész kártya életciklusának is. A Kártyamenedzser:

- birtokolja és kezeli a kártya életciklus állapot információit,
- az APDU parancsokra adott válaszként kezeli a kért életciklus változtatásokat.

2.2.1 A Kártyamenedzser életciklus állapotai

Az alábbi táblázat a Kártyamenedzser életciklus állapotait tekinti át.

állapot	leírás
VOP megszemélyesítés (5. fázis)	Ez az életciklus a Kártyamenedzser applet kezdeti állapota, közvetlenül installálását követi. Ebben az állapotban (mielőtt az OP_READY állapotba kapcsolnák) kell betölteni az inicializáló kulcsot.
OP_READY (5. fázis)	Ebben az életciklus állapotban a futásidejű környezet valamennyi alaptulajdonsága elérhető, és a Kártyamenedzser kész az APDU parancsok fogadására, végrehajtására és megválaszolására. A kártyára a következő feltételezések vonatkoznak ebben az életciklus állapotban: • a futásidejű környezet végrehajtásra kész, • egy inicializáló kulcs elérhető a Kártyamenedzseren belül.
INITIALISED (5. fázis)	Ez az életciklus állapot egy adminisztratív kártya gyártási állapot. A legtöbb Kártyamenedzser megszemélyesítő feladatra ebben az állapotban kerül sor.
SECURED	A kártya kibocsátása során ez az életciklus állapot a normál működési állapot. Ez az állapot jelzi a Kártyamenedzser számára, hogy érvényre juttassa a kártya kibocsátás utáni viselkedésére vonatkozó biztonsági szabályokat, mint pl. az appletek betöltését és aktivizálását. A kártyára a következő feltételezések vonatkoznak ebben az életciklus állapotban: • a Kártyamenedzser tartalmazza a teljes funkcionalitáshoz szükséges összes kulcskészletet és biztonsági elemet, • a kártya kibocsátó által megadott kezdeti kártya tartalom csak a Kártyamenedzseren keresztül változtatható, • a kártya kibocsátóhoz tartozó appletek kibocsátás utáni megszemélyesítése csak a Kártyamenedzseren keresztül végezhető.
CM_LOCKED	Ez az életciklus állapot jelzi a Kártyamenedzsernek, hogy átmenetileg valamennyi appletet elérhetetlenné tegyen, saját magán kívül. Ez az állapot teszi lehetővé a kártya kibocsátó számára, hogy (kártyán belüli vagy kívüli) biztonsági támadás észlelése esetén átmenetileg elérhetetlenné tegye a kártya funkcionalitását. Ebben az állapotban a kártya csak a kártya kibocsátója által ellenőrzött Kártyamenedzseren keresztül működik.
TERMINATED	Ezzel az életciklus állapottal a kártya funkcionalitása folyamatosan elérhetetlenné válik, beleértve magát a Kártyamenedzsert is. Ez az állapot a kártya logikai megsemmisítésére ad mechanizmust, melyre a kártya lejárásakor, vagy egy komoly veszély detektálása esetén van szükség. Ez az állapot visszafordíthatatlan, s a kártya életciklusának végét jelzi.

2.2.2 A BIOS életciklusa

Az alábbi táblázat a BIOS két életciklus állapotát tekinti át.

állapot	leírás
Üres EEPROM	Az EEPROM üres, amikor az IC gyártó leszállítja a mikrochip-et, kivéve a gyártó titkos kulcsát (Transport key, MSK).
Inicializált EEPROM	Első bekapcsoláskor a BIOS inicializálja saját adatait: • az ATR fájlokat, • az alapértelmezett (default) applet hivatkozásokat, • a FAT táblát.

2.2.3 A rezidens alkalmazás életciklusa

Az alábbi táblázat a rezidens alkalmazás három életciklus állapotát tekinti át.

állapot	leírás
Elő-megszemélyesítési állapot	A rezidens alkalmazás alábbi parancskészlete aktív: • EXTERNAL_AUTHENTICATE, • GET_CHALLENGE, • GET_DATA, • INSTALL, • LOAD_APPLET, • LOAD_STRUCTURE, • MANAGE_CHANNEL.
Használat	A rezidens alkalmazás alábbi parancskészlete aktív, amennyiben nincs applet kiválasztva: • SELECT, • MANAGE_CHANNEL, • GET_DATA.
Zárolt/blokkolt	Valamennyi rezidens alkalmazás parancs inaktív.

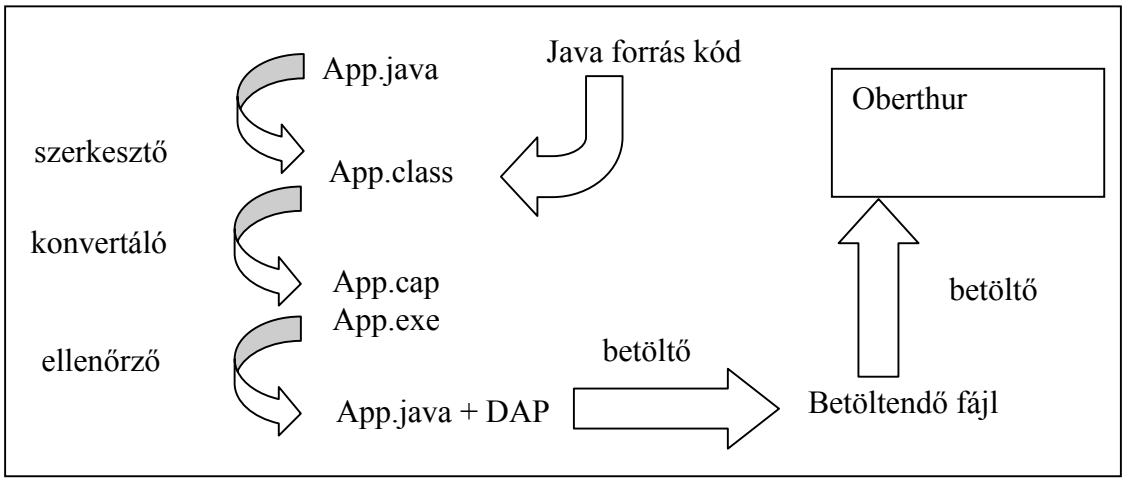
2.2.4 A betöltött fájl életciklusa

Az alábbi táblázat a betöltött fájl két életciklus állapotát tekinti át.

Állapot	leírás
LOADED	A Kártyamenedzser valamennyi betöltött fájlt a kártyán lévőnek és használhatónak tekint.
LOGICALLY_DELETED	Amennyiben a Kártyamenedzser parancsot kap egy olyan betöltött fájl törlésére, melyet fizikailag nem képes törölni, átállítja annak állapotát „logikailag törölt”-re. Egy betöltött fájl „logikailag törölt” állapotát nem lehetséges visszaállítani. A Kártyamenedzser a betöltött fájl „logikailag törölt” állapotát a betöltött fájl fizikai törlésével egyenértékűnek tekinti.

2.2.5 Az applet életciklusa

Egy applet leszállításának meg kell felelnie annak a folyamatnak, melyet a következő ábra szemléltet:



Az applet életciklusa akkor kezdődik, amikor a kártyára telepítik. A telepítésre kétféleképpen kerülhet sor:

- közvetlenül egy betöltő tranzakció során közvetlenül,
- egy kártyán lévő betöltött fájlból.

A Kártyamenedzser felelős egy applet kezdeti életciklus állapota változás kezeléséért az applet teljes működőképessé válásáig. Onnantól kezdve, hogy egy applet a külvilág felöl kiválaszthatóvá válik, maga felügyeli saját életciklusát.

Az applet kezelésre vonatkozó életciklus állapotok tájékoztatják a Kártyamenedzsert az applet állapotáról. Ezek az állapotok applet-függők, s csak az applet által ismertek.

A Kártyamenedzser újra ellenőrzése alá vonhatja egy applet életciklusát, ha:

- a kártya vagy az applet kibocsátója biztonsági problémákat észlel,
- az appletet logikailag vagy fizikailag törölni kell.

A Kártyamenedzser:

- az applet telepítésekor az applet életciklus állapotát a kezdeti INSTALLED értékre állítja,
- az appletet kiválaszthatóvá teszi az állapot SELECTABLE értékre állításával.

Az applet kezeli saját életciklus állapotváltozásait a SELECTABLE állapotból a PERSONALISED vagy az opcionális BLOCKED állapotba. Az appletek betöltése, telepítése és megszemélyesítése a kártya általános életciklus modelljének 5. 6. és 7. szakaszaiban lehetséges.

Az applet életciklusának bármely pontján a Kártyamenedzser biztonsági okokból ismét ellenőrzése alá vonhatja, BLOCKED értékre állítva életciklus állapotát. Ha az appletet el kell távolítani a kártyáról, ezt a folyamatot is a Kártyamenedzser vezérli, megfelelő értékre állítva az életciklus állapotot. ismét

Az alábbi táblázat az applet hat életciklus állapotát mutatja be.

Állapot	Leírás
INSTALLED	Ez az állapot a nyílt platform kontextusában azt jelenti, hogy: • Az applet végrehajtható változata helyesen beszerkesztődött, • Valamennyi szükséges memória lefoglalás megtörtént, • Az applet végrehajtható.
SELECTABLE	Ebben az életciklus állapotban az applet APDU parancsok fogadására kész a külvilágtól. Csak a jól működő, megfelelőn telepített appleteket szabad ebbe az állapotba helyezni.
PERSONALISED	Az ebbe az életciklus állapotba kerülés előfeltételei applet-specifikusak. Ugyanakkor ez az állapot azt mutatja, hogy az appletet ellátták a funkcionalitásához szükséges valamennyi megszemélyesítő adattal és kulccsal. Az applet viselkedését ebben az állapotban maga az applet határozza meg, a kártyamenedzser nem érintett ebben.
BLOCKED	Az ebbe az életciklus állapotba kerülés előfeltételei applet-specifikusak. Ugyanakkor ez az állapot azt mutatja, hogy applet-specifikus biztonsági problémát észleltek, vagy a kártyán kívülről, vagy az appleten belülről. Az applet viselkedését ebben az állapotban maga az applet határozza meg, a kártyamenedzser nem érintett ebben.
LOCKED	Ezt az életciklus állapot használja a Kártyamenedzser vagy a kártya kibocsátó annak megakadályozására, hogy az applet kiválasztható, s így végrehajtható legyen. Amennyiben a Kártyamenedzser egy támadást észlel, s azt egy konkrét applethez kapcsolódónak értékel, akkor ez az állapot teszi lehetővé az applet kiválasztásának megakadályozását. A kártya kibocsátó is megállapíthatja, hogy a kártya egy konkrét appletjét zárolni kell üzleti, vagy biztonsági okokból, s kezdeményezheti az életciklus megváltoztatását (zárolást) a Kártyamenedzseren keresztül. Egy LOCKED állapotú appletet csak úgy lehet ismét kiválaszthatóvá tenni, ha a Kártyamenedzser ugyanabba az állapotba állítja vissza az appletet, mint amiből a zárolást végezte.
LOGICALLY_DELETED	Amennyiben a Kártyamenedzser közvetlenül vagy közvetve parancsot kap egy biztonsági tartománytól egy olyan applet törlésére, melyet fizikailag nem képes törölni, átállítja annak állapotát „logikailag törölt”-re. Egy applet „logikailag törölt” állapotát nem lehetséges visszaállítani. A Kártyamenedzser az applet „logikailag törölt” állapotát az applet fizikai törlésével egyenértékűnek tekinti.

2.3 A CosmopolIC intelligens kártya biztonsági tulajdonságai

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

- ***a kivételek (exceptions) kezelése***
  A potenciális támadás vizsgálata automatikusan kivétel jelzést vált ki. Ez az aktuálisan futó folyamatot befejezi (abbahagyja). A következő eseményekkel jelzi a hibát:
  - bejegyzi a biztonsági naplóba, amennyiben a hiba típusa elemezhető a biztonság megsértéseként,
  - a biztonsági kivételt okozó appletet bezárja,
  - végrehajtja az applet fejlesztője által megírt kivétel kezelési folyamatot (a JavaCard 2.2.1 Exception Handling szerint),
  - egyébként hiba állapottal tér vissza.

- ***a CAP fájl sértetlenségének ellenőrzése***
  A CAP fájlt (vagyis az optimálisan konvertált appletet tartalmazó fájlt) alá kell írni. Az intelligens kártya ellenőrzi ezt az aláírást a CAP (konvertált applet) fájl betöltésekor. Integritás hiba esetén a CAP fájl nem kerül betöltésre.

- ***biztonságos csatorna a külső felhasználókkal kicserélt információk sértetlenségének biztosítására***
  Az adatok, kulcsok és privilégiumok sértetlenségének ellenőrizhetőségét a velük átküldött MAC garantálja. /A kártya kibocsátóval folytatott információcsere biztonsági követelményeit a Kártyamenedzser életciklusa határozza meg. Ez a szolgáltatás (a kártyával kicserélt információk MAC-on alapuló integritásvédelme) az appletek számára is elérhető/.

- ***biztonságos csatorna a külső felhasználókkal kicserélt információk bizalmasságának biztosítására***
  Az adatok és kódok bizalmasságát a DES algoritmussal való titkosítás garantálja. /A kártya kibocsátóval folytatott információcsere biztonsági követelményeit a Kártyamenedzser életciklusa határozza meg. Ez a szolgáltatás (a kártyával kicserélt információk DES-en alapuló titkosítása) az appletek számára is elérhető/.

- ***a kártya kibocsátó (adminisztrátor) hitelesítése***
  Egy biztonságos csatornát kiépítő kommunikációs munkaszakasz kezdetén kötelező a kölcsönös hitelesítés, még mielőtt bármilyen lényeges adat továbbításra kerülne.

- ***Az érzékeny adatok bizalmassága***
  Az intelligens kártya megvédi az alábbi adatok bizalmasságát két (RAM-beli vagy EEPROM-beli) memória blokk összehasonlítása során:
  - PIN értékek,
  - bájt rendezők.

Az intelligens kártya biztosítja a maradvány információk bizalmasságát:
- a FAT tábla kezelésével és a hulladékinformáció összegyűjtésével,
- a deallokálásra kerülő EEPROM törlésével,
- az allokálásra kerülő átmeneti rendezők törlésével.

- ***tranzakciók védelme (pl. áramkimaradás esetén)***
  Egy tranzakció a hosszú távon tárolt adatok részleges módosítására irányul. Az intelligens kártya erős támogatást ad az elemi tranzakcióknak, a tranzakció előtti állapotok automatikus visszaállítását biztosítva a normálistól eltérő befejezések esetén. Ez védelmet biztosít például az olyan események ellen, amikor áramkimaradás következik be egy tranzakció közben.
  Annak érdekében, hogy a PIN kódok ellenőrzését áramkimaradással, illetve egyéb zavarással ne lehessen megkerülni, a PIN kód megadásra rendelkezésre álló kísérletek száma még az összehasonlítás (ellenőrzés) előtt csökkentésre kerül.

- ***ratifikálás***
  Ez a biztonsági funkció:
  - kezeli a PIN kód megadásra még rendelkezésre álló kísérletek számát,
  - lelassítja a kártyakibocsátó (adminisztrátor) hitelesítési idejét,
  - naplóbejegyzésben rögzíti a kártya gyártó sikertelen hitelesítését.

- ***EEPROM kvóta***
  A kártya kibocsátó (adminisztrátor) az appletek számára egy (teljes életciklusukra érvényes) korlátot határozhat meg a felhasználható nem-felejtő memória területre.

- ***Az érzékeny adatok sértetlenségének ellenőrzése***
  Az intelligens kártya ellenőrzi a kriptográfiai kulcsok, hitelesítő adatok (PIN kódok) és az érzékeny applet adatok sértetlenségét. Integritási hiba észlelése esetén hibajelzést ad, az érintett adatot elérhetetlenné teszi, s a folyamatban lévő műveletet megszakítja. Ez a művelet véd az adatok manipulálással történő felfedése ellen.

- ***az objektumok sértetlenségének ellenőrzése***
  Az intelligens kártya felhasználás előtt ellenőrzi a Java objektumok, kártya nyilvántartási adatok (applet azonosító, applet privilégiumok), kulcskészlet verziók és biztonsági napló fájlok sértetlenségét. Integritási hiba észlelése esetén hibajelzést ad, az érintett adatot elérhetetlenné teszi, s a folyamatban lévő műveletet megszakítja.

- ***az appletek sértetlenségének ellenőrzése***
  Egy applet végrehajtása előtt az intelligens kártya ellenőrzi annak sértetlenségét.

- ***a ROM kódok sértetlenségének ellenőrzése***
  Az intelligens kártya ellenőrzi a ROM-ban tárolt kód sértetlenségét:
  - minden reset során (részleges ellenőrzés),
  - a gyártó hitelesítése során az „External Authenticate” parancs segítségével (teljes ellenőrzés).

- ***belső szerepkör kezelés: kártya nyilvántartás***
  Az intelligens kártya kezeli az appletek belső szerepköreit, a kártya nyilvántartásában tárolt privilégiumokon keresztül.

- ***az elindítási folyamat következetessége***
  Az elindítás folyamán az intelligens kártya elnémítja (leállítja) magát a következő hibák esetén:
  - a Kártyamenedzser életciklusának ellentmondó állapot,
  - az EEPROM integritás hibája,
  - a biztonsági napló fájl integritás hibája,
  - a ROM kód integritás hibája,
  - a biztonsági napló fájlba írt rekordok száma elér vagy meghalad egy korlátot,
  - az opcionális kód terület integritás hibája,
  - a véletlenszám generátor blokkolása,
  - a kriptográfiai modul hibás működése,
  - a FAT tábla integritás hibája,
  - kivétel jelzés kiadása.

- ***a biztonsági napló fájl elemzése***
  Ez a funkció azt vizsgálja meg, hogy a biztonsági napló fájlba írt rekordok száma elér-e vagy meghalad-e egy korlátot. Ha igen, lenémítja a kártyát.

- ***biztonsági információ bejegyzése a biztonsági naplóba***
  Olyan kivétel bekövetkezése esetén, melynek típusa a biztonság megsértésének tekinthető, a kivétel típusa, s a kiváltó applet bejegyzésre kerül a biztonsági naplóba.

- ***a kártya gyártó hitelesítése***
  A megszemélyesítés folyamata során kötelező a gyártó hitelesítése a kommunikációs munkaszakasz kezdetén, még mielőtt bármilyen lényeges adat a kártyára kerülne.

- ***A rezidens alkalmazás parancs irányítója***
  A megszemélyesítés folyamata során ez a funkció állapítja meg, hogy a gyártó hitelesítése szükséges-e minden parancsnál.

- ***a kulcs sértetlenségének folyamatos ellenőrzése: kulcsellenőrző érték***
  Ez a funkció egy kulcsellenőrző érték algoritmus használatával a kulcs integritását ellenőrzi, a Visa nyílt platform kártya specifikációnak megfelelően (VOP CS: 9.3.4).

- ***a Kártyamenedzser parancs irányítója***
  A Kártyamenedzser kiválasztásakor ez a funkció állapítja meg, hogy a kártya kibocsátó hitelesítése szükséges-e minden parancsnál.
  Egy biztonságos csatorna megnyitása esetén ez a funkció állapítja meg a Kártyamenedzser életciklusa alapján, hogy kötelező-e minden parancsnál a biztonságos üzenetváltás.

- ***a biztonsági napló fájl olvasása***
  Ez a funkció (a kártya kibocsátó sikeres hitelesítését követően) kiolvassa, majd érthető formában kiadja a biztonsági napló fájlt.

- ***Titok generálása***
  Ez egy kettős funkció:
  - véletlenszám generálás: a mikrochip véletlenszám generátorára építve egy véletlen számot állít elő,
  - munkaszakasz kulcs generálás: a Kártyamenedzsert érintő valamennyi munkaszakasz kommunikáció biztonságának érdekében munkaszakasz kulcsot állít elő. Az így előállított DES munkaszakasz kulcsokat a biztonságos csatorna műveletihez (bizalmasság és sértetlenség garantálására) használják.

- ***RSA kulcsok generálása***
  Az intelligens kártya appleteket biztosít RSA kulcsgenerálási szolgáltatásra. Ez a szolgáltatás a mikrochip RSA koprocesszorát használja.

- ***DES algoritmus***
  Az intelligens kártya ezt a funkciót a DES hardverrel valósítja meg.

- ***RSA algoritmus***
  Az intelligens kártya ezt a funkciót a FameX koprocesszor segítségével gyorsítja meg.

- ***Tűzfal***
  Ez egy összetett funkció az alábbi funkció elemekkel:
  - applet elkülönítés
    Az intelligens kártya támogatja az appletek és kontextusok (applet környezetek) elkülönítését.
    Az elkülönítés azt jelenti, hogy egy applet nem férhet hozzá egy másik kontextus appletjének mezőihez és objektumaihoz, hacsak a másik applet nem biztosít közvetlenül egy hozzáférési interfészt.
  - JCRE privilégiumok
    Lévén a JCRE kontextus egy rendszer kontextus, speciális előjoga van: a kártya valamennyi objektumának eljárásait elvégezheti. A CosmopolIC intelligens kártya esetén a Kártyamenedzser kontextusa a JCRE kontextus (s így minden kártya objektum eljárásait elvégezheti).
  - JCRE belépési pont
    A JCRE belépési pontok olyan objektumok, melyek tulajdonosa a JCRE kontextus, egyben meg vannak jelölve, mint belépési pont eljárásokat tartalmazók.
    A tűzfal megvédi ezeket a belépési pontokat az appletek felöli eléréstől. Ugyanakkor a belépési pont kijelölés lehetővé teszi ezen objektumok eljárásai számára, hogy bármely kontextusból meghívják.
    A CosmopolIC intelligens kártya JCRE belépési pontjai az APDU objektum és a kártya futásidejű kivétel jelzései (runtime exceptions).

Ha egy objektum JCRE belépési pont, akkor az applet elkülönítésre vonatkozó általános szabályok eltérnek, megengedve az aktuális kontextus ellenőrzése alatti általános hozzáférést.

- globális rendezők (arrays)
  A globális rendezők tulajdonosa a JCRE kontextus, de valamennyi kontextusból elérhetők.
  A CosmopolIC intelligens kártya egyetlen globális rendezője az APDU buffer.
  Erre a globális rendezőre (APDU buffer) az applet elkülönítésre vonatkozó általános szabályok eltérnek, megengedve az aktuális kontextus ellenőrzése alatti általános hozzáférést.
- megosztható interfész
  A megosztható interfész a megosztott objektumok azonosítására használható. Minden olyan objektumnak, melyet az applet tűzfalon keresztül meg kell osztani, közvetve vagy közvetlenül ezt az interfészt kell alkalmaznia. A tűzfalon keresztül csak a megosztható interfészben meghatározott eljárások érhetők el.
  Ha az applet meghívja a *getPreviousContextAID* parancsot akár magából az appletből, akár egy külső appletből a megosztható interfészen keresztül elérhető eljárásból, a parancs azonosítja meghívóját.

- ***Kulcskészlet verziójának menedzselése***
  Egy kulcskészlet betöltése frissítheti, törölheti vagy kiegészítheti a korábbi kulcskészlet.

- ***Hozzáférés a DES kulcsokhoz***
  A DES kulcsokhoz való hozzáférés megfelel azoknak a szabványoknak, melyeket a JavaCard 2.1.1 API, OP CS, VOP CS dokumentumok tartalmaznak. Ez a hozzáférés megvédi a kulcsot az illetéktelen felfedéstől.

- ***Hozzáférés az RSA kulcsokhoz***
  Az RSA kulcsokhoz való hozzáférés megfelel azoknak a szabványoknak, melyeket a JavaCard 2.1.1 API dokumentum tartalmaz. Ez a hozzáférés megvédi a kulcsot az illetéktelen felfedéstől.

- ***Az átmeneti rendezők kezelése a logikai csatornákban***
  Ez a funkció garantálja az applet(ek)hez tartozó, különböző logikai csatornákban végrehajtott CLEAR_ON_DESELECT átmeneti rendezők elkülönítését.

2.4 A CosmopolIC intelligens kártya alapját képező chip biztonsági tulajdonságai

A CosmopolIC intelligens kártya alapját a Philips P8WE5033V0G típusú chip-je biztosítja.

Az P8WE5033V0G egy teljes mikrochip, melynek hardver alkotó elemei az alábbiak:

- 8-bites (80C51) központi feldolgozó egység (CPU),
- speciális funkciójú regiszterek (melyeken keresztül a szoftverek elérhetik a chip biztonsági funkcióit),
- Triple-DES titkosítást végző koprocesszor,
- FameX nagy egészekkel moduláris műveleteket végző koprocesszor,
- memóriák:
  - RAM (2304 bájt)
  - ROM (96 Kbájt felhasználói, 8 Kbájt tesztelési),
  - EEPROM (32 Kbájt, adat- és program-memóriaként egyaránt elérhető)
- biztonsági érzékelőkkel és biztonsági logikával ellátott áramforrás modul,
- az integrált áramkör egész tervezésével megvalósított fizikai biztonsági védelmi mechanizmusok,
- belső óra,
- véletlenszám generátor,

Az P8WE5033V0G mikrochip förmver alkotó eleme az alábbi:

- az IC dedikált teszt szoftvere (ROM-ban tárolva, csak a teszt üzemmódban elérhető módon).

Az P8WE5033V0G mikrochip-et nagy biztonságot igénylő alkalmazások széles skálájához fejlesztették, s az ISO 7816 szabványnak megfelelő chip kártyákba ágyazáshoz tervezték. Támogatja a titkos adatokból számított hitelesítést, adatok és kulcsok titkosítását, valamint digitális aláírások készítését. Valamennyi biztonsági ellenintézkedését a teljes rendszer szerves részeként úgy tervezték, hogy azok egységes egészként erősítsék egymást. A biztonsági ellenintézkedések két csoportra oszthatók, a teljesen hardverben megvalósítottakra (mely nem enged meg szoftver által vezérelt kivétel kezelést), illetve a szoftver úton felügyeltekre.

Az P8WE5033V0G mikrochip alábbi biztonsági funkcióit érintette az előzetes értékelés, majd az ezt követő (német séma alapján végzett) tanúsítás, melynek eredményeit a CosmopolIC intelligens kártya értékelése és tanúsítása, mint kiindulási alapot vett figyelembe:

- ***Véletlenszám generálás***
  A mikrochip-ben egy valódi, fizikai véletlen jelenségen alapuló véletlenszám generátor van, mely a „műveleti feltételek ellenőrzés” biztonsági tulajdonság által garantált határok között stabilan működik. A véletlenszám generátor folyamatosan 1 bájtos véletlenszámokat generál. Minden bájt legalább 7 bitnyi entrópiával rendelkezik.

- ***Nagy egész számok moduláris műveleteinek támogatása***
  A mikrochip támogatást nyújt nagy egész számok moduláris műveleteihez. Az aritmetikai funkciók az aszimmetrikus kriptográfiai algoritmusok (pl. az RSA) gyorsítására használhatók. Az intelligens kártya beágyazott szoftverének kell kiválasztania a koprocesszor megfelelő funkcióját, majd kell megadnia az aritmetikai függvények változóit. Ez a biztonsági funkció a moduláris aritmetikai műveleteket támogatja általában, s nem konkrét algoritmusokat.

- ***DES koprocesszor***
  A mikrochip hardver koprocesszora szabványos Triple-DES titkosítást hajt végre, 112 bites kulcsméret mellett. A titkosítási algoritmus megvalósítása garantálja, hogy a Triple-DES műveletek során a külsőleg is megfigyelhető jelekből (viselkedésből) nem lehet következtetni sem a nyílt, sem a kulcs adatokra. Ez egyaránt vonatkozik az egyszerű áramfelvételre irányuló (SPA), az áramfelvétel különbségére irányuló (DPA), valamint a műveletek időigényén alapuló (TA) támadásokra.

- ***Működési állapot ellenőrzés***
  A mikrochip megszűri a feszültséget és az óra frekvenciát, érzékelőkkel folyamatosan figyelemmel kíséri (monitorozza) a feszültséget, az óra frekvenciát, a hőmérsékletet, valamint az EEPROM-ba írási folyamat áramerősségét, valamint ellenőrzi a program végrehajtását is. A felhasználóhoz való szállítás előtt a mód-kapcsolót teszt üzemmódról felhasználói üzemmódra állítják. A felhasználói üzemmódban a mikrochip működése közben automatikusan eléri az érzékelőket, s azt is megakadályozza, hogy az alkalmazás kikapcsolja az érzékelőket.

- ***Az üzemmód és konfiguráció védelme, teszt funkciók biztosítása***
  A mikrochip két üzemmódja (teszt üzemmód és felhasználói üzemmód) hozzáférés ellenőrzést biztosít. Teszt üzemmódban a teszt szoftver futtatható, de a beágyazott szoftver nem. A mikrochip kezdeti állapota a teszt üzemmód. Ez átállítható felhasználói üzemmódba, de ezután a teszt üzemmód már nem érhető el többé. A teszt üzemmódban a mikrochip képes EEPROM-ban tárolni az azonosító, elő-megszemélyesítő adatokat, illetve a beágyazott szoftvereket támogató paramétereket. A felhasználóhoz való szállítás előtt a mód-kapcsolót teszt üzemmódról felhasználói üzemmódra állítják (s ezt követően már csak így használható).

- ***Fizikai manipulációk elleni védelem***
  A mikrochip megvédi a manipulálástól alábbi komponenseit:
  - hardver,
  - az IC ROM-ban tárolt dedikált teszt szoftvere,
  - az intelligens kártya ROM-ban és EEPROM-ban tárolt beágyazott szoftvere,
  - EEPROM-ban és RAM-ban tárolt alkalmazói adatok,
  - az EEPROM biztonsági szegmensében tárolt konfigurációs adatok,
  - üzemmód-kapcsoló.

  A mikrochip feldolgozásuk során megvédi az EEPROM-ban és RAM-ban tárolt titkos felhasználói adatok bizalmasságát is.

3. A Common Criteria szerinti értékelés és tanúsítás eredményeinek összefoglalása

A CosmopolIC 2.1 V4 intelligens kártya megfelel a „CosmopolIC 2.1 V4, Open Platform Security Target" biztonsági előirányzatnak.

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_VLA.4 /Nagymértékű ellenállás (csak EAL6-os szinten elvárt)/.

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

A tanúsítás szponzora az Oberthur Card Systems volt.

A CosmopolIC 2.1 V4 intelligens kártya értékelése egy olyan összetett értékelés volt, mert figyelembe vette a termék hardver platformját biztosító P8WE5033V0G mikrochip korábbi értékelési és tanúsítási eredményeit is.

A Philips által fejlesztett P8WE5033V0G mikrochip tanúsítását az alábbiak jellemzik:

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

A tanúsítást a T-Systems ISS GmbH végezte.

Az értékelés és tanúsítás a következő védelmi profilnak való megfelelést igazolta, tanúsította: Smartcard IC Platform Protection Profile (regisztrálta és tanúsította a BSI, BSI-PP-0002-2001).

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_VLA.4 /Nagymértékű ellenállás(csak EAL6-os szinten elvárt)/.

Ennek a tanúsításnak a szponzora a Philips Semiconductors GmbH volt.

4. A CosmopolIC 2.1 V4 értékelési követelményei a Common Criteria szerint készített biztonsági előirányzat szerint

Az alábbiakban áttekintjük annak a biztonsági előirányzatnak (Security Target) a legfontosabb elemeit (a környezetre vonatkozó állításokat, valamint a biztonsági célokat, követelményeket és funkciókat), melynek való megfelelőséget a CosmopolIC 2.1 V4 intelligens kártya értékelését végző laboratórium[4] vizsgálta és igazolta[5].

4.1 A CosmopolIC 2.1 V4 intelligens kártya biztonsági környezete

Az intelligens kártyának a következő értékeket kell megvédenie:

Az alábbi felhasználói adatok bizalmasságát és/vagy sértetlenségét:

- D.BYTECODE /bájt kód (appletek és az appleteket betöltő fájl)/,
- D.JAVAOBJ /Java objektumok/,
- D.LOADFILE /betöltendő fájl/,
- D.APPLIFECYC /applet életciklus állapot/,
- D.PIN /globális és az appletekhez tartozó PIN kódok/,
- D.KEY /a DES algoritmus által felhasznált, az appletek és a kártyamenedzser által birtokolt kriptográfiai kulcsok/.

Az alábbi TSF adatok (az intelligens kártya biztonsági funkcióinak adatai) bizalmasságát és/vagy sértetlenségét:

- D.NBAUTHENTIC /a hitelesítések száma/,
- D.NB_RMAINTRYOWN /az appletekhez tartozó PIN kód találgatására megmaradt kísérletek száma/,
- D.NB_RMAINTRYGLB /a globális PIN kód találgatására megmaradt kísérletek száma/,

[4] Serma Technologies

[5] A CosmopolIC 2.1 V4 fejlesztői nem egy már kész (korábban értékelt, s már elfogadott) védelmi profilt választottak, melyhez saját biztonsági előirányzatukat csak igazítani kellett volna, hanem önálló biztonsági előirányzatot készítettek, s ennek helyességét, szakszerűségét és konzisztenciáját a termékkel együtt értékeltették.

- D.CRYPTOGRAM /annak jelzése, hogy a hitelesítés bemenő adata egy kulcsból eredő, véletlenből számított rejtjelszöveg/,
- D.AUDITLOG /biztonsági napló fájl/,
- D.AUDITLOG_SIZE /a biztonsági napló fájl mérete/,
- D.FLG_INTEGRITY /sértetlenséget jelző flag/,
- ASG.CARDREG /kártya nyilvántartások (applet azonosító és Kártyamenedzser azonosító)/,
- ASG.APPPRIV /különböző applet privilégiumok/,
- AS.CURCONTEXT /aktuális kontextus, applet környezet/,
- AS.AUTH_MSK_STATUS /az MSK (gyártó titkos kulcsa) hitelesítésének állapota/,
- AS.AUTH_CM_STATUS /a Kártyamenedzser hitelesítésének állapota/,
- AS.CMLIFECYC /a Kártyamenedzser életciklusának állapota/,
- AS.CMCONTEXT /a Kártyamenedzser kontextusa/,
- AS.EEPROM_FLAG /az EEPROM sértetlenségét jelző flag/,
- AS.KEYSET_VERSION /a kulcskészlet verziószáma/,
- AS.KEYSET_VALUE /a kulcskészlet értéke/,
- AS.SESSION_KEY /munkaszakasz kulcs/,
- AS.LOGIC_CHANNEL_NB /logikai csatorna sorszáma (1-4)/,
- AS.MAC /egy biztonságos csatornához tartozó parancsok láncolt hitelesítő kódja/,
- AS.SECUR_CHANNEL_NUM /biztonságos csatorna sorszáma/,
- AS.MSKEY /biztonságos csatorna sorszáma/,
- AS.SECURITY_LEVEL /a biztonságos csatorna biztonsági szintjei (bizalmasságot biztosító, sértetlenséget biztosító, bizalmasságot és sértetlenséget biztosító/,
- AS.DAP /Adat hitelesítő lenyomat (letöltött fájl aláírása)/,

- AS.SENRST /az érzékelő-nullázó kijelzője/,
- Check Objects /objektumok sértetlenségének ellenőrzője/,
- Check Code /a program kódok sértetlenségének ellenőrzője/,
- Check ROM /a ROM sértetlenségének ellenőrzője/,
- Check FAT /a FAT tábla sértetlenségének ellenőrzője/,
- Quotas EEPROM /az EEPROM-ból felhasználható kvóta/.

4.1.1 A biztonságra irányuló veszélyek

Az alábbiakban azokat a veszélyeket tekintjük át, mellyel szemben az intelligens kártya felvállalja a védelmet (döntően információs technológiai eszközökkel).

4.1.1.1 Az intelligens kártya fejlesztési fázisának veszélye

A fejlesztés és ellenőrzés fázisaiban az intelligens kártyára vonatkozó következő értékek jogosulatlan módosítása vagy felfedése:

- specifikációk,
- tervek,
- megvalósítások,
- a teszteléshez és fejlesztéshez használt eszközök,
- teszteredmények,
- a gyártók által szállított IC specifikáció.

Az intelligens kártya jogosulatlan módosítása vagy felfedése tárolás és szállítás közben.

4.1.1.2 Veszélyek az intelligens kártya aktív fázisaiban

A ROM-ban és EEPROM-ban tárolt információk jogosulatlan módosítása. Az intelligens kártya manipulálása vagy hiba miatt a következők módosulhatnak:

- felhasználói adatok,
- TSF adatok (az intelligens kártya biztonsági funkcióinak adatai),
- az operációs rendszer kódja.

A betöltendő inicializáló kulcs (Init Key) módosítása vagy felfedése.

A szállító kulcs (Transport key, a gyártó titkos kulcsa) felfedése.

A következő értékek jogosulatlan módosítása vagy felfedése:

- globális PIN kód,
- az appletekhez tartozó PIN kód
- kulcskészletek,
- kulcsok.

Appletek jogosulatlan betöltése és telepítése, fájlok jogosulatlan betöltése. A ROM-ban tárolt betöltő fájl elérhetővé tétele jogosulatlan módon.

Az applet kódjának felfedése betöltés közben.

A bájt kód (appletek és betöltő fájl) jogosulatlan végrehajtása.

A bájt kód (appletek és betöltő fájl) jogosulatlan módosítása.

A bájt kód (appletek és betöltő fájl) jogosulatlan törlése.

A következő értékek életciklus állapotának jogosulatlan módosítása:

- Kártyamenedzser,
- betöltő fájl,
- rezidens alkalmazás,
- applet.

Egy applet jogosulatlan kiválasztása. /Bizonyos applet életciklus állapotok megtiltják egyes appletek kiválasztását. Bizonyos Kártyamenedzser életciklus állapotok megtiltják az összes applet kiválasztását./

Egy applet vagy a Kártyamenedzser azonosítójának jogosulatlan módosítása.

Jogosulatlan applet megszemélyesítés a Kártyamenedzser ProviderSecurityDomain szolgáltatását használva (kulcsokat, Jáva objektumokat, PIN kódokat, applet életciklus állapotot módosítva).

Jogosulatlan kapcsolat létrehozása a biztonsági tartomány és az applet között.

A privilégiumok (előjogok) módosítása, felfedése.

Azonosító applet általi megszerzése egy megosztható Java objektumhoz való hozzáférés érdekében.

Jogosulatlan hozzáférések (PIN kódokhoz, kulcsokhoz, adat táblákhoz, objektumokhoz) miközben egy applet vagy egy felhasználó applet adatokat ír vagy olvas.

A kártyán generált kulcsok felfedése.

A rezidens alkalmazás jogosulatlan elő-megszemélyesítése (az EEPROM tartalmának módosításával).

A virtuális gép adatainak és kódjának jogosulatlan módosítása.

Az EEPROM-ban tárolt ATR fájlok (vagyis azon bájtsorozatok, melyet az intelligens kártya küld válaszként egy reset feltételt követően) jogosulatlan módosítása.

A platform által szállított kártyaerőforrások teljes vagy részleges rejtett összegyűjtése egy rosszindulatú applet által.

4.1.2 Érvényre juttatott biztonsági szabályok

Az intelligens kártya támogatja a Javacard specifikáció (core) API-ját.

A VOP (Visa nyílt platform) kriptográfiai és egyéb szolgáltatásokat biztosít az appletek számára, a biztonsági mechanizmusok megvalósításához.

4.2 A CosmopolIC 2.1 V4 intelligens kártya biztonsági céljai

A biztonsági célok az alábbi fő kérdésköröket érintik:

- az értékek sértetlensége és bizalmassága,
- az intelligens kártya védelme az aktív életszakaszokban, aktív biztonsági funkciók által,
- az intelligens kártya fejlesztési szakaszának és szállítási folyamatainak a védelme.

A fenti fő célok az alábbi négy csoportba sorolhatók:

- a Kártyamenedzser biztonsági céljai,
- az applet menedzselés biztonsági céljai,
- a rezidens alkalmazás biztonsági céljai,
- a BIOS biztonsági céljai.

A következő négy alfejezet ezeket a fő biztonsági célokat részletezi.

4.2.1 A Kártyamenedzserre vonatkozó biztonsági célok

A megszemélyesítő hitelesítése
A megszemélyesítőnek hitelesítenie kell magát, mielőtt a Kártyamenedzser telepítő parancsait végrehajtja. Az appletek betöltése és telepítése (beleértve a ROM-ban tároltakat is) is sikeres hitelesítést követeljen az előzetes személyre szabási (elő-megszemélyesítési) folyamat során.

Az inicializáló kulcs védelme
Az intelligens kártyának ellenőriznie kell, hogy az inicializáló kulcs titkosítva és aláírva van-e a szállító kulccsal.

Az érzékeny adatok sértetlenségének védelme
Biztosítani kell a tárolt érzékeny adatok (napló adatok, kulcskészlet, globális PIN kód, stb.) sértetlenségét.

A kulcskészlet és a globális PIN kód védett betöltése
Az intelligens kártyának ellenőriznie kell, hogy a kulcskészlet és a globális PIN kód titkosítva és aláírva kerül-e betöltésre. A kulcskészlet és a globális PIN kód betöltése és törlése minden fázisban csak sikeres hitelesítés után legyen lehetséges.

Hitelesített applet betöltés
Egy appletet vagy betöltött fájlt minden fázisban csak sikeres hitelesítés után lehessen betölteni, telepíteni vagy törölni a Kártyamenedzseren keresztül.

Aláírt applet betöltés
Az intelligens kártyának ellenőriznie kell, hogy minden betöltött applet alá van-e írva. Ellenkező esetben a kriptográfia algoritmusokat elérhetetlenné kell tenni, vagy korlátozni kell használatukat.

Védett applet betöltési folyamat
Egy alkalmazásfejlesztő által biztosított, a kibocsátó által aláírt bájtkód kártyára töltése folyamán az intelligens kártyának védelmet kell garantálnia a bizalmasság és a sértetlenség szempontjából.

Ellenőrzött kártyamenedzselés
A Kártyamenedzsment rendszernek a Visa nyílt platformot kell használni, amíg azt ellenőrzi, hogy a következő kezelő utasításokat kizárólag a kártya kibocsátó hajtja-e végre:

- az életciklus állapotok változtatása (sikeres hitelesítés után),
- a jelentősebb hibák (melyek mindig naplózásra kerülnek) kiolvasása a naplóból,
- informálás a kártyán lévő appletekről, betöltött fájlokról, illetve ezek életciklus állapotáról.

Életciklus állapotok kezelése
Az appletek és a Kártyamenedzser életciklus állapotának mindig érvényesnek kell lennie, és csak ezen feltétel teljesülése esetén legyenek végrehajthatók az appletek.

Hitelesített azonosító csere
Csak a Kártyamenedzser módosíthassa az appletek és a Kártyamenedzser azonosítóját, az is csak a kártyakibocsátó sikeres hitelesítését követően.

4.2.2 Az applet menedzselés biztonsági céljai

Applet megszemélyesítés
Egy applet megszemélyesítését csak saját maga végezhesse el:

- saját erőforrásait felhasználva,
- a Kártyamenedzserhez vagy saját biztonsági tartományához delegálás mellett.

Védett privilégiumok
Az applet privilégiumok sértetlenségét védeni kell. Ezek a privilégiumok a következők lehetnek:

- Applet - biztonsági tartomány összerendelés,
- Alapértelmezett (default) applet,
- A CM állapot CM_LOCKED állapotra cserélésének joga.

Hitelesített privilégium módosítás
Csak sikeres hitelesítés után módosíthasson bizonyos applet privilégiumokat a kártya kibocsátó (a Kártyamenedzseren keresztül).

Hitelesített életciklus módosítás
Egy applet életciklus állapotainak változtatása csak a kártya kibocsátó sikeres hitelesítés után legyen lehetséges.

Sértetlenség
Az intelligens kártya biztosítsa a felhasználók, a Java objektumok és a felhasználói csomagok sértetlenségét.

Az érzékeny adatok bizalmasságának védelme
Biztosítani kell az érzékeny adatok (PIN kód, kulcsok, stb.) bizalmasságát.

Tűzfal
Az appletek között tűzfal legyen. Egyúttal az appletek ne módosíthassák az intelligens kártya adatait és a kódokat.

Kriptográfiai alkalmazások támogatása
Az intelligens kártya az API-n keresztül biztosítsa az alábbiakat:

- kriptográfiai műveletek (DES, RSA) /a műveleteknek ellenőrizniük kell a kulcsok bizalmasságát és sértetlenségét/,
- biztonságos RSA kulcs generálás,
- valódi véletlen generálás,
- PIN kezelés (létrehozás, módosítás, ellenőrzés, törlés),
- áramkimaradás és tranzakció közbeni kikapcsolás elleni védelem.

Erőforrások védelme
Az intelligens kártyának olyan eszközöket kell biztosítania erőforrásai felhasználásának ellenőrzésére, melyek megakadályozzák a folyamatos jogosulatlan szolgáltatás megtagadást.

4.2.3 A rezidens alkalmazásra vonatkozó biztonsági célok

A megszemélyesítő hitelesítése
A megszemélyesítőnek hitelesítenie kelljen magát, mielőtt a Kártyamenedzser telepítő parancsait végrehajtja. Az appletek betöltése és telepítése (beleértve a ROM-ban tároltakat is) is sikeres hitelesítést követeljen meg az előzetes személyre szabási (elő-megszemélyesítési) folyamat során.

Hitelesített életciklus állapot módosítás
A rezidens alkalmazás életciklusának módosítása csak sikeres hitelesítés után legyen lehetséges.

Bővíthetőség
Az intelligens kártya – megfelelő specifikáció és feljogosítás esetén – támogassa funkcionalitásának módosítását vagy bővítését.

4.2.4 A BIOS-ra vonatkozó biztonsági célok

ATR fájlok védelme
Az ATR fájlok módosítása csak megfelelő jogosultsággal (a kártya gyártó vagy az applet privilégium jogosultsága esetén) legyen lehetséges.

A következő három alfejezet azokat a biztonsági célokat tekinti át, melyeket az intelligens kártya környezetének kell megvalósítania (nem technikai eszközökkel).

4.2.5 A fejlesztői környezetre vonatkozó biztonsági célok

Feljogosított személyzet
Csak az erre feljogosított személyzet férhessen az intelligens kártyára vonatkozó specifikációkhoz, szoftverekhez, részletes tervekhez, tervrajzokhoz vagy bármely más tervezési információhoz (fizikai, személyi, szervezeti és műszaki eljárások).

Tervezés
Az intelligens kártyára teljesüljenek az alábbiak:

- a programok és adatok integritását szem előtt tartó, biztonságos módon legyenek tervezve,
- a kártya tervezők által megkövetelteknek megfelelően használjanak valamennyi biztonsági tulajdonságot, illetve hajtsanak végre minden biztonsági mechanizmust (pl. a kriptográfiát),

Feltételezzük, hogy az intelligens kártya funkcionalitása megfelelő módon tesztelésre kerül az 1. fázis során.

Fejlesztő eszközök
A program és adat sértetlenség érdekében a kártyát biztonságos módon kell tervezni, különös tekintettel az alábbiak alkalmazására:

- szoftver fejlesztési eszközök (szerkesztők, konvertálók, szimulátorok, ellenőrzők, stb.),
- szoftver-hardver integrációs tesztelési eszközök (emulátorok).

Biztonságos szállítási eljárások
A kifejlesztett szoftverek és e szoftverekkel feltöltött IC-k olyan biztonságos szállítási és ellenőrzési eljárásokon essenek keresztül, melyek garantálják a sértetlenséget és bizalmasságot.

Nyomon követhető szállítások eljárások
A kifejlesztett szoftvereket és e szoftverekkel feltöltött IC-ket olyan biztonságos szállítási és ellenőrzési eljárásokkal továbbítsák a megfelelő partnerek felé, melyek garantálják a teljes nyomon követhetőséget.

4.2.6 Az intelligens kártya környezetére vonatkozó biztonsági célok

A szállító kulcs kezelése
A szállító kulcsra teljesíteni kell az alábbiakat:

- biztonságos területen tárolják,
- A platform fejlesztő és az IC gyártó biztonságos módon (a kulcs bizalmasságát és sértetlenséget egyaránt garantálva) cseréljék ki egymás között.

Applet fejlesztés
Az appleteket biztonságos módon kell fejleszteni (a kulcsok bizalmasságát és sértetlenséget egyaránt garantálva).

Applet ellenőrzés
Minden appletet ellenőriztetni kell aláírás előtt. Minden betöltött appletet alá kell írni.

A kódok kezelése
Az appletek kódját, adatait és kulcsait biztonságos módon kell továbbítani (a bizalmasságot és sértetlenséget egyaránt garantálva). Az ebben érintett szereplők: applet megszemélyesítő, gyártó, kártya kibocsátó, applet fejlesztő.

IC kezelése
Az IC gyártójának a 2. 3. és 4. fázisban garantálnia kell az intelligens kártya bizalmasságát és sértetlenségét.

4.2.7 Az intelligens kártya informatikai környezetére vonatkozó biztonsági célok

Kriptográfiai alkalmazások támogatása
Az IC biztosítsa az alábbi kriptográfiai szolgáltatásokat:

- kriptográfiai műveletek (DES, RSA) /a műveleteknek ellenőrizniük kell a kulcsok bizalmasságát és sértetlenségét/,
- valódi véletlen generálás,
- a kriptográfiai pufferek törlése (a deallokálás során).

Manipuláció elleni védelem
Az IC biztosítson védelmet az alábbiak manipulálása ellen:

- hardver,
- a chip RAM-jában, ROM-jában és EEPROM-jában tárolt szoftverek és adatok.

4.3 A CosmopolIC 2.1 V4 intelligens kártya funkcionális biztonsági követelményei

Az alábbiakban felsoroljuk a biztonsági előírás funkcionális biztonsági követelményeit ***(vastag és dőlt betűvel megjelenítve,*** a Common Criteria által használt rövidítéseket is feltüntetve), majd alatta röviden kitérünk arra , hogy a CosmopolIC 2.1 V4 intelligens kártya hogyan felel meg az egyes követelményeknek.

4.3.1 Biztonsági naplózás

Biztonsági napló lista generálása (speciális, CC-n kívüli követelmény)

Az intelligens kártya képes egy biztonsági napló listát generálni a következő naplózandó eseményekkel:

- biztonsági kivételek (exceptions),
- érvénytelen hivatkozási kivételek,
- objektumok sértetlenségének elvesztése.

Az intelligens kártya minden biztonsági naplóbejegyzésben rögzíti legalább az alábbi információkat:

- az esemény típusa,
- a szubjektum (az esemény kiváltója) azonosítója.

Védett napló tárolás (FAU_STG.1)

Az intelligens kártya megvédi a tárolt napló bejegyzéseket a jogosulatlan törléssel szemben.
Az intelligens kártya észleli és megakadályozza a napló bejegyzések módosítását.

Napló áttekintés (FAU_SAR.1)

Az intelligens kártya a kártya kibocsátója számára biztosítja a következő események bekövetkezését jelző bejegyzések kiolvasásának lehetőségét:

- biztonsági kivételek,
- érvénytelen referencia kivételek,
- naplózott „objektum sértetlenség elvesztése” bejegyzések.

A napló bejegyzések módja alkalmas a felhasználó számára ahhoz, hogy az információt értelmezze.

A potenciális megsértés vizsgálata (FAU_SAA.1)

Az intelligens kártya a biztonsági naplóbejegyzések monitorozásakor képes egy szabály készletet alkalmazásával a biztonság potenciális megsértésének kijelzésére.
Hardver eszközökkel képes kijelezni, hogy:

- egy reset-et a normális működtetési körülményektől eltérő kivételeket figyelő érzékelők okozták.

Szoftver eszközökkel képes az alábbi szabályok érvényre juttatására:

- az alábbi naplózott események akkumulálásával vagy kombinálásával képes kijelezni a biztonság potenciális megsértését:

1. a Kártyamenedzser életciklusával ellentmondó események (melyeket az öntesztelő mechanizmusok vagy az adminisztrátori műveletekben mindig aktivizáló életciklus állapot ellenőrzések rögzítenek).
2. az aktív kontextuson (az éppen futó appleten) kívüli jogosulatlan objektum hozzáférések (melyet a tűzfal mechanizmus rögzít, s mely automatikus „biztonsági kivétel”-t generál),
3. egy referenciához való érvénytelen hozzáférés (melyet az objektum hozzáférés mechanizmus rögzít, s mely automatikus „érvénytelen referencia kivétel”-t generál),
4. az EEPROM sértetlenségét jelző flag integritáshibát jelző állapota (mely elnémíttatja a kártyát),
5. biztonsági naplózás,
6. egy kulcs objektum sértetlenségének elvesztése (melyet a kulcs használat mechanizmus rögzít, „objektum sértetlenség elvesztése” bejegyzéssel).

- Egy platform reset után, ha a biztonsági naplóban a naplófájl beteltségét jelző bejegyzés szerepel, a kártya elnémul.

Biztonsági riasztások (FAU_ARP.1)

Az intelligens kártya a biztonság potenciális megsértésének észlelése esetén képes az alábbiak végrehajtására:

- a kártya elnémítása,
- a biztonság megsértését eredményező tevékenység blokkolása, kivétel jelzés (exception) kiadása, a felelős applet lezárása.

4.3.2 Kommunikáció

Választható eredet bizonyítás (FCO_NRO.1)

A megosztható interfészekre vonatkozóan:
/Egy appletben szabályozni lehet, hogy csak bizonyos, egyben hitelesített appletektől fogadjon el bizonyos külső eljárás-felhívásokat./

Az intelligens kártya képes a továbbított eljárás-felhívás eredetére vonatkozó bizonyíték előállítására a fogadó kérésére.
Az intelligens kártya képes összekapcsolni az információ eredőjének kontextusát (vagyis, hogy melyik appletből hívták fel az adott eljárást) és az információ (vagyis az eljárás-felhívás) paramétereit.
Az intelligens kártya lehetővé teszi a fogadó számára az eredet ellenőrzését a felhívás folyamán.

Megjegyzés: a megosztható interfészeket menedzselni kell (meghatározva, hogy milyen appletekből milyen eljárások hívhatók meg, mely más appletekben, a megosztható interfészeken keresztül).

A kívülről betöltendő fájlokra vonatkozóan:
/Egy appletben szabályozni lehet, hogy kívülről csak hitelesített forrásból származó fájlt lehessen betölteni a biztonságos csatornán keresztül./

Az intelligens kártya képes a továbbított D.LOADFILE (betöltendő fájl) és ASG.APPPRIV (az applet privilégiumai) eredetére vonatkozó bizonyíték előállítására a feladó (küldő) kérésére.
Az intelligens kártya képes összekapcsolni az információ eredőjéhez tartozó AS.KEYSET_VALUE-t (vagyis, a betöltendő fájl küldőjének kulcs készletét) és a megfelelő APDU parancsot.
Az intelligens kártya lehetővé teszi a fogadó számára a biztonságos csatornán érkező eredet ellenőrzését.

Megjegyzés: ez a funkció akkor alkalmazható, amikor a Kártyamenedzser életciklus szakasza: OP_READY vagy INITIALISED.

Kikényszerített eredet bizonyítás (FCO_NRO.2)

A CAP fájlokra (konvertált appletekre) vonatkozóan:
/Egy applet betöltése csak hitelesített forrásból lehetséges./

Az intelligens kártya a továbbított (appletet tartalmazó) CAP fájlokra minden esetben kikényszeríti az (appletek) eredetére vonatkozó bizonyíték előállítását.
Az intelligens kártya képes összekapcsolni az információ eredőjéhez tartozó AS.KEYSET_VALUE-t (vagyis, a betöltendő applet küldőjének kulcs készletét) és a CAP fájl komponenseit.
Az intelligens kártya lehetővé teszi a fogadó számára a CAP fájl betöltése folyamán az eredet ellenőrzését.

A biztonságos kártyamenedzselésre vonatkozóan:
/Kívülről fájlt, kulcskészletet, applet privilégiumokat és globális PIN kódot csak hitelesített forrásból lehetséges betölteni./

Az intelligens kártya a továbbított D.LOADFILE (betöltendő fájl), AS.KEYSET_VALUE-t (a betöltendő információk küldőjének kulcs készlete), ASG.APPPRIV (applet privilégiumok), D.GLPIN (globális PIN kód) minden esetben kikényszeríti a (kívülről küldött információ) eredetére vonatkozó bizonyíték előállítását.
Az intelligens kártya képes összekapcsolni az információ eredőjéhez tartozó AS.KEYSET_VALUE-t (vagyis, a betöltendő információ küldőjének kulcs készletét) és a megfelelő APDU parancsot.
Az intelligens kártya lehetővé teszi a fogadó számára a biztonságos csatornán érkező eredet ellenőrzését.

Megjegyzés: ez a funkció (a betöltendő fájlok és privilégiumok esetén) akkor alkalmazható, amikor a Kártyamenedzser életciklus szakasza: SECURED.

4.3.3 Kriptográfiai támogatás

Kriptográfiai kulcs generálás (FCS_CKM.1)

Az intelligens kártya képes 512, 768, 1024 és 2048 bites RSA kulcsokat generálni az ANSI X9.31 szabványnak megfelelően.

A kriptográfiai kulcsokhoz való hozzáférés (FCS_CKM.3)

Az intelligens kártya képes a DES és RSA kriptográfiai kulcsokhoz hozzáférni az alábbi szabványoknak megfelelően:

- Open Platform Card Specification (8. és 9.9 fejezet),
- Visa Open Platform Card Implementation Specification (9.3 fejezet),
- Java Card 2.1.1 Application Programming Interfaces (Javacard.security és Javacardx.crypto csomagok)

A kriptográfiai kulcsok megsemmisítése (FCS_CKM.4)

Az intelligens kártya képes tárolt kulcsértékeinek fizikailag visszafordíthatatlan megsemmisítésére az alábbi szabványokban meghatározott kulcsmegsemmisítési módszerekkel (egyúttal a már megsemmisített kulcsokra való hivatkozásokat is megakadályozva):

- Visa Open Platform Card Implementation Specification (6.4.2 fejezet),
- ISO 11166 for asymmetric keys (RSA),
- ISO 11568 for symmetric keys (DES).

Kriptográfiai eljárás (FCS_COP.1)

Az intelligens kártya képes az alábbi kriptográfiai algoritmusok szabványos végrehajtására:

- DES titkosítás és dekódolás (56 bites kulcsmérettel, a FIPS PUB 46-3, FIPS PUB 81, ANSI X3.92-nek megfelelően),
- Triple-DES titkosítás és dekódolás (112, illetve 168 bites kulcsmérettel, a FIPS PUB 46-3, FIPS PUB 81, ANSI X3.92-nek megfelelően),
- Kriptográfiai kontrollösszeg képzés és ellenőrzés a DES algoritmus segítéségével (ISO 9797),
- Digitális aláírás és aláírás ellenőrzés az RSA algoritmussal (512, 768, 1024 és 2048 bites kulcsmérettel, valamint a PKCS #1 szabványnak megfelelően.

4.3.4 A felhasználói adatok védelme

Biztonsági jellemzőkön alapuló hozzáférés ellenőrzés /JCRE_PRIV/ (FDP_ACF.1)

Az intelligens kártya érvényre juttatja a Kártyamenedzser kontextusán (AS.CMCONTEXT) alapuló, úgynevezett JCRE_PRIV (Java Card Runtime Environment Privilege) hozzáférés ellenőrzést, amikor objektumokat ír.
Az intelligens kártya a következő szabályt juttatja érvényre annak eldöntésére, hogy egy művelet végrehajtható-e a felügyelt objektumok és szubjektumok között:

- Current Context = AS.CMCONTEXT (a Kártyamenedzser aktív)

Részleges hozzáférés ellenőrzés /JCRE_PRIV/ (FDP_ACC.1)

Az intelligens kártya érvényre juttatja az API OCSystem által megvalósított JCRE_PRIV hozzáférés ellenőrzést az objektumok, szubjektumok és műveletek alábbi listájára:
szubjektum:

- S.CM.

Objektum:

- ATR fájlok,
- Card Manager life cycle,
- Applet life cycle,
- Applet privileges,
- Applet export rights,
- Transport key
- Applet,
- CAP file,
- Package.

Művelet:

- setATR,
- lockCard,
- useCard,
- SMWithTransportKey,
- delete,
- setDefaultApplet,
- setStatus,
- setAID,
- setAIDRef,
- setRights,
- getRights.getAIDRef,
- getRights,
- install,
- LoadInit,
- LoadNext,
- LoanEnd.

/A fenti két követelmény lényegében azt jelenti, hogy az aktív Kártyamenedzser végrehajthatja a felsorolt műveleteket a felsorolt objektumokon (ahol ennek értelme van)./

Biztonsági jellemzőkön alapuló hozzáférés ellenőrzés /APP_PRIV/ (FDP_ACF.1)

Az intelligens kártya érvényre juttatja az appletek privilégiumain (ASG.APPPRIV) alapuló, úgynevezett APP_PRIV (Applet Privilege) hozzáférés ellenőrzést, amikor objektumokat ír.
Az intelligens kártya a következő szabályt juttatja érvényre annak eldöntésére, hogy egy művelet végrehajtható-e a felügyelt objektumok és szubjektumok között:

- az aktuális applet privilégium megengedi-e az adott műveletet.

Részleges hozzáférés ellenőrzés /APP_PRIV/ (FDP_ACC.1)

Az intelligens kártya érvényre juttatja az API OPSystem által megvalósított APP_PRIV hozzáférés ellenőrzést az objektumok, szubjektumok és műveletek alábbi listájára:
szubjektum:

- S.Applet.

Objektum:

- ATR fájlok,
- Card Manager life cycle,
- Applet life cycle,
- Global PIN.

Művelet:

- setATRHystoricalBytes,
- TerminatedCard,
- CMLock,
- LockApplet,
- SetCardContentState,
- SetPIN,
- VerifPIN.

/A fenti két követelmény lényegében azt jelenti, hogy egy applet csak akkor hajthatja végre a felsorolt műveleteket a felsorolt objektumokon (ahol ennek értelme van), ha az adott applet fel van előzetesen erre jogosítva (privilégiumai megengedik ezt)./

Biztonsági jellemzőkön alapuló hozzáférés ellenőrzés /Pre_Personal/ (FDP_ACF.1)

Az intelligens kártya érvényre juttatja a gyártó titkos kulcsának hitelesítési állapotán (AS.AUTH_MSK_STATUS) alapuló, úgynevezett Pre_Personal (Prepersonalisation) hozzáférés ellenőrzést, amikor objektumokat ír.
Az intelligens kártya a következő szabályt juttatja érvényre annak eldöntésére, hogy egy művelet végrehajtható-e a felügyelt objektumok és szubjektumok között:

- a gyártó titkos kulcsának hitelesítési állapota = True (hitelesített).

Teljes hozzáférés ellenőrzés /Pre_Personal/ (FDP_ACC.2)

Az intelligens kártya a rezidens alkalmazásra nézve érvényre juttatja a Prepersonalisation hozzáférés ellenőrzést valamennyi objektumra, s valamennyi objektum-szubjektum közötti műveletre vonatkozóan.
Az intelligens kártya azt is garantálja, hogy az objektumok és szubjektumok közötti minden műveletet lefedi valamelyik hozzáférés ellenőrzése.

/A fenti két követelmény lényegében azt jelenti, hogy az elő-megszemélyesítés teljeskörűen felügyeli a rezidens alkalmazást, s az elő-megszemélyesítésnek feltétele, hogy a kártya gyártó hitelesítse magát saját titkos kulcsa segítségével./

Biztonsági jellemzőkön alapuló hozzáférés ellenőrzés /Firewall/ (FDP_ACF.1)

Az intelligens kártya érvényre juttatja az aktuális kontextuson (AS.CURCONTEXT) alapuló, úgynevezett Firewall hozzáférés ellenőrzést, amikor objektumokat ír.
Az intelligens kártya a következő szabályt juttatja érvényre annak eldöntésére, hogy egy művelet végrehajtható-e a felügyelt objektumok és szubjektumok között:

- Current Context = Object Context.

Az intelligens kártya közvetlenül felhatalmaz egy szubjektumot az objektumokhoz való hozzáférésre az alábbi járulékos szabály esetén:

- Object Context = JCRE Context.

Teljes hozzáférés ellenőrzés /Firewall/ (FDP_ACC.2)

Az intelligens kártya az appletekre nézve érvényre juttatja a Firewall hozzáférés ellenőrzést valamennyi adat objektumra, s valamennyi objektum-szubjektum közötti műveletre vonatkozóan.
Az intelligens kártya azt is garantálja, hogy az objektumok és szubjektumok közötti minden műveletet lefedi valamelyik hozzáférés ellenőrzése.

/A fenti két követelmény lényegében azt jelenti, hogy a tűzfal teljeskörűen felügyeli az appletek (más appletek) adat objektumaihoz való hozzáférését, melynek hatására egy applet csak akkor írhat egy más applet objektumába, ha a tűzfal beállításai ezt kifejezetten megengedik számára./

Biztonsági jellemzőkön alapuló hozzáférés ellenőrzés /CardManager/ (FDP_ACF.1)

Az intelligens kártya érvényre juttatja a Kártyamenedzser hitelesítési állapotán (AS.AUTH_CM_STATUS) és a biztonsági szinten (AS.SECURITY_LEVEL) alapuló, úgynevezett CardManager hozzáférés ellenőrzést, amikor objektumokat ír.
Az intelligens kártya a következő szabályokat juttatja érvényre annak eldöntésére, hogy egy művelet végrehajtható-e a felügyelt objektumok és szubjektumok között:

- AS.AUTH_CM_STATUS = True (a Kártyamenedzser aktív),
- Ha AS.SECURITY_LEVEL > 0, és MAC> 0: a kívülről importált adatok sértetlensége garantált.
- Ha AS.SECURITY_LEVEL > 0, és ENC> 0: a kívülről importált adatok bizalmassága garantált.

Teljes hozzáférés ellenőrzés /CardManager/ (FDP_ACC.2)

Az intelligens kártya a Kártyamenedzserre nézve érvényre juttatja a CardManager hozzáférés ellenőrzést az alábbi objektumokra:

- D.LOADFILE /a betöltendőfájl/,
- AS.KEYSET_VALUE /a kulcskészlet értéke/,
- D.GLPIN /a globális PIN/,
- ASG.APPPRIV /az applet privilégiumai/,
- AS.CMLIFECYC /a Kártyamenedzser életciklus állapota/,
- AS_KEYSET_VERSION /a kulcskészlet verziószáma/,
- D.APPLIFECYC /az applet életciklus állapota/,
- ASG.CARDREG /a kártya nyilvántartása/,

s valamennyi objektum-szubjektum közötti műveletre vonatkozóan.
Az intelligens kártya azt is garantálja, hogy az objektumok és szubjektumok közötti minden műveletet lefedi valamelyik hozzáférés ellenőrzése.

/A fenti két követelmény lényegében azt jelenti, hogy a Kártyamenedzser teljeskörűen felügyeli a felsorolt objektumokra irányuló valamennyi műveletet, s ezen keresztül a kívülről importált adatok sértetlensége és bizalmassága is biztosítható/

Felhasználói adatok exportálása biztonsági jellemzők nélkül /CardManager/ (FDP_ETC.1)

A biztonsági funkciók érvényre juttatják a CardManager hozzáférés ellenőrzést, amikor a felügyeletük alá tartozó felhasználói adatot a hatókörükön kívülre exportálnak.
A biztonsági funkciók a felhasználói adatokat a hozzájuk kapcsolódó biztonsági jellemzők nélkül exportálják.

Felhasználói adatok exportálása biztonsági jellemzők nélkül /Firewall/ (FDP_ETC.1)

A biztonsági funkciók érvényre juttatják a Firewall hozzáférés ellenőrzést, amikor a felügyeletük alá tartozó felhasználói adatot a hatókörükön kívülre exportálnak.
A biztonsági funkciók a felhasználói adatokhoz kapcsolódó minden biztonsági jellemzőt figyelmen kívül hagynak a hatókörükön kívülre történő adat exportálás során.

Felhasználói adatok importálása biztonsági jellemzők nélkül /CardManager/ (FDP_ITC.1)

A biztonsági funkciók érvényre juttatják a CardManager hozzáférés ellenőrzést, amikor a felügyeletük alá tartozó felhasználói adatot a hatókörükön kívülről importálnak.
A biztonsági funkciók a felhasználói adatokhoz kapcsolódó minden biztonsági jellemzőt figyelmen kívül hagynak a hatókörükön kívülről történő adat importálás során.

Felhasználói adatok importálása biztonsági jellemzők nélkül /Firewall/ (FDP_ITC.1)

A biztonsági funkciók érvényre juttatják a Firewall hozzáférés ellenőrzést, amikor a felügyeletük alá tartozó alábbi felhasználói adatokat importálják hatókörükön kívülről:

- DES kulcs,
- RSA kulcs,
- PIN érték,
- applet adatok,
- bájt kód (appletek és az appleteket betöltő fájl).

A biztonsági funkciók a felhasználói adatokat a hozzájuk kapcsolódó biztonsági jellemzők nélkül importálják.

Felhasználói adatok importálása biztonsági jellemzők nélkül /APP_PRIV/ (FDP_ITC.1)

A biztonsági funkciók érvényre juttatják az APP_PRIV hozzáférés ellenőrzést, amikor a felügyeletük alá tartozó felhasználói adatot a hatókörükön kívülről importálnak.
A biztonsági funkciók a felhasználói adatokhoz kapcsolódó minden biztonsági jellemzőt figyelmen kívül hagynak a hatókörükön kívülről történő adat importálás során.

Felhasználói adatok importálása biztonsági jellemzőkkel /CM_CAPfile/ (FDP_ITC.2)

A biztonsági funkciók érvényre juttatják a CardManager hozzáférés ellenőrzést, amikor a felügyeletük alá tartozó felhasználói adatot a hatókörükön kívülről importálnak.
A biztonsági funkciók a felhasználói adatokhoz kapcsolódó biztonsági jellemzőket felhasználják.
A biztonsági funkciók garantálják, hogy az alkalmazott protokoll félreérthetetlenül kapcsolja össze a fogadott adatokat és a biztonsági jellemzőket.
A biztonsági funkciók garantálják, hogy az importált adatok biztonsági jellemzőinek értelmezése megfelel a felhasználói adatküldő szándékával.

Megjegyzés: ez a funkció a CAP fájlok importálásakor alkalmazandó.

Részleges maradvány információ védelem /DEALLOC/ (FDP_RIP.1)

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

- Valamennyi Java objektum,
- Hulladékinformáció gyűjtő,
- Kriptográfiai pufferek,
- Átmeneti pufferek.

Részleges maradvány információ védelem /ALLOC/ (FDP_RIP.1)

Az intelligens kártya biztosítja, hogy erőforrás lefoglalás (allokáció) után semmilyen korábbi információ tartalom ne legyen hozzáférhető az alábbi objektumokra nézve:

- Átmeneti objektumok,
- APDU puffer.

A tárolt adatok sértetlenségének figyelése és beavatkozás /EEPROM/ (FDP_SDI.2)

Az intelligens kártya folyamatosan ellenőrzi (monitorozza) valamennyi hatáskörébe tartozó, EEPROM-ban tárolt felhasználói adat sértetlenségét, az alábbi jellemzőre alapulva:

- AS.EEPROM_FLAG

Integritás hiba észlelése esetén az intelligens kártya:

- elnémítja magát.

A tárolt adatok sértetlenségének figyelése és beavatkozás /AUDITLOG/ (FDP_SDI.2)

Az intelligens kártya folyamatosan ellenőrzi (monitorozza) valamennyi hatáskörébe tartozó, a biztonsági naplóban tárolt felhasználói adat sértetlenségét, az alábbi jellemzőre alapulva:

- Audit log checksum

Integritás hiba észlelése esetén az intelligens kártya:

- elnémítja magát.

A tárolt adatok sértetlenségének figyelése és beavatkozás /ROM/ (FDP_SDI.2)

Az intelligens kártya folyamatosan ellenőrzi (monitorozza) valamennyi hatáskörébe tartozó, ROM-ban tárolt felhasználói adat sértetlenségét, az alábbi jellemzőre alapulva:

- ROM code checksum

Integritás hiba észlelése esetén az intelligens kártya:

- elnémítja magát.

A tárolt adatok sértetlenségének figyelése és beavatkozás /JAVAOBJ/ (FDP_SDI.2)

Az intelligens kártya folyamatosan ellenőrzi (monitorozza) valamennyi hatáskörébe tartozó, Java objektumban (D.JAVAOBJ) tárolt felhasználói adat sértetlenségét, az alábbi jellemzőre alapulva:

- D.JAVAOBJ checksum

Integritás hiba észlelése esetén az intelligens kártya:

- hibabejegyzés tesz a biztonsági naplóba és
- jelzi a hibát egy kivétel jelzés generálásával.

A tárolt adatok sértetlenségének figyelése és beavatkozás /BYTECOD/ (FDP_SDI.2)

Az intelligens kártya folyamatosan ellenőrzi (monitorozza) valamennyi hatáskörébe tartozó bájtkódban (D.BYTECOD) tárolt felhasználói adat sértetlenségét, az alábbi jellemzőre alapulva:

- D.BYTECOD checksum

Integritás hiba észlelése esetén az intelligens kártya:

- hibabejegyzés tesz a biztonsági naplóba,
- bezárja a kiválasztott appletet és
- jelzi a hibát egy kivétel jelzés generálásával.

Alapszintű adat-csere bizalmasság (FDP_UCT.1)

Az intelligens kártya képes érvényre juttatni a Pre_Personal és a CardManager hozzáférés ellenőrzéseket annak biztosítására, hogy a fogadott adatok védve legyenek a jogosulatlan felfedés ellen.

Az adatcsere sértetlensége (FDP_UIT.1)

Az intelligens kártya képes érvényre juttatni a CardManager hozzáférés ellenőrzést annak biztosítására, hogy a fogadott adatok védve legyenek módosítás/módosulás ellen.
A fentieken kívül, az intelligens kártya képes az általa fogadott adatokra észlelni, hogy történt-e módosítás/módosulás.

Megjegyzés: a fenti hibák az alábbi esetekben bekövetkezhetnek be:

- adatok továbbítása a biztonságos csatornán,
- a kulcs generálása és fogadása között,
- a CAP file ellenőrzése és fogadása között.

4.3.5 Azonosítás és hitelesítés

A hitelesítési hiba kezelése /kártya gyártó/ (FIA_AFL.1)

Az intelligens kártya képes detektálni, ha 3 téves hitelesítési kísérlet történt a kártya gyártó hitelesítésekor.
Három sikertelen hitelesítési kísérlet után a biztonsági funkciók elnémítják a kártyát.

A hitelesítési hiba kezelése /kártya kibocsátó/ (FIA_AFL.1)

Az intelligens kártya képes detektálni, ha (1) téves hitelesítési kísérlet történt a kártya kibocsátó hitelesítésekor.
Téves hitelesítési kísérlet esetben a kártya lelassítja a következő hitelesítési folyamatot.
A (két hitelesítési kísérlet közötti) várakozási idő exponenciálisan nő, egészen a maximálisan megengedett 15 hitelesítési kísérletig.

A hitelesítési hiba kezelése /kártya felhasználó/ (FIA_AFL.1)

Az intelligens kártya képes detektálni, ha a felhasználó által meghatározott számú téves hitelesítési kísérlet történt bármilyen PIN kódot használó felhasználói hitelesítéskor. /A meghatározható szám 1-127 közötti az appletekhez tartozó PIN kódok esetében, illetve 3-15 közötti a globális PIN kód esetében./
A meghatározott számú sikertelen hitelesítési kísérlet után a biztonsági funkciók blokkolják a megfelelő PIN kódot.

A felhasználói jellemzők meghatározása /kártya gyártó/ (FIA_ATD.1)

Az intelligens kártya képes kezelni a kártyakibocsátóhoz tartozó biztonsági jellemzők következő listáját:

- AS.AUTH_MSK_STATUS /az MSK (a gyártó titkos kulcsa) hitelesítésének állapota/.

A felhasználói jellemzők meghatározása /kártya kibocsátó/ (FIA_ATD.1)

Az intelligens kártya képes kezelni a kártyakibocsátóhoz tartozó biztonsági jellemzők következő listáját:

- AS.CMLIFECYC /a Kártyamenedzser életciklus állapota/,
- AS.CMCONTEXT /a Kártyamenedzser kontextusa/,
- AS.KEYSET_VERSION /a kulcskészlet verziószáma/,
- AS:KEYSET_VALUE /a kulcskészlet értéke/.

A felhasználói jellemzők meghatározása /applet/ (FIA_ATD.1)

Az intelligens kártya képes kezelni az applethez tartozó biztonsági jellemzők következő listáját:

- ASG.APPPRIV /az applet privilégiumai/,
- AS.CURCONTEXT /az applet aktuális kontextusa/,

A titkok ellenőrzése /RSA kulcsgenerálás/ (FIA_SOS.1)

A biztonsági funkciók mechanizmust biztosítanak arra, hogy a kulcsgenerálás kielégítse a Miller-Rabin módszer titkokra vonatkozó metrikáját (véletlenszerűség-mértékét).

A titkok generálása a biztonsági funkciók által /véletlen generálás/ (FIA_SOS.2)

A biztonsági funkciók mechanizmust biztosítanak arra, hogy a véletlenszám generálás kielégítse a FIPS PUB 140-1 véletlen metrikáját (statisztikai próbákkal ellenőrzött véletlenszerűségét).
Az intelligens kártya (biztonsági funkciói segítségével) képes kikényszeríteni a véletlenszám generálás használatát az alábbi esetekben:

- a kártyagyártó hitelesítése,
- a kártya kibocsátó hitelesítése,
- a biztonságos csatorna menedzselése.

A hitelesítés időzítése (FIA_UAU.1)

A felhasználó hitelesítése előtt az intelligens kártya az alábbiakat engedi meg:
A rezidens alkalmazás számára:

- Get Challange,
- Get Data,
- Manage Channel,
- Select Applet.

A Kártyamenedzser számára:

- Get Data,
- Initialise Update.

Az intelligens kártya bármilyen további, általa közvetített tevékenységet csak akkor engedélyez, ha a felhasználó sikeresen hitelesítette magát.

Hamisíthatatlan hitelesítés /applet PIN kódok védelme/ (FIA_UAU.3)

A biztonsági funkciók megakadályozzák, hogy bármelyik felhasználó által hamisított hitelesítési adatot használhassanak fel.
A biztonsági funkciók megakadályozzák, hogy bármelyik másik felhasználó által lemásolt hitelesítési adatot használhassanak fel.

Egyszer használatos hitelesítési mechanizmusok (FIA_UAU.4)

A kártya gyártó és a kártya kibocsátó hitelesítése során a biztonsági funkciók megakadályozzák a hitelesítési adatok újrafelhasználását.

Védett hitelesítési visszajelzés /kártya gyártó/ (FIA_UAU.7)

A kártya gyártó hitelesítése során a biztonsági funkciók csak az alábbiakat biztosítják:

- véletlen (a hitelesítés véletlen „kihívás” értéke, melyre a hiteles választ várja),
- a hitelesítés eredménye.

Védett hitelesítési visszajelzés /kártya kibocsátó/ (FIA_UAU.7)

A kártya kibocsátó hitelesítése során a biztonsági funkciók csak az alábbiakat biztosítják:

- a kulcskészlet verziója,
- az induló kulcs index,
- a kártya által generált véletlen (a kártya által megkövetelt hitelesítés véletlen „kihívás” értéke, melyre a kibocsátótól a hiteles választ várja),
- kriptogram (mely azt jelzi, hogy a hitelesítés bemeneteként egy kulcsból és véletlenből számolandó kriptogramot kell használni),
- a hitelesítés eredménye.

Az azonosítás időzítése (FIA_UID.1)

A felhasználó azonosítása előtt az intelligens kártya az alábbiakat engedi meg:

- a Kártyamenedzser végrehajtása.

Az intelligens kártya bármilyen további, általa közvetített tevékenységet csak akkor engedélyez, ha a felhasználó sikeresen azonosította magát.

Felhasználó-szubjektum összekötés (FIA_USB.1)

A biztonsági funkciók a megfelelő felhasználói biztonsági jellemzőket összekapcsolják az adott felhasználó nevében tevékenykedő szubjektumokkal.

4.3.6 Biztonság kezelés

A biztonsági funkciók viselkedésének kezelése (FMT_MOF.1)

Az intelligens kártya a rezidens alkalmazás alábbi funkcióinak elérhetetlenné tételét (letiltását) csak az elő-megszemélyesítő számára teszi lehetővé:

- GET CHALLANGE,
- EXTERNAL AUTHENTICATE,
- LOAD STRUCTURE,
- INSTALL,
- LOAD APPLET,
- GET DATA.

A biztonsági jellemzők kezelése (FMT_MSA.1)

Az intelligens kártya képes a Pre_Personal hozzáférés ellenőrzés érvényre juttatásával az alábbi biztonsági jellemző módosítási lehetőségét az elő-megszemélyesítőre korlátozni:

- AS.MSKEY

Az intelligens kártya képes a CardManager hozzáférés ellenőrzés érvényre juttatásával az alábbi biztonsági jellemzők módosítási lehetőségét a Kártyamenedzserre korlátozni:

- AS.KEYSET_VERSION,
- AS.KEYSET_VALUE,
- AS.CMLIFECYC,
- Default selected privilege.

Az intelligens kártya képes a CardManager hozzáférés ellenőrzés érvényre juttatásával az alábbi biztonsági jellemzők törlési lehetőségét a Kártyamenedzserre korlátozni:

- AS.KEYSET_VERSION,
- AS.KEYSET_VALUE.

Az intelligens kártya képes az APPPRIV hozzáférés ellenőrzés érvényre juttatásával az alábbi biztonsági jellemző törlési lehetőségét az Applet_privilégium-ra korlátozni:

- AS.CMLIFECYC

Biztonságos biztonsági jellemzők (FMT_MSA.2)

Az intelligens kártya biztosítja, hogy biztonsági jellemzőknek csak biztonságos értékek kerülnek elfogadásra.

Statikus jellemző inicializálás (FMT_MSA.3)

Az intelligens kártya képes a CardManager hozzáférés ellenőrzés érvényre juttatásával korlátozó (default) alapértékeket biztosítani a kártya biztonsági politikáját érvényre juttató biztonsági funkciók számára.
Az intelligens kártya lehetővé teszi a megszemélyesítő számára, hogy a fenti korlátozó (default) alapértéket felülírja, amikor egy kulcskészlet kezdeti értékeit meghatározza.

A biztonsági funkciók adatainak kezelése (FMT_MTD.1)

Az intelligens kártya a megszemélyesítőre korlátozza a DAP (a kártyára töltött appletek és egyéb fájlok digitális aláírása) ellenőrzéséhez szükséges alábbi jellemzők módosításának lehetőségét:

- AS.CMID (Kártyamenedzser azonosító),
- AS.APID (applet azonosító),
- AS.KEYSET_VALUE (kulcskészlet értéke).

Az intelligens kártya a Kártyamenedzserre és az API_használóra korlátozza az alábbi jellemző lekérdezésének lehetőségét:

- AS.APID (applet azonosító).

Az intelligens kártya a Kártyamenedzserre korlátozza az alábbiak törlési lehetőségét:

- a biztonsági napló tartalma (az integritáshibák kivételével).

Megjegyzés: az utolsó funkció (napló törlés) csak akkor elérhető, ha a Kártyamenedzser nem SECURED és nem LOCKED állapotban van.

A biztonsági funkciók adataira vonatkozó korlátok kezelése /GLBPIN/ (FMT_MTD.2)

Az intelligens kártya a Kártyamenedzserre korlátozza az alábbi adatra vonatkozó korlát meghatározásának lehetőségét:

- D.NB_REMAINTRYGLB (a globális PIN kódra elfogadható sikertelen kísérletek számára)

Ha a sikertelen globális PIN kód megadási kísérletek elérik vagy meghaladják a megadott korlátot, az intelligens kártya blokkolja a globális PIN kódot.

A biztonsági funkciók adataira vonatkozó korlátok kezelése /OWNPIN/ (FMT_MTD.2)

Az intelligens kártya az API_használóra korlátozza az alábbi adatra vonatkozó korlát meghatározásának lehetőségét:

- D.NB_REMAINTRYOWN (az appletekhez tartozó PIN kódra elfogadható sikertelen kísérletek számára)

Ha a sikertelen appletekhez tartozó PIN kód megadási kísérletek elérik vagy meghaladják a megadott korlátot, az intelligens kártya blokkolja az adott (appletekhez tartozó) PIN kódot.

Biztonsági szerepkörök (FMT_SMR.1)

Az intelligens kártya képes az alábbi szerepkör kezelésére:

- SIGN_LOAD_FILE (a kártyára töltött fájl aláírója).

Az intelligens kártya képes összekapcsolni a felhasználókat a fenti szerepkörrel.

A biztonsági szerepkörökre vonatkozó korlátozások (FMT_SMR.2)

Az intelligens kártya képes az alábbi táblázatban feltüntetett szerepkörök kezelésére.
Az intelligens kártya képes összekapcsolni a felhasználókat az egyes szerepkörökkel.
Az intelligens kártya garantálja, hogy az alábbi táblázatban meghatározott feltételek teljesüljenek:

Szerepkörök	Feltételek
Elő-megszemélyesítő	(A kártya gyártó) sikeres hitelesítése a transport key-t (a gyártó titkos kulcsa) használva, és a kártya elő-megszemélyesítési állapotban van.
Megszemélyesítő	(A kártya gyártó vagy a kártya kibocsátó) sikeres hitelesítése a Kártyamenedzser egy kulcs készletét használva, és a Kártyamenedzser életciklus állapota OP_READY-ből SECURED-re változik.
Kártyamenedzser	(A kártya kibocsátó) sikeres hitelesítése a Kártyamenedzser egy kulcs készletét használva, és a Kártyamenedzser életciklus állapota OP_READY-ből SECURED-re változik.
API_használó	(Az applet) sikeres azonosítása, és az applet életciklus állapota SELECTABLE, vagy az utáni.
Applet_privilégium	A Kártyamenedzser életciklus állapotát, az ATR fájlokat és a globális PIN kódot csak egy privilegizált applet módosíthatja.

4.3.7 Magántitok

Megfigyelhetetlenség (FPR_UNO.1)

Az intelligens kártya garantálja, hogy egyetlen felhasználó sem képes megfigyelni az alábbi objektumokon az alábbi szubjektumok által végzett alábbi műveleteket:

Szubjektum	Művelet	Objektum
Applet	A PIN (megadott és letárolt) értékeinek összehasonlítása	D.GLPIN (globális PIN) D.OWNPIN (az appletekre vonatkozó PIN)
Applet	Importálás és használat	D.KEY (kulcsok)
Kártyamenedzser	Importálás és használat	D.KEY (kulcsok)
Applet	Két bájt rendező összehasonlítása	D.ARRAY (rendezők)

4.3.8 A biztonsági funkciók védelme

A biztonságos állapot megőrzése hiba esetén (FPT_FLS.1)

Az intelligens kártya megőriz egy biztonságos állapotot, ha a következő típusú hibák lépnek fel:

- „érvénytelen hivatkozás” kivétel,
- kód vagy adat integritás hiba,
- feldolgozás közbeni áramkimaradás.

Funkcionális helyreállítás (FPT_RCV.4)

Az intelligens kártya egy „megszakadás-ellenes” tulajdonságot biztosít, mely garantálja, hogy egy funkció vagy sikeresen befejeződik, vagy hiba esetén (véletlen áramkimaradás következik be egy tranzakció közben, vagy a PIN kódok ellenőrzését szándékos áramkimaradással, egyéb zavarással próbálják megkerülni) helyreállít egy biztonságos és ellentmondásmentes állapotot.

A biztonsági politika megkerülhetetlensége (FPT_RVM.1)

Az intelligens kártya biztosítja, hogy a biztonsági politikáját érvényre juttató funkciókat meghívták, s azok sikeresen befejeződtek, mielőtt bármely, az intelligens kártya hatóköréhez tartozó funkció elindulását engedélyezné.

Tartomány elkülönítés a biztonsági funkciók számára (FPT_SEP.1)

Az intelligens kártya egy biztonsági tartományt tart fenn biztonsági funkciói végrehajtására, amely megvédi ezeket a biztonsági funkciókat egy nem megbízható szubjektum kölcsönhatásától, illetve beavatkozásától.
Az intelligens kártya érvényre juttatja a hatókörén belüli szubjektumok biztonsági tartományainak elkülönítését.

Megjegyzés: Elkülönített biztonsági tartományai vannak a (szintén Java nyelven íródott) Kártyamenedzsernek és az appleteknek, illetve a különböző logikai csatornák ideiglenes adatainak.

A biztonsági funkció adatainak konzisztenciája biztonsági funkciók közötti átvitel során (FPT_TDC.1)

Az intelligens kártya biztonsági funkciói képesek konzisztensen értelmezni a kulcskészlet értékét (AS.KEYSET_VALUE), amikor azok megosztásra kerülnek egy másik megbízható informatikai termékkel.
Az intelligens kártya a PUT KEY adat formátumot használja, amikor egy másik megbízható informatikai terméktől (nevezetesen egy külső kulcs generátortól) kapott biztonsági funkció adatot értelmez.

A biztonsági funkciók tesztelése /Reset/ (FPT_TST.1)

Az intelligens kártya minden kártya reset-eléskor 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 biztonsági funkciókat végrehajtó kódok sértetlenségét ellenőrizni.

A biztonsági funkciók tesztelése /Card/ (FPT_TST.1)

Az intelligens kártya a kártyán lévő programok futtatása során 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 biztonsági funkciókat végrehajtó kódok sértetlenségét ellenőrizni.

4.3.9 Erőforrás hasznosítás

Maximális kvóták (FRU_RSA.1)

Az intelligens kártya egy kvóta érvényesítésével korlátozza az alábbi erőforrások maximális mennyiségét:

- az egy applet által (az applet teljes életciklusában) felhasználható EEPROM méret.

4.3.10 A CosmopolIC-hez való hozzáférés

A választható jellemzők korlátozása (FTA_LSA.1)

Az intelligens kártya az alábbi munkaszakasz biztonsági jellemzőkre korlátozza a munkaszakasz kulcsok (AS.SESSION_KEY) hatókörét:

- AS.KEYSET_VERSION (kulcskészlet verziószám),
- AS.KEYSET_VALUE (kulcskészlet érték),
- AS.CURCONTEXT (az aktuális kontextus),
- AS.LOGIC_CHANNEL_NB (a logikai csatornák /1-4-ig terjedő/ sorszáma)

4.3.11 Megbízható út/csatorna

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 megköveteli ennek a megbízható útvonalnak a használatát az alábbiakhoz:

- kulcskészlet betöltése,
- globális PIN megadása.

Megjegyzés: Az appleteknek is használniuk kell ezt a megbízható útvonalat az adatok és bájtkódok (appletek és az appleteket betöltő fájl) betöltéséhez, illetve az applet adatok, kulcsok és privilégiumok sértetlenségének ellenőrzéséhez.

5. A P8WE5033V0G 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 P8WE5033V0G mikrochip értékelését végző laboratórium[6] vizsgálta és igazolta.

5.1 A P8WE5033V0G 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[7]:

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[8].

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[9] (mialatt ezeket végrehajtják/feldolgozzák, illetve a mikrochip memóriájában tárolják).
3. A véletlen számok gyengesége.

---

[6] T-Systems ISS GmbH

[7] Valamennyi másodlagos értéknek a bizalmasságát és a sértetlenségét kell védeni.

[8] 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.

[9] 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 semmilyen információt nem 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:

- Triple-DES titkosítás és dekódolás,
- nagy számok aritmetikája (pl. az RSA számítások támogatásához).

5.2 A P8WE5033V0G 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[10] 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[11].

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 chip-ek 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[12].

[10] 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.
[11] 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.
[12] 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[13].

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[14].

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.

[13] 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.

[14] 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 inicializáló és elő-megszemélyesítő adatok nem-felejtő memóriáiban való tárolására. Az inicializáló 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.

Triple DES funkcionalitás
A mikrochip a beágyazott szoftver számára biztosítja a triple DES titkosítás és dekódolás funkcionalitást[15].

Moduláris aritmetika
A mikrochip a beágyazott szoftver számára biztosítja a nagy egész számokkal való moduláris műveletvégzések támogatását, elsősorban a moduláris hatványozást[16].

[15] A mikrochip biztosítja a felhasználói adatok (különösen a kriptográfiai kulcsok) bizalmasságát a Triple-DES műveletek során. Ezt támogatja „A működéssel járó információ kiszivárgás elleni védelem” biztonsági cél is.

[16] A mikrochip biztosítja a felhasználói adatok (különösen a kriptográfiai kulcsok) bizalmasságát az aritmetikai műveletek során, s ezt a megfelelő beágyazott szoftvereknek is támogatniuk kell. „A működéssel járó információ kiszivárgás elleni védelem” biztonsági cél támogatja a mikrochip részéről biztosított védelmet.

5.3 A P8WE5033V0G mikrochip környezetre vonatkozó biztonsági céljai

A hardver platform használata

Annak biztosítására, hogy a mikrochip biztonságos módon legyen felhasználva, az intelligens kártya beágyazott szoftverét úgy kell tervezni, hogy a következő dokumentumokból származó követelmények teljesüljenek:

- hardver adatlap a mikrochip-hez,
- a mikrochip-re vonatkozó alkalmazási megjegyzések, és
- a mikrochip-re vonatkozó értékelési beszámoló azon következtetései, amelyek az intelligens kártya beágyazott szoftvere szempontjából fontosak.

A felhasználói adatok kezelése

Az intelligens kártya beágyazott szoftverének úgy kell kezelnie a biztonság szempontjából fontos felhasználói adatokat (különös tekintettel a kriptográfiai kulcsokra), hogy az megfeleljen az egyedi alkalmazási körülmények biztonsági igényeinek.

Például az intelligens kártya beágyazott szoftverének nem szabad felfednie a biztonság szempontjából fontos felhasználói adatokat a jogosulatlan felhasználók vagy eljárások számára, amikor egy terminálon keresztül kommunikálnak.

Védelem a mikrochip fejlesztése és gyártása során

A mikrochip gyártójának biztosítania kell, hogy az intelligens kártya integrált áramkörének fejlesztése és gyártása biztonságos legyen olyan módon, hogy véletlenül (nem szándékosan) semmilyen információt se bocsássanak rendelkezésre 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 a feljogosított személyekre kell korlátozni,
- a selejtet meg kell semmisíteni.

Ez nemcsak a mikrochip-re vonatkozik, hanem minden információra és anyagra, amelyet az intelligens kártya beágyazott szoftverének fejlesztőjével kicserélnek, és így elsősorban magára az intelligens kártya beágyazott szoftverére.
A mikrochip-ekre vonatkozóan egy pontos azonosító rendszer van kialakítva, s minden mikrochip példány hordozza az ehhez szükséges egyedi azonosítót.

Védelem a tokozás, végső elkészítés és megszemélyesítés során

Biztonsági eljárásrendet kell használni a mikrochip szállítása után a végfelhasználóhoz történő leszállításig a mikrochip és annak gyártási, valamint teszt adatai bizalmasságának és sértetlenségének megőrzése céljából (bármilyen lehetséges másolás, módosítás, visszatartás, lopás vagy jogosulatlan felhasználás megakadályozása érdekében).

Az alábbi három biztonsági cél az intelligens kártya azon (4.-7.) életciklus szakaszaira vonatkozik, melyekben az intelligens kártya IC az alkalmazói szoftver felügyelete alatt áll.

Kulcsok generálása

Kulcs vagy kulcspár generálását bizalmas módon kell végrehajtani, egyúttal a generált kulcsoknak nagyon nagy valószínűséggel egyedieknek, valamint kriptográfiailag erőseknek kell lenniük. Ezen kívül egy magánkulcsra annak is teljesülnie kell, hogy nem származtatható a megfelelő nyilvános kulcsból[17].

Kulcs-függő funkciók

A kulcs-függő funkciókat a beágyazott szoftverben olyan módon kell végrehajtani, hogy ne legyenek kitéve a kriptográfiai kulcsokat kompromittáló támadásoknak, mint például az intelligens kártya IC által kisugárzásának vizsgálata.

Erős kulcsok használata

Az intelligens kártya beágyazott szoftverének csak megfelelő titkos kulcsokat szabad használnia (elegendően nagy kulcstérből, elegendő nagy entrópiával választva) a mikrochip által felkínált kriptográfiai funkciók bemeneteként.

[17] Ez a cél a beágyazott szoftver fejlesztési szakaszára vonatkozik, minthogy a belső kulcsgenerálás a beágyazott szoftver felügyelete alatt történik.

5.4 A P8WE5033V0G mikrochip funkcionális biztonsági követelményei

Az alábbiakban felsoroljuk a mikrochip védelmi profiljában szereplő funkcionális biztonsági követelményeket ***(vastag és dőlt betűvel megjelenítve,*** a Common Criteria által használt rövidítéseket is feltüntetve), majd alatta röviden kitérünk arra, hogy a P8WE5033V0G mikrochip hogyan felel meg az egyes követelményeknek.

5.4.1 A védelmi profil funkcionális biztonsági követelményei

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)[18].

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[19].

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[20].
A biztonsági funkciók szétválasztják a hatókörükbe tartozó szoftverek biztonsági tartományait.

Korlátozott képességek (FMT_LIM.1)

A mikrochip-et úgy tervezték, hogy képességei korlátozva legyenek[21], s így a "Korlátozott rendelkezésre állás"-sal együtt érvényre juttassa a következő politikát: *a mikrochip felhasználókhoz való leszállítása után a tesztelési lehetőségek kihasználása 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.*

[18] Ezek konkrét maghatározása csak a biztonsági funkciók nem nyilvános leírásában található meg.
[19] A konkrét hibatípusok listája csak a biztonsági funkciók nem nyilvános leírásában szerepelnek.
[20] 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.
[21] Bizonyos életciklus szakaszokban, pl. a gyártást követő részletes tesztelést követően.

Korlátozott rendelkezésre állás (FMT_LIM.2)

A mikrochip-et úgy tervezték, hogy rendelkezésre állása korlátozva legyen[22], s így a "Korlátozott képességek"-kel együtt érvényre juttassa a következő politikát: *a mikrochip felhasználókhoz való leszállítása után a tesztelési lehetőségek kihasználása 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.*

Napló tárolás (FAU_SAS.1)

A biztonsági funkciók a mikrochip szállítása előtt a tesztelő személyzet számára biztosítják annak lehetőségét, hogy inicializáló és elő-megszemélyesítő adatokat, illetve az intelligens kártya beágyazott szoftveréhez kiegészítéseket tároljanak a napló bejegyzésekben.

A fizikai támadásnak való ellenállás (FPT_PHP.3)

A mikrochip biztonsági funkciói ellenállnak a fizikai manipulációknak és fizikai szondázásnak[23] egy automatikus reagálás[24] útján úgy, hogy a mikrochip biztonsági politikája ne sérüljön[25].

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-processor) közötti átvitel során.

---

[22] 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.

[23] Nem tárgya jelen jelentésnek, hogy konkrétan mely biztonsági funkciók, s milyen fizikai támadási forgatókönyvekre készültek fel.

[24] 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.

[25] 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.

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-processor) 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.

A véletlenszámok minőségi mértéke (FCS_RND.1)

A mikrochip biztonsági funkciói egy olyan mechanizmust biztosítanak a véletlenszámok generálásához, mely kielégít egy meghatározott minőségi mértéket[27].

5.4.2 Kiegészítő biztonsági funkcionális követelmények

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

Kriptográfiai eljárás – Triple_DES (FCS_COP.1)

A mikrochip képes az alábbi kriptográfiai algoritmus szabványos[28] végrehajtására:

- 112 bites Triple-DES titkosító/dekódoló algoritmus.

Kriptográfiai eljárás – moduló hatványozás (FCS_COP.1)

A mikrochip képes az alábbi művelet szabványos végrehajtására:

- hatványozás moduló egy egész szám (1024 bit).

[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.

[27] A meghatározott konkrét minőségi mérték az alábbi: „Minden generált bájt legalább 7 bitnyi entrópiát biztosítson" a Shannon entrópia fogalma szerint.

[28] A szabvány, melynek az algoritmus megfelel: FIPS PUB 46-3

6. A CosmopolIC 2.1 V4 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 CosmopolIC 2.1 V4 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.2 A vizsgálatok megerősaítése
	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, a titkos és magánkulcsok tárolása, s több 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 P8WE5033V0G mikrochip 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 felhasználói 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 CosmopolIC intelligens kártya
/Oberthur Card Systems, France,
Philips Semiconductors GmbH, Germany/

tanúsítás tárgyát képező verziója

/mikrochip:	P8WE5033V0G,
nyílt platform:	CosmopolIC (2.1 V4 verzió),
alkalmazás (applet):	nem tárgya a tanúsításnak

a tanúsítás érvényességi feltételeinek[29] együttes teljesülése esetén

Biztonságos intelligens kártya platform,

mely különböző kriptográfiai szolgáltatást megvalósító alkalmazások (elektronikus aláírást, titkosítást, hitelesítést végző appletek) számára biztosít:

megbízható kriptográfiai alaptámogatást és
védett futtatási környezetet

[29] Lásd a 7.2 "Az eredmények érvényességi feltételei" alfejezet 1.-4. feltételeit.

7.2 Az eredmények érvényességi feltételei

A CosmopolIC 2.1 V4 intelligens kártya:

- „lefelé" egy igen általános, kriptográfiai funkcionalitást is támogató mikrochip-re épül,
- „felfelé" pedig különböző felhasználói alkalmazások futtatására alkalmas platformot, biztonságos futtatási környezetet biztosít.

Mindkét „irány" megbízhatóságát, biztonságosságát igen magas garanciaszinten elvégzett független értékelések és tanúsítások igazolják.

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

7.2.1 A mikrochip tanúsítási eredményének (teljesített) érvényességi feltételei

Az alábbi négy feltételt csak a teljesség kedvéért tekintjük át.
A mikrochip tanúsítványának alábbi érvényességi feltételeit, melyek a mikrochip-re platformot fejlesztőkre vonatkozó elvárásokat fogalmaznak meg, a későbbi értékelő/tanúsító szervezetek már figyelembe vették (teljesítettnek nyilvánították, vagy saját feltételeik közé is beépítették).

Védelem a tokozás, végső elkészítés és megszemélyesítés során

Biztonsági eljárásokat kell alkalmazni attól kezdődően, hogy a mikrochip gyártója leszállította a mikrochip-et az intelligens kártya platform fejlesztőinek, egészen a kártya végfelhasználónak való kézbesítésig (a mikrochip, valamint gyártási és teszt adatai bizalmasságának és sértetlenségének megőrzése céljából), hogy bármely lehetséges másolást, módosítást, visszatartást, lopást vagy jogosulatlan felhasználást megakadályozzanak.

A hardver platform használata

Az intelligens kártya beágyazott szoftverét úgy kell tervezni, hogy teljesüljenek a következő dokumentumokból származó követelmények:

- A mikrochipre vonatkozó útmutató dokumentumok,
- A mikrochip értékelési jelentésének azon megállapításai, amelyek az intelligens kártya beágyazott szoftverére vonatkoznak.

A felhasználói adatok kezelése

Minden felhasználói adatnak az intelligens kártya beágyazott szoftvere a birtokosa. Ezért a biztonság szempontjából fontos felhasználói adatokat (különösen a kriptográfiai kulcsokat) az intelligens kártya beágyazott szoftverének a speciális alkalmazási összefüggéseknek megfelelően kell kezelnie.

Kriptográfiai támogatás a beágyazott szoftver részére

A beágyazott szoftvert tartalmazó mikrochip-nek egy sor biztonsági funkciót kell biztosítania: DES és RSA primitívek, véletlenszám generálás, a kriptográfiai számításokat végző pufferek biztonságos törlése.

7.2.2 Az intelligens kártya platform tanúsítási eredménye érvényességi feltételei

1. Felhasználási környezet

Valamennyi érzékeny adat (kulcsok, PIN kódok, appletek) sértetlenségét és/vagy bizalmasságát védeni kell az intelligens kártya külső környezetében történő tárolás és továbbítás során (pl. a szoftver megszemélyesítése vagy az applet betöltése során).

2. Appletek fejlesztése

Az intelligens kártya platform telepítése után a kártyára töltött appletek fejlesztése során az appletek fejlesztésére vonatkozó „programozási útmutató” valamennyi szabályát be kell tartani.

Az appleteket oly módon kell fejleszteni, hogy azok megfelelő védelmet biztosítsanak saját érzékeny adataiknak[30].

Valamennyi utólag a kártyára töltött appletet a JavaCard specifikációknak megfelelő eszközökkel kell összeszerkeszteni, konvertálni és ellenőrizni. Alapvető fontosságú az appletek aláírása (DAP kiszámítása, mellékelése) is ebben a folyamatban.

3. Biztonságos csatorna alkalmazása

Az importált adatok sértetlenségének és bizalmasságának biztosítása érdekében a biztonságos csatornát használva, az adattitkosító funkciót kell alkalmazni.

4. A tanúsított verzió használata

Az applet fejlesztők és a végfelhasználók pontosan a tanúsítás tárgyát képező verziót használják:

- mikrochip: P8WE5033V0G,
- nyílt platform: CosmopolIC (2.1 V4 verzió).

[30] A mikrochip hardver védelmet biztosít a tárolt adatoknak. Az intelligens kártya platform megvédi az egyes appleteket a külvilág, illetve a többi applet irányából induló támadásoktól. Egyik előző komponens sem képes megvédeni ugyanakkor az érzékeny adatokat a saját appletjüktől. (Egy rosszul megírt applet kiadhatja pl. a külvilágnak az általa kezelt bizalmas adatokat.)

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

Certificat 2002/05: CosmopolIC 2.1 v4 JavaCard Open Platform Embedded Software version 1

Certification Report 2002/05: CosmopolIC 2.1 v4 JavaCard Open Platform Embedded Software version 1

CosmopolIC 2.1 v4 JavaCard Open Platform Security Target (EAL4+)

Certificate BSI-DSZ-CC-0199-2002: Philips Smart Card Controller P8WE5033V0G

Certificate Report BSI-DSZ-CC-0199-2002 for Philips Smart Card Controller P8WE5033V0G from Philips Semiconductors GmbH

Security Target Lite BSI-DSZ-CC-0199, version 1.6: Evaluation of the Philips P8WE5033V0G Secure 8-bit Smart Card Controller (EAL5+)

BSI-PP-0002-2001: Smart Card IC Platform Protection Profile (EAL5+)

Oberthur Card Systems: PKCS#11 Cryptoki library for AuthentIC

Oberthur Card Systems: GalactIC version 2.1 V2 Operating System Reference Guide

Oberthur Card Systems: GalactIC version 2.1 V2 Java Card 2.1 Open Platform 2.0.1 Application note Issue 01

9. Rövidítések

ANSI	American National Standards Institute
APDU	Application Protocol Data Unit
API	Application Programmer Interface
ATR	Answer for Reset
BIOS	Basic Interface for Operating System
BSI	Bundesamt für Sicherheit in der Informationstechnik
CAP	Converted APplet (file format)
CEN	European Comittee for Standardization
CPU	Central Processing Unit
DAP	Data Authentication Pattern
DES	Data Encryption Standard /FIPS PUB 46-3, FIPS PUB 74, FIPS PUB 81/
DPA	Differencial Power Attack
EAL	Evaluation Assurance Level
EEPROM	Electrically Erasable Programmable Read Only Memory
EU	European Union
FAT	File Allocation Table
FIPS PUB	Federal Information Processing Standards Publications
JCRE	Java Card Runtime Environment
IC	Integrated Circuit
IEC	International Electrotechnical Comission
I/O	Input/Output
ISO	International Organization for Standardization
IT	Information Technology
MAC	Message Authentication Code
MMU	Memory Management Unit
MSK	Manufacturer Secret Key
OP CS	Open Platform Card Specification
OS	Operating System
PIN	Personal Identification Number
PKCS	Public Key Cryptographic Standards
PKCS #11	Cryptographic Token Interface Standard
PP	Protection Profile
RAM	Random Access Memory
ROM	Read Only Memory
RSA	Rivest-Shamir-Adleman (public key cryptosystem) /ANSI X9.31/
SHA-1	Secure Hash Algorithm /FIPS PUB 180-1/
SPA	Simple Power Attack
SSCD	Secure Signature Creation Device (lásd BALE)
SSCD-PP	Secure Signature Creation Device – Protection Profile
TA	Timing Attack
Triple-DES	/FIPS PUB 46-3, ANSI X9.52/
TSF	TOE /Target of Evaluation/ Security Function
VOP	Visa Open Platform
VOP CS	Visa Open Platform Card Specification
BALE	Biztonságos aláírás-létrehozó eszköz