Tanúsítási jelentés

Hung-TJ-009-2003

Az SLE66CX320P mikrochip-ből
és a
MICARDO v 2.1 64/32 R1.0
operációs rendszerből álló
intelligens kártya
mint

biztonságos aláírás-létrehozó eszköz

/Infineon Technologies AG, Germany,
ORGA Kartensysteme GmbH, Germany/

Tartalom

1. Bevezetés

1.1 A tanúsítási jelentés tárgya

Jelen tanúsítási jelentés tárgya egy olyan intelligens kártya, mely egy SLE66CX320P mikrochip-et, s egy ebbe ágyazott MICARDO v 2.1 64/32 R1.0 operációs rendszert tartalmaz (a későbbiekben erre a termékre „**MICARDO**”-ként, illetve „**MICARDO intelligens kártya**”-ként hivatkozunk), s melyet minősített aláírás létrehozásához kívánnak felhasználni, mint biztonságos aláírás-létrehozó eszköz (BALE).

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

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

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

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

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,
- 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.”

A 3-as típusú BALE-re két Common Criteria szerinti védelmi profil is készült, a garanciális biztonság szempontjából egy szigorú és egy még szigorúbb változat:

- EAL4-es értékelés garancia szint (Protection Profile – Secure Signature-Creation Device Type 3, version: 1.05, EAL4),
- EAL4+ (emelt szintű) értékelési garancia szint (Protection Profile – Secure Signature-Creation Device Type 3, version: 1.05, EAL4+).

A MICARDO intelligens kártya nem rendelkezik a fenti védelmi profiloknak való megfelelőséget igazoló tanúsítvánnyal.

A fenti védelmi profilokban megalapozott, megfogalmazott és megindokolt követelményrendszer biztosan helyes szakmai lebontása és részletezése az EU direktíva és a hazai elektronikus aláírás törvény magas szinten megfogalmazott követelményeinek. Ugyanakkor az általános törvényi elvárásokat nem csak a fent említett két védelmi profil követelményeinek való megfeleléssel lehet teljesíteni.

1.2 A tanúsítási jelentés feladata

Jelen tanúsítási jelentés fő feladata annak megállapítása, hogy:

- a MICARDO intelligens kártyára vonatkozó értékelési és tanúsítási eredmények (a mikrochip-re és az operációs rendszerre létező ITSEC tanúsítványok) alapján ki lehet-e mutatni, hogy az megfelel a „BALE specifikus" védelmi profil követelményeinek is, s ezáltal alkalmas legalább az egyik minősített aláírás-létrehozáshoz való felhasználásra[3],
- az ITSEC tanúsítványok érvényessége, illetve a többi kielégítendő funkcionális és biztonsági követelmény teljesülése milyen korlátozásokat, feltételeket támaszt a MICARDO intelligens kártya 3-as típusú BALE-ként való felhasználására.

1.3 A tanúsítási jelentés hatóköre

Jelen tanúsítási jelentés hatóköre csak a biztonságos aláírás-létrehozó eszközként való felhasználhatóságra és ennek feltétel-rendszerének meghatározására szorítkozik.
Nem terjed ki a MICARDO egyéb tulajdonságaira (pl. titkosításra való felhasználhatóságára).

1.4 A tanúsítási jelentés szerkezete

A tanúsítási jelentés további szerkezete a következő:

- A 3-as típusú BALE-kre vonatkozó CC szerinti SSCD védelmi profil fontosabb elemei /biztonsági környezet (kivédendő veszélyek és érvényre

[3] S amennyiben megfelel, akkor melyiknek: az EAL4-es változatnak, vagy a még szigorúbb EAL4+ (emelt szintű) változatnak is?

juttatandó biztonsági szabályok), biztonsági célok, funkcionális és garanciális követelmények/ (2. fejezet).

- A MICARDO intelligens kártya néhány különleges tulajdonsága (3. fejezet).
- A MICARDO operációs rendszerére vonatkozó ITSEC tanúsítvány eredményei (4. fejezet).
- A MICARDO mikrochip-jére vonatkozó ITSEC tanúsítvány eredményei (5. fejezet).
- Az SSCD védelmi profil követelményeinek kimutatása a MICARDO intelligens kártya tulajdonságaiból, valamint az ITSEC tanúsítványok eredményeivel igazolt, kielégített követelményekből (6. fejezet).
- A minősített aláírás-létrehozáshoz való alkalmasság megállapítása, valamint az alkalmazás feltételeinek és korlátainak a meghatározása (7. fejezet).
- A jelen tanúsítási jelentéshez figyelembe vett dokumentumok jegyzéke (8. fejezet).
- Az alkalmazott rövidítések jegyzéke (9. fejezet).

2. Egy 3-as típusú BALE-re vonatkozó CC követelmények az SSCD védelmi profil szerint

Az alábbiakban áttekintjük annak az SSCD védelmi profilnak a fontosabb részeit (a környezetre vonatkozó állításokat, biztonsági célokat, funkcionális és garanciális követelményeket), melyeknek való megfelelőséget kívánjuk a MICARDO intelligens kártyára a későbbiekben kimutatni.

2.1 Egy 3-as típusú BALE biztonsági környezete

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

2.1.1 A biztonságra irányuló veszélyek

A fizikai környezet sebezhetőségének kihasználása

Egy támadó kölcsönhatásba lép a BALE-val abból a célból, hogy kihasználja a fizikai környezet sebezhetőségét, és ezzel a biztonságot veszélyezteti.

A magánkulcs letárolása, lemásolása

Az aláírás-létrehozó adat BALE-n kívüli tárolása vagy lemásolása veszélyt jelent az elektronikus aláírások jogi hitelességére.

Az aláírás-létrehozás adatok származtatása

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

Az aláírás-létrehozó adat kiszivárgása

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

Az elektronikus aláírás hamisítása

A támadó meghamisítja a BALE által készített elektronikus aláírással aláírt adatokat úgy, hogy azt nem észleli az aláíró vagy egy harmadik fél.

Az elektronikus aláírások letagadása

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

Az aláírás-ellenőrző adatok hamisítása

Egy támadó meghamisítja a BALE által szolgáltatott aláírás-ellenőrző adatot.

Az aláírandó adat reprezentánsának meghamisítása

Egy támadó módosítja az aláírás-létrehozó alkalmazás által küldött aláírandó adat reprezentánst, s így a BALE ténylegesen a módosított értéket írja alá.

Visszaélés a BALE aláírás-létrehozó funkciójával

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

2.1.2 Érvényre juttatandó biztonsági szabályok

Szakértő támadók

A BALE-t szándékosan támadhatják magas támadó képességgel rendelkező szakértők, akik részletes ismeretekkel rendelkeznek a BALE biztonsági alapelveiről, koncepcióiról. A BALE-nak védeni kell az aláírás-létrehozó adatot az ilyen támadásokkal szemben (is).

Minősített tanúsítvány

A hitelesítés-szolgáltató megbízható tanúsítvány-létrehozó alkalmazást használ arra, hogy minősített tanúsítványt állítson elő a BALE által generált aláírás-ellenőrző adathoz. A minősített tanúsítvány tartalmazza a jogszabályokban[4] meghatározott elemeket, köztük az aláíró nevét és az aláíró kizárólagos ellenőrzése alatt álló BALE-n implementált aláírás-létrehozó adatnak megfelelő aláírás-ellenőrző adatot[5]. A hitelesítés-szolgáltató a tanúsítvány vagy más nyilvánosan rendelkezésre álló információn keresztül biztosítja, hogy a BALE-nak az aláírással kapcsolatos használata nyilvánvaló legyen.

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

A rendszer teljes életciklusára kiterjedő biztonság

Az informatika biztonság szempontjait a BALE és az aláírás-létrehozó adat teljes életciklusában figyelembe kell venni.

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

A BALE, mint biztonságos aláírás-létrehozó eszköz

A BALE az aláírás létrehozáshoz használt aláírás-létrehozó adatot az aláíró kizárólagos ellenőrzése alatt implementálja. Az aláírás létrehozásra szolgáló aláírás-létrehozó adat gyakorlatilag csak egyszer fordulhat elő.

2.2 Egy 3-as típusú BALE biztonsági céljai

Fizikai kisugárzás elleni védelem

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

Aláírás-létrehozó / aláírás-ellenőrző adatpárok generálása

A BALE-nak biztosítania kell, hogy az aláírás-létrehozó / aláírás-ellenőrző adatpár generálását csak feljogosított felhasználók válthassák ki.

Az életciklus biztonsága

A fejlesztőnek a BALE fejlesztési fázisa során eszközöket, technikákat és biztonságos körülményeket kell biztosítania. A BALE-nak támogatnia kell a hitelesítés-szolgáltatót és az aláírót abban, hogy az üzemeltetési fázis során észleljék és pótolják a hiányosságokat. A BALE-nak biztonságos aláírás-létrehozó adat megsemmisítési technikákat kell nyújtania.

Az aláírás-létrehozó adatok titkossága

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

Az aláírás-ellenőrző és az aláírás-létrehozó adat közötti megfelelés

A BALE-nak biztosítania kell az aláírás-ellenőrző és az aláírás-létrehozó adat közötti megfelelést, amikor ezeket előállítja. A BALE-nak igény esetén bizonyítania kell a megfelelést az általa tárolt aláírás-létrehozó adat és a számára elküldött aláírás-ellenőrző adat között.

Az aláírás-ellenőrző adat hitelességének biztosítása

A BALE-nak eszközöket kell nyújtania arra, hogy lehetővé váljon a tanúsítvány-létrehozó alkalmazás számára a BALE által exportált aláírás-ellenőrző adat hitelességének ellenőrzése.

A módosítás detektálása

A BALE-nak rendszer szintű tulajdonságokat kell biztosítania, amelyekkel a rendszer komponensek fizikai módosításait észlelni lehet, egyúttal ezeket a tulajdonságokat alkalmaznia kell a biztonság megszegésének korlátozására.

A fizikai módosítással szembeni ellenállás
A BALE akadályozza meg a speciális rendszer eszközök és komponensek fizikai módosításait, vagy álljon ellen ezeknek.

Az aláírás-létrehozó adatok egyedisége

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

Az aláírandó adat-reprezentáns sértetlenségének ellenőrzése

A BALE-nak ellenőriznie kell, hogy az aláírás-létrehozó alkalmazásból származó aláírandó adat-reprezentáns nem lett-e módosítva az aláírás-létrehozó alkalmazás és a BALE közötti átvitel során. Az intelligens kártyának biztosítania kell azt is, hogy önmaga se módosítsa az aláírandó adat-reprezentánst.

Az aláírás előállítási funkció csak a törvényes aláírónak áll rendelkezésre

A BALE-nak az aláírás előállítási funkciót csak a törvényes aláíró számára szabad biztosítania, és védenie kell az aláírás-létrehozó adatot a mások általi felhasználással szemben. Az intelligens kártyának ellen kell állnia a magas támadási potenciállal rendelkező támadásoknak is.

Az elektronikus aláírás kriptográfiai biztonsága

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

2.3 Egy 3-as típusú BALE funkcionális biztonsági követelményei

Az alábbiakban felsorolt funkcionális biztonsági követelmények kielégítése esetén a BALE:

- kivédi a biztonságra irányuló veszélyeket (2.1.1),
- érvényre juttatja a biztonsági szabályokat (2.1.2), egyúttal
- megvalósítja a biztonsági célokat (2.2).

Az alábbi táblázat összefoglalja a 3-as típusú BALE-kra vonatkozó SSCD védelmi profil funkcionális biztonsági követelményeit.

Funkcióosztályok	Funkció családok és összetevők
Biztonsági naplózás	---
Kommunikáció	---
Kriptográfiai támogatás	FCS_CKM.1 Kriptográfiai kulcs generálás
	FCS_CKM.4 Kriptográfiai kulcs megsemmisítés
	FCS_COP.1 Kriptográfiai eljárás
A felhasználói adatok védelme	FDP_ACC.1 Részleges hozzáférés ellenőrzés
	FDP_ACF.1 Biztonsági jellemzőkön alapuló hozzáférés ellenőrzés
	FDP_RIP.1 Részleges maradvány információ védelem
	FDP_SDI.2 A tárolt adatok sértetlenségének figyelése és beavatkozás
	FDP_UIT.1 Az adatcsere sértetlensége
Azonosítás és hitelesítés	FIA_AFL.1 A hitelesítési hiba kezelése
	FIA_ATD.1 A felhasználói jellemzők meghatározása
	FIA_UID.1 Az azonosítás időzítése
	FIA_UAU.1 A hitelesítés időzítése
Biztonság kezelés	FMT_MOF.1 A biztonsági funkciók viselkedésének kezelése
	FMT_MSA.1 A biztonsági jellemzők kezelése
	FMT_MSA.2 Biztonságos biztonsági jellemzők
	FMT_MSA.3 Statikus jellemző inicializálás
	FMT_MTD.1 A biztonsági funkciók adatainak kezelése
	FMT_SMR.1 Biztonsági szerepkörök
Magántitok	---
A biztonsági funkciók megbízható védelme	FPT_AMT.1 Az absztrakt gép tesztelése
	FPT_EMSEC.1 A BALE kisugárzása
	FPT_FLS.1 A biztonságos állapot megőrzése hiba esetén
	FPT_PHP.1 A fizikai támadások passzív észlelése
	FPT_PHP.3. A fizikai támadásokkal szembeni ellenálló képesség
	FPT_TST.1 A biztonsági funkciók tesztelése
Erőforrás hasznosítás	---
Az értékelés tárgyához való hozzáférés	---
Megbízható útvonal /csatorna	FTP_ITC.1 Megbízható csatorna
	FTP_TRP.1 Megbízható útvonal

2.4. Egy 3-as típusú BALE garanciális biztonsági követelményei

Egy 3-as típusú BALE-re vonatkozó, a fejlesztőktől független ellenőrző vizsgálat garancia szintje **EAL4-es** vagy emelt **EAL 4**-es /módszeresen tervezett, vizsgált és átnézett rendszer/.

Az alábbi táblázat összefoglalja az EAL 4-es (illetve az emelt EAL 4-es**,** /EAL4+/) szintű értékelés garanciaosztályait és garancia komponenseit.

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

3. A MICARDO speciális tulajdonságai

A MICARDO legfontosabb tulajdonságait a 4.2 - 4.5 alfejezetek részletezik.
Az alábbiakban csak azokat a jellemzőit emeljük ki, melyek alapvetően megkülönböztetik más intelligens kártyáktól (pl. a nyílt Java platformot alkalmazó megoldásoktól), s melyek jelen tanúsítás szempontjából lényegbe vágóak.

A MICARDO intelligens kártya fő alkotóelemei az alábbiak:
- chip
- operációs rendszer,
- fájl rendszer.

A MICARDO nem támogat kártyán tárolt végrehajtható kódokból álló alkalmazásokat.
Az alkalmazásokat kizárólag a host oldalról kiadott, szabványos (és az operációs rendszer által támogatott, értelmezett és a chip segítségével végrehajtott) parancsok megfelelő sorozatával lehet megvalósítani. Ez a filozófiai megközelítés bizonyos szempontból növeli a felhasználhatóság rugalmasságát, ugyanakkor számos biztonsági veszélyt is okoz, mivel a host oldalról akár nem biztonságos konfigurálások is beállíthatók, elérhetők.

Biztonsági attribútumokat csak az adminisztrátor hozhat létre, módosíthat.
/A perszonalizáció során beállítható (és beállítandó) minden olyan attribútum, mely később kikényszeríti a helyes (biztonságos) működést./

A MICARDO által kezelt (ISO 7816-4 –nek megfelelő) fájlrendszer egy mester fájlból (MF) /gyökér/ és több dedikált fájlból /DF, könyvtár, alkönyvtár/, illetve elemi fájlból /EF, adatokat tartalmazó fájl/ áll.
Az operációs rendszer az ezekhez való hozzáférést kontrollálja. A fájlrendszer minden fájlját egy biztonsági tulajdonság (attribútum) védi.
A hierarchikusan strukturált fájlrendszer egy mesterfájllal indul, mint gyökér.
Egy dedikált fájl egy vagy több dedikált és elemi fájlt tartalmazhat.
Az elemi fájlok felhasználói adatokat (munka fájl) vagy biztonsági tulajdonságokat, kulcsokat és jelszavakat (belső fájl) tartalmazhatnak. Egy elemi fájl egy hivatkozási fejrészből, biztonsági attribútumból és adatokból áll. Az alkalmazások parancsok segítségével elérhetik az elemi fájlokat.

Minden alkalmazásnak létrehozható egy saját könyvtár (DF) az intelligens kártyán, mely az alkalmazás-specifikus személyi adatokat (kulcsok, jelszavak, felhasználó azonosítók) tárolja.
Az alkalmazás forgalmazója felelős annak biztosításáért, hogy az alkalmazás használható és perszonalizálható legyen[6].

[6] A MICARDO nem ellenőrzi a CREATE FILE, UPDATE BINARY, APPEND RECORD és UPDATE RECORD parancsok végrehajtása során az adatok tartalmát!

4. A MICARDO operációs rendszerére vonatkozó ITSEC tanúsítvány eredményeinek összefoglalása

A MICARDO v2.1 intelligens kártya operációs rendszert egy informatikai termékek (ITSEC és CC szerinti) értékelésére Németországban akkreditált laboratórium[7] megvizsgálta, értékelte és tesztelte egy termékspecifikus (a MICARDO-ra külön kidolgozott) biztonsági előirányzat (Security Target) követelményeinek való megfelelőség szempontjából:

4.1 Az ITSEC értékelés eredményei

Az értékelés sikerrel zárult. Az értékelés megerősítette, hogy a biztonságot érvényre juttató funkciók a biztonsági előirányzatnak megfelelően működnek.
Az értékelés megcélzott **E4-es** szintje teljesül, az ellenőrzött biztonsági mechanizmusok minimális erőssége: **magas**.

Annak érdekében, hogy a fenti pozitív eredmény egy másik követelményrendszernek (CC SSCD védelmi profil) való megfelelőség kimutatásához is használható legyen, az alábbiakban áttekintjük az ITSEC értékelés (s ezzel a MICARDO termék) legfontosabb részleteit is.

4.2 Megvédett értékek

Az alábbi objektumok állnak védelem alatt:
- parancsok,
- image (az operációs rendszer és a kezdeti fájlrendszer EEPROM része, mely a gyártási szakaszban kerül az intelligens kártyára)
- dedikált fájlok (könyvtárak),
- elemi fájlok (adatfájlok),
- biztonsági tulajdonságok (attribútumok),
- kulcsok,
- jelszavak,
- felhasználói adatok.

Az alábbi alanyokat különböztetjük meg:
- adminisztrátor (új dedikált és elemi fájlokat hozhat létre, új alkalmazásokat vehet fel a kártyán, meghatározhatja az alkalmazások jogos felhasználóit),
- végfelhasználó (meghatározott hozzáférése van egy vagy több alkalmazáshoz (a MICARDO képes több végfelhasználót is kezelni egy kártyán), ha egy végfelhasználó dedikált vagy elemi fájlokat hozhat létre egy alkalmazáson belül, akkor őt adminisztrátorként kezelik).

Az alábbi hozzáférési típusokat különböztetjük meg:
A dedikált fájlokhoz való hozzáférés típusok:
- kiválasztás,
- létrehozás és törlés,

[7] a TÜV IT GmbH.

- aktivizálás, deaktivizálás.

Az elemi fájlokhoz való hozzáférés típusok:

- kiválasztás,
- létrehozás és törlés,
- olvasás és (tartalom) keresés,
- (tartalom) hozzáillesztés,
- (tartalom) módosítás,
- aktivizálás, deaktivizálás.

A titkokhoz való hozzáférés típusok:

- belső és külső hitelesítés,
- a (hozzáférési kísérleteket) számláló törlése,
- a hivatkozási adat módosítása,
- ellenőrzés,
- egyéb parancs-specifikus hozzáférések (pl. digitális aláírás számolás, dekódolás).

A következő táblázat összefoglalja a hozzáférési módokat:

	adminisztrátor	**végfelhasználó**
parancsok	---	végrehajtás
image[8]	---	---
dedikált fájlok	kiválasztás létrehozás/törlés aktivizálás/deaktivizálás	---
elemi fájlok	kiválasztás létrehozás/törlés aktivizálás/deaktivizálás	---
biztonsági attribútumok	módosítás, hozzáillesztés	olvasás/keresés
kulcsok	használat, módosítás, hozzáillesztés	használat, módosítás, hozzáillesztés
jelszavak	használat, módosítás	használat, módosítás
felhasználói adatok	olvasás/keresés, módosítás, hozzáillesztés	olvasás/keresés, módosítás, hozzáillesztés

4.3 Kivédett fenyegetések

Az ITSEC értékelés megerősítette, hogy a MICARDO intelligens kártya kivédi az alábbi fenyegetéseket.

T1 Az értékek jogosulatlan felfedése

T1.1: Védett objektumokhoz való jogosulatlan hozzáférés, a hozzáféréshez szükséges titok ismerete nélkül.

T1.2: Rejtett csatornák vizsgálata, tárolt adatok vagy titkok (pl. kulcsok) felfedése céljából.

[8] az operációs rendszer és a kezdeti fájlrendszer EEPROM része, mely a gyártási szakaszban kerül az intelligens kártyára

T1.3: A felhasználó és az intelligens kártya közötti kommunikáció során továbbított adatok vagy titkok elfogása.

T2 Az értékek jogosulatlan módosítása

T2.1: Védett objektumokhoz való jogosulatlan hozzáférés, a hozzáféréshez szükséges titok ismerete nélkül, az értékek módosítása céljából.

T2.2: Továbbított adatok vagy titkok észrevétlen (szándékos vagy véletlen) módosítása.

T2.3: Az intelligens kártyán tárolt adatok észrevétlen véletlen módosítása.

T2.4: Az intelligens kártyán generált adatok észrevétlen módosítása más adatok vagy titkok (pl. digitális aláírások, titkos kulcsok) felfedése vagy hamisítása céljából.

T2.5: Jogosulatlan objektumok tárolása a hozzá tartozó titkok ismerete nélkül, az értékek módosítása céljából.

T2.6: Az intelligens kártyán tárolt adatok észrevétlen szándékos módosítása.

T3 Az értékek jogosulatlan használata

T3.1: Védett objektumokhoz való jogosulatlan hozzáférés, a hozzáféréshez szükséges titok ismerete nélkül, az értékek eltulajdonítása vagy a velük való visszaélés céljából.

4.4 Teljesített biztonsági célok

Az ITSEC értékelés megerősítette, hogy az alábbi biztonsági célok megvalósulnak.

SO1 Jogosult hozzáférés

A MICARDO védje meg objektumait a jogosulatlan hozzáféréstől. Minden objektumhoz a hozzáférés csak a meghatározott biztonsági jellemzőknek (különösen a hozzáférési feltételeknek) megfelelő elvárt módon legyen lehetséges.

SO2 Ellenállás a fizikai támadásoknak

Ne legyen lehetséges az intelligens kártyán tárolt vagy feldolgozott adatok (különösen a magán aláíró kulcsok) felfedése, vagy észrevétlen módosítása. A MICARDO védjen minden ismert hardver támadás ellen, hatékonyan alkalmazva a hardver (mikrochip) által biztosított valamennyi mechanizmust.

SO3 Memória védelem

A MICARDO védje meg a memóriákban tárolt vagy feldolgozott valamennyi objektumot a jogosulatlan hozzáférés, elrontás és módosítás ellen. Erőforrás visszavétel (deallkokáció) után a memória semmilyen információt ne tartalmazzon az előzőleg ott tárolt adatokról.

SO4 A kriptográfia műveletek biztonsága

A MICARDO garantálja, hogy a kriptográfiai műveletek során aktivizált egyetlen kulcsot se lehessen felfedni, s ne lehessen a feldolgozott adatokra se következtetni. A kriptográfiai műveletek során bekövetkező bármilyen adatmódosítás észlelhető legyen. A digitális aláíró funkció úgy működjön, hogy az aláíró magánkulcsa ne legyen származtatható az aláírásból, s e titkot nem birtokló más egyén ne generálhasson aláírást. A kártyán tárolt titkos kulcsról az aláírási folyamat során se lehessen információt nyerni.

SO5 A továbbított adatok sértetlensége és hitelessége

A kommunikáció során továbbított adatok és titkok sértetlensége és hitelessége védve legyen.

SO6 A továbbított adatok bizalmassága

A kommunikáció során továbbított adatok és titkok bizalmassága védve legyen.

SO7 A kulcsgenerálás minősége

Minden felhasznált kulcs kriptográfiai minőség szempontjából erős legyen. Ez vonatkozik a MICARDO által generált valamennyi kulcsra is. A generált titkos kulcsok nagyon nagy valószínűséggel egyediek és kriptográfiailag erősek legyenek. A felhasználó magán aláíró kulcsát lehetetlen legyen kiszámolni nyilvános párjából.

SO8 Az EEPROM-ba töltött konfigurációs adatok hitelessége

Az inicializálás során betöltött konfigurációs állomány (image) hiteles legyen, esetleges módosulása detektálódjon.

4.5 A biztonságot érvényre juttató funkciók (biztonsági funkciók)

Az ITSEC értékelés megerősítette az alábbi biztonsági funkciók helyes működését.

SF1 Ellenőrzés és hitelesítés

Az SF1 biztonsági funkció a felhasználók (szubjektumok) ellenőrzését és hitelesítését teszi lehetővé, bizonyos objektumokhoz való hozzáférés engedélyezése érdekében. A sikeres ellenőrzés és hitelesítés után a szubjektum hozzáférhet a kártyán tárolt bizonyos objektumokhoz.

SF1.1 Kulcs alapú felhasználó hitelesítés

SF1.1 a felhasználó vagy az intelligens kártya, illetve mindkettő ellenőrzését és hitelesítését teszi lehetővé egy véletlenszámokat és kriptográfiai kulcsokat felhasználó kérdés/felelet eljárással.
SF1.1 észleli, ha egy előre meghatározott számú sikertelen hitelesítési kísérlet következett be bármely kulcs alapú hitelesítési eljárásban, ennek túllépése esetén érvényteleníti a megfelelő kulcsot.
Beállítható egy ún. „felhasználás számláló" értéke, mely erre a darabszám értékre korlátozza a kulcs lehetséges felhasználását. Meghaladása esetén a megfelelő kulcsot érvényteleníti.

SF1.2 Jelszó alapú felhasználó hitelesítés

SF1.2 összehasonlítja a felhasználó által megadott jelszót (vagy PIN-t) egy a kártyán tárolt titkos referencia értékkel.
SF1.1 észleli, ha egy előre meghatározott számú sikertelen hitelesítési kísérlet következett be, bármely jelszó alapú hitelesítési eljárásban, ennek túllépése esetén blokkolja a megfelelő jelszót. Ilyenkor csak egy reset funkció állíthatja vissza a számláló kiindulási értékét a blokkolás feloldására.
Beállítható egy ún. „felhasználás számláló" értéke, mely erre a darabszám értékre korlátozza a jelszó lehetséges felhasználását. Csak egy jelszócsere funkció állíthatja vissza a számláló kiindulási értékét a blokkolás feloldására, melynek során új jelszót kell megadni.
A titkos jelszó megvédhető (titkosított üzenetváltással) kártyára továbbítása során.

SF2 Hozzáférés ellenőrzés

SF2.1 A hozzáférés ellenőrzés menedzselése

SF2.1 az adminisztrátorra korlátozza a biztonsági attribútumok létrehozásának, módosításának és törlésének lehetőségét.
SF2.1 az alábbi szempontokból menedzseli az egyes objektumokhoz való hozzáférést:

- hozzáférési szabályok,
- felhasználási cél,
- életciklus állapot.

A hozzáférési szabályok fájlokra, kulcsokra és jelszavakra vonatkozhatnak, a hozzáférés típusát és feltételét meghatározva.
A hozzáférés lehetséges típusait 4.2 megadta.

A hozzáférés feltételei azt határozzák meg, hogy egy végrehajtandó parancs hozzáférhet-e egy adott objektumhoz. Lehetséges értékei:
- mindig (nincs feltétel),
- soha,
- sikeres jelszó alapú felhasználói hitelesítés után,
- sikeres kulcs alapú felhasználói hitelesítés után,
- hitelességet és sértetlenséget biztosító titkos üzenetváltás esetén,
- bizalmasságot biztosító titkos üzenetváltás esetén,
- egyéb, parancs-specifikus feltételek esetén.

A fenti értékek (logikai „vagy", illetve „és" műveletekkel) kombinálhatók, logikai kifejezésbe vehetők.
Hozzáférni csak olyan objektumhoz lehet, melyhez (létrehozásakor) az adminisztrátor csatolt egy hozzáférési szabályt is. A hozzáférés csak akkor lehetséges, ha a hozzáférési szabály teljesül (a logikai kifejezés „igaz" értékű). Egy hozzáférési szabály eltörlése esetén az adott objektumhoz többé nem lehet hozzáférni.

A felhasználás cél kulcsok esetén a lehetséges másik hozzáférést vezérlő szempont.
Egy kulcsra a következő felhasználási célok jelölhetők meg:
- külső hitelesítés,
- digitális aláírás számítása,
- dekódolás,
- belső hitelesítés,
- a titkos üzenetváltásnál kriptográfiai kontrollösszeg képzés,
- a titkos üzenetváltásnál titkosítás.

Az életciklus állapot valamennyi fájl esetén a lehetséges harmadik hozzáférést vezérlő szempont. Az életciklus állapot lehetséges két értéke a következő:
- aktivizált (működésre alkalmas és adatai /elvben/ hozzáférhetőek) ,
- deaktivizált (működésre alkalmas, de adatai nem hozzáférhetőek).

Az életciklus állapot nem törölhető, értékét csak az adminisztrátor változtathatja meg.

SF2.2 Biztonsági attribútum alapú hozzáférés ellenőrzés

SF2.2 érvényre juttatja a hozzáférési szabályok, felhasználási cél, és életciklus állapot által meghatározott hozzáférés politikát (kiértékelve azok aktuális értékét, megengedi vagy megtiltja az éppen igényelt hozzáférést).

SF3 Adat sértetlenség

SF3.1 A tárolt adatok sértetlenségének monitorozása, szükség esetén közbelépés

SF3.1 az intelligens kártyán elemi (EF) és dedikált (DF) fájlokban tárolt valamennyi felhasználói adatot folyamatosan figyeli a következő attribútumok alapján:
- a minden fájl fejrészéhez csatolt ellenőrző összeg (CRC),
- a fájlok adattartalmára számolt, s ehhez csatolt ellenőrző összeg (CRC).

Adat integritás hiba észlelése esetén SF3.1 értesíti a felhasználót a hibáról.
Fejrész ellenőrző összeg hiba esetén a fájlban tárolt felhasználói adathoz nem lehet többé hozzáférni.

SF4 Adat hitelesség

SF4.1 Adat hitelesítés

SF4.1 az alábbi objektumok hitelességét képes ellenőrizni:

- image (az operációs rendszer és a kezdeti fájlrendszer EEPROM része, mely a gyártási szakaszban kerül az intelligens kártyára)

A fenti objektumot csak akkor lehet használni, ha hitelességét egy hitelesítő kód segítségével ellenőrzik.

SF5 Adat csere

SF5.1 Adat csere bizalmasság

SF5.1 biztosítja a felhasználó és az intelligens kártya között kicserélt titkos adatok bizalmasságának megteremthetőségét a továbbítás során. Ennek érdekében kriptográfiai kulcsokon alapuló rejtjelezést alkalmaz az adatokra. A felhasznált kulcsokat vagy egy felhasználó tölti rá a kártyára, vagy a felhasználó hitelesítése során generálódnak (session key).

SF5.2 Adat csere hitelesség és sértetlenség

SF5.2 biztosítja a felhasználó és az intelligens kártya között kicserélt titkos adatok hitelességének és sértetlenségének megteremthetőségét a továbbítás során. Ennek érdekében kriptográfiai kulcsokon alapuló kriptográfiai ellenőrzőösszeg képzést alkalmaz ebből a célból. A felhasznált kulcsokat vagy egy felhasználó tölti rá a kártyára, vagy a felhasználó hitelesítése során generálódnak (session key).

SF6 Objektum újrahasználat

SF6.1 Maradvány információ védelem

SF6.1 biztosítja, hogy egy erőforrás minden előző információ tartalma közvetlen törlésre kerüljön a következő objektumok deallokálása során:

- valamennyi elemi és dedikált fájl,
- a titkos kulcsok és egyéb titkok számítására használt felejtő memóriák.

SF7 Fizikai védelem

SF7.1 Hardver hiba elleni védelem

SF7.1 megőriz egy biztonságos állapotot, a következő típusú hibák bekövetkezése esetén:

- egy parancs végrehajtása során bekövetkező átmeneti vagy folyamatos hardver hiba,
- fizikai támadás.

SF7.1 úgy reagál a fenti hibák észlelésekor, hogy a biztonság politika ne sérüljön (pl. az intelligens kártya megnyitott munkaszakasza ne maradjon használható a továbbiakban).

SF7.1 hardver alapú (a chip által támogatott) biztonsági funkciókat és az ezeknek megfelelő mechanizmusokat használ a hardver hibák monitorozására és a biztonságos állapot érvényre juttatására.

SF7.2 Rejtett csatorna vizsgálat ellenőrzés

SF7.2 kezeli az összes olyan hardver alapú (a chip által támogatott) biztonsági mechanizmust, mely felhasználható a rejtett csatornák elemzésének a megakadályozására (mint amilyen az egyszerű és a differenciál áramfelvételi támadás /SPA és DPA/).
SF7.2 az intelligens kártya valamennyi kriptográfiai műveletét támogatja ezekkel a hardver mechanizmusokkal. SF7.2 biztosítja, hogy valamennyi rendelkezésre álló szoftver és hardver ellenintézkedés egymást kiegészítve és támogatva működjön.
SF7.2 kikényszeríti, hogy egy biztonságos munkaszakasz (secure session) épüljön ki, még mielőtt bármilyen kriptográfiai kulcs felejtő memóriába töltődne, illetve bármilyen kriptográfiai művelettel feldolgozásra kerülne.

SF8 Kriptográfiai működés

SF8.1 Kriptográfiai kulcsgenerálás

SF8.1 512 – 1024 bites RSA kulcsokat képes generálni. Biztosítja az alábbiakat:
- a kulcsgeneráláshoz felhasznált véletlen számok jó véletlenszerűségi tulajdonságai garantálják, hogy nagy valószínűséggel egyedi kulcsok keletkeznek,
- a kulcsgeneráláshoz felhasznált prímszámok nagy valószínűséggel egyediek (mind különbözők),
- egyetlen magánkulcs sem határozható meg a megfelelő nyilvános kulcsból.

SF8.1 úgy működik, hogy csak kriptográfiailag erős kulcsok generálódnak (a meghatározott kulcsméret mellett).

SF8.2 A digitális aláírások számítása

SF8.1 egy digitális aláírás funkcionalitást biztosít. Ez a digitális aláírás funkcionalitás úgy működik, hogy az intelligens kártyán tárolt és a digitális aláíráshoz felhasznált titkos (magán)kulcsra nem lehet következtetni a digitális aláírás képzéséből. Egyúttal a magánkulcs nem következtethető ki az aláírásból, s a titkos magánkulcsot nem birtoklók nem is generálhatnak aláírást.

5. A MICARDO mikrochip-jére vonatkozó ITSEC tanúsítvány eredményeinek összefoglalása

5.1 Az ITSEC értékelés eredményei

Az SLE66CX320P / m1421b25 mikrochip értékelését végző laboratórium[9], illetve a tanúsítást kiállító BSI[10] legfontosabb megállapításai az alábbiak:

Az értékelés sikerrel zárult. Az értékelés megerősítette, hogy a biztonságot érvényre juttató funkciók a biztonsági előirányzatnak (Security Target) megfelelően működnek.
Az értékelés megcélzott **E4-es** szintje teljesül, az ellenőrzött biztonsági mechanizmusok minimális erőssége: **magas**.

5.2 A mikrochip legfontosabb tulajdonságai

Bár a mikrochip értékelési eredményeit a MICARDO v2.1 operációs rendszer értékelésénél és tanúsításánál figyelembe vették és beépítették, a MICARDO BALE követelményeknek való megfelelése kimutatásánál a későbbiekben szükségünk lesz néhány hardver-specifikus értékelési eredményre (ellenőrzött biztonsági funkcióra). Ezért röviden áttekintjük a mikrochip összetevőit és fő biztonsági funkcióit.

A MICARDO intelligens kártya alapját az Infineon SLE66CX320P / m1421b25 típusú mikrochip-je biztosítja.

Az SLE66CX320P mikrochip hardver alkotó elemei

- biztonsági logika,
- ECO 2000 típusú központi feldolgozó egység (CPU),
- memória rejtjelző és dekódoló egység (MED)
- memóri kezelő egység (MMU),
- memóriák:
  - RAM (256 bájt IRAM, 2 Kbájt XRAM)
  - ROM (64 Kbájt felhasználói, 8 Kbájt tesztelési, 32 Kbájt EEPROM)
- fizikai véletlenszám generátor,
- kontrollösszeg képző modul,
- megszakító modul,
- belső óra,
- cím és adat busz,
- egy kriptográfiai műveleteket végző modul (ACE) az RSA nagy egészekkel végzett moduló számításokhoz,
- egy DES algoritmus végrehajtását támogató kriptográfiai gyorsító modul.

[9] TÜV IT GmbH.
[10] A német informatika biztonsági értékelési/tanúsítási sémában központi szerepet betöltő tanúsító szervezet.

Az SLE66CX320P mikrochip förmver alkotó elemei

- rutinok az EEPROM programozására,
- a véletlenszám generátor belső tesztelő rutinjai,
- erőforrás kezelő rendszer (RMS),
- önteszt szoftver (STS) teszt és inicializáló rutinjai (védett teszt ROM-ban tárolva) /az önteszt szoftver négy részből áll: .
  - a reset utáni chip inicializáló rutinok,
  - a normál üzemmódot tesztelő rutinok,
  - a chip azonosítására használható rutinok,
  - csak a védett gyártási szakaszban használható rutinok/

Az SLE66CX320P mikrochip szoftver alkotó eleme

- operációs rendszer (nem volt része a mikrochip alap értékelésének és tanúsításának)[11].

Az SLE66CX320P mikrochip alábbi biztonsági tulajdonságait érintette az előzetes értékelés, majd az ezt követő (német séma alapján végzett) tanúsítás. Ennek eredményeit a MICARDO v2.1 intelligens kártya operációs rendszer értékelése és tanúsítása - mint kiindulási alapot – figyelembe vette.

SF1 Működési állapot ellenőrzés

Az SLE66CX320P helyes működése csak bizonyos tartományon belül garantált. Az ezen tényt kihasználni igyekvő támadások megakadályozása érdekében szükség van annak észlelésére, hogy a környezeti körülmények elhagyták a garantált tartományt. Minden műveleti jelet megszűrnek a hibás működés elkerülése érdekében.
Egyúttal a működési állapotokat folyamatosan figyelemmel kísérik (a feszültséget és az óra jel frekvenciát érzékelő szenzorokkal).

SF2 Adat titkosítás, a chip-en működő kulcsmenedzsment és véletlenszámgenerálás

Az adatok kiolvasása kontrollálható titkosítás alkalmazásával. Csak a kulcs tulajdonosának van lehetősége az adatok kiolvasására.

Az SLE66CX320P memóriatartalma titkosításra kerül, hogy védjen a tárolt, illetve a belül továbbított adatok elemzése ellen. A kiszivárgó információ értelmezésének megakadályozására az információ közé véletlen elemeket iktatnak.

A véletlen adatok alapvető fontossággal bírnak mind a kriptográfiai, mind a fizikai biztonsági mechanizmusok támogatásában. Az SLE66CX320P-ben egy valódi, fizikai véletlen jelenségen alapuló véletlenszám generátor van. A generált véletlen adatokat mind a biztonságot érvényre juttató funkciók, mind a felhasználói szoftverek használhatják.

[11] Ez a MICARDO 2.1 értékelésének és tanúsításának volt a feladata

SF3 Életciklus fázis kezelés és a teszt üzemmód lezárása

A működés szempontjából három különböző üzemmód van: teszt-, felhasználói- és chip azonosítói üzemmód.
Egy inicializáló modul és különböző hardver és szoftver flag-ek kombinációja kontrollálja az egyes üzemmódok közötti váltást.

SF4 Kifürkészés elleni védelem

Számos biztonsági mechanizmus próbál védekezni a felhasználói adatok kifürkészése ellen, mind a működtetés során, mind kikapcsolt állapotban.

Topológiai tervező ellenintézkedések álcázzák a tervezést (pl. aktív jelzést adó fém védőréteg a kritikus adatok védelmére). Az egész tervezés folyamán kerülték a szabványos megoldásokat, hogy megakadályozzák a szabványos vizsgálati módszerek alkalmazását. Egy külön erre az intelligens kártyára tervezett CPU és egy nem nyilvános busz protokoll nehezíti a támadók vizsgálatait.

6. A MICARDO intelligens kártya megfelelése az SSCD védelmi profil követelményeinek

6.1 A MICARDO megfelelése az SSCD védelmi profil funkcionális biztonsági követelményeinek

Kriptográfiai kulcs generálás (FCS_CKM.1)	
Követelmény (CC SSCD-PP)	A BALE legyen képes kriptográfiai kulcsokat generálni a következőknek megfelelően: ***[behelyettesítés: kriptográfiai kulcs generálási algoritmus]*** és ***[behelyettesítés: kriptográfiai kulcs méret],*** mely eleget tesz a következőknek: ***[behelyettesítés: szabványok listája.]***
MICARDO tulajdonság	A MICARDO képes: • az **RSA** digitális aláírás algoritmushoz kulcsokat generálni, • **DES és Triple-DES** kulcsokat generálni a host oldali aláíró alkalmazással kialakított megbízható csatorna kiépítéséhez (üzenetek és a jelszavak /PIN-ek/ titkosítására és kriptográfiai ellenőrzőösszeg számítására). A MICARDO képes 512 – 1024 bites **RSA** kulcsok generálására egy olyan belső kulcs generálási funkcióval, mely biztosítja az alábbiakat: • a kulcsgeneráláshoz felhasznált véletlen számok jó véletlenszerűségi tulajdonságai garantálják, hogy nagy valószínűséggel egyedi kulcsok keletkeznek, • a kulcsgeneráláshoz felhasznált prímszámok nagy valószínűséggel egyediek (mind különbözők), • egyetlen magánkulcs sem határozható meg a megfelelő nyilvános kulcsból. A MICARDO képes 56 bites **DES** és 112 bites **Triple-DES** kulcsok előállítására két különböző módszerrel: • egy kártyaspecifikus mesterkulcsból való származtatással, • a host oldal és a kártya kölcsönös hitelesítési eljárása során folytatott kulcsegyeztetési eljárásban kialakított munkaszakasz kulcs (session key) generálásával. Mindkét módszer biztosítja, hogy a generált kulcsok nagyon nagy valószínűséggel egyediek és kriptográfiailag erősek.
Ellenőrzött követelmények (MICARDO ITSEC tanúsítás)	• teljesülő SO7 biztonsági cél (A kulcsgenerálás minősége) • helyesen működő SF8.1 biztonsági funkció (Kriptográfiai kulcsgenerálás)

Kriptográfiai kulcs generálás (FCS_CKM.1) /folytatás/	
Értékelés	Az RSA (legalább 1020 bitméret mellett) minősített aláíráshoz elfogadott algoritmus. A MICARDO képes a megfelelő méretű (1024 bites) RSA kulcsok szabványos generálására. Következésképp a MICARDO képes minősített aláírásokhoz elfogadott digitális aláíró algoritmusok kulcsainak generálására. A Triple-DES szabványos kriptográfiai algoritmus, kulcsmérete alapján alkalmas a megbízható csatorna bizalmasságának sértetlenségének és hitelességének biztosítására. A MICARDO képes 112 bites triple-DES kulcsok biztonságos generálására. Következésképpen a MICARDO képes a megbízható csatorna és útvonal kiépítéséhez szükséges titkosító és kriptográfiai ellenőrzőösszeg számító algoritmus kulcsainak generálására.
Következtetés	A MICARDO (a feltételek betartása esetén) **megfelel** az SSCD-PP „Kriptográfiai kulcs generálás” követelményének.
Feltételek:	5. és 6.

Kriptográfiai kulcs megsemmisítés (FCS_CKM.4)	
Követelmény (CC SSCD-PP)	A BALE legyen képes megsemmisíteni a kriptográfiai kulcsokat a következőknek megfelelően: ***[behelyettesítés: kriptográfiai kulcs megsemmisítési módszer],*** mely eleget tesz a következőknek: ***[behelyettesítés: szabványok listája.]***
MICARDO tulajdonság	A MICARDO: • automatikusan törli (0-kkal való felülírással) a titkos kulcsok és egyéb titkok számítására használt felejtő memóriákat az adott erőforrás deallokálása során (vagyis a munkaszakasz kulcsokat a kommunikációs munkaszakasz lezárásakor, az aláíró magánkulcsot a digitális aláírás kiszámítása után), • valamennyi nem felejtő memóriában hosszú távon a kártyán tárolt fájl (köztük a kriptográfiai kulcsokat tartalmazó fájlok) törlése visszafordíthatatlan módon elveszti tartalmát.
Ellenőrzött követelmények (MICARDO ITSEC tanúsítás)	• teljesülő SO3 biztonsági cél (Memória védelem), • helyesen működő SF6.1 biztonsági funkció (Maradvány információ védelem).
Értékelés	A kulcsok egy része (munkaszakasz kulcsok, digitális aláírásra átmenetileg felejtő memóriába másolt magánkulcs másolatok) automatikusan törlődik, a többi kulcsra pedig biztosított a törlés lehetősége. Az ITSEC értékelés azt is igazolta, hogy a törlés a tárolt kulcsértékeinek fizikailag visszafordíthatatlan megsemmisítésével jár. Következésképpen a BALE képes tárolt kulcsértékeinek fizikailag visszafordíthatatlan, szabványos megsemmisítésére.
Következtetés	A MICARDO (a feltételek betartása esetén) **megfelel** az SSCD-PP „Kriptográfiai kulcs megsemmisítés” követelményének.
Feltétel:	8.

Kriptográfiai eljárás (FCS_COP.1)	
Követelmény (CC SSCD-PP)	1. A BALE képes legyen végrehajtani az alábbiakat: a magán és nyilvános kulcsok megfelelőségének igazolása az alábbiaknak megfelelően: ***[behelyettesítés: kriptográfiai algoritmus] -***és ***[behelyettesítés: kriptográfiai kulcs méret]***, eleget téve a következőknek: ***[behelyettesítés: szabványok listája]***. 2. A BALE képes legyen végrehajtani az alábbiakat: digitális aláírás-létrehozás az alábbiaknak megfelelően: ***[behelyettesítés: kriptográfiai algoritmus] -***és ***[behelyettesítés: kriptográfiai kulcs méret]***, eleget téve a következőknek: ***[behelyettesítés: szabványok listája].***
MICARDO tulajdonság	A MICARDO: • támogatja a magán és nyilvános kulcsok megfelelőségének ellenőrzését (egy véletlenül megválasztott üzenet kártyán történő aláírásával, majd az aláírás host oldali ellenőrzésével elvégzett páronkénti konzisztencia teszttel az RSA kulcspárok generálását követően), amennyiben a megfelelő parancs sorozatot meghívják a host oldalon, a kulcspár generálás lezárásaként, (lásd a 14/2. feltétel), • támogatja az **RSA** digitális aláírás algoritmust (*512-1024 bit közötti kulcsmérettel, általános (host oldalról vezérelt), illetve szabványos PKCS#1-es formátumban*),
Ellenőrzött követelmények (MICARDO ITSEC tanúsítás)	• teljesülő SO4 biztonsági cél (A kriptográfia műveletek biztonsága), • teljesülő SO7 biztonsági cél (A kulcsgenerálás minősége), • helyesen működő SF8.1 biztonsági funkció (Kriptográfiai kulcsgenerálás), • helyesen működő SF8.2 biztonsági funkció (A digitális aláírások számítása).
Értékelés	A MICARDO képes egy minősített aláíráshoz elfogadott szabványos kriptográfiai algoritmus végrehajtásával (RSA, 1024 bites kulcsmérettel, PKCS#1 aláírási formátummal SHA-1 lenyomatoló függvénnyel) az alábbi feladatokat ellátni: • a magánkulcs/nyilvános kulcs megfelelésének bizonyítása, • az aláírandó adatok digitális aláírása.
Következtetés	A MICARDO (a feltételek betartása esetén) **megfelel** az SSCD-PP „Kriptográfiai eljárás” követelményének.
Feltételek:	14.

Részleges hozzáférés ellenőrzés (FDP_ACC.1)	
Követelmény (CC SSCD-PP)	A BALE legyen képes a következő hozzáférés ellenőrzések érvényre juttatására: 1. az aláírás-létrehozó adatot (magánkulcsot) csak az erre felhatalmazott aláíró vagy adminisztrátor generálhatja (a megszemélyesítés fázisában), 2. az aláírás-ellenőrző adatot (nyilvános kulcsot) csak az aláíró vagy az adminisztrátor exportálhatja (tanúsítvány generálása céljából, a minősített hitelesítés-szolgáltatóhoz), 3. a hitelesítő adatot (PIN kódot vagy jelszót) csak az adminisztrátor hozhatja létre (a megszemélyesítés fázisában). 4. az aláíró alkalmazás által küldött lenyomat értéket csak az aláíró írhatja alá.
MICARDO tulajdonság	A MICARDO támogatja a felhasználói és adminisztrátori szerepkör szétválasztását. Egy BALE-ként használt MICARDO esetén az „aláíró” a „felhasználó”, míg az intelligens kártya megszemélyesítési folyamatában különleges jogosultságokkal rendelkező személy az „adminisztrátor”. Ilyen szerepkör megfeleltetés, valamint a 14. feltétel betartása esetén: • csak az „aláíró” vagy az „adminisztrátor” generálhatja az aláírói magánkulcsot, • csak az „aláíró” vagy az „adminisztrátor” exportálhatja a nyilvános kulcsot, • az aláíró PIN kódját csak az „adminisztrátor” hozhatja létre, • csak az „aláíró” írhat alá magánkulcsa aktivizálásával.
Ellenőrzött követelmények (MICARDO ITSEC tanúsítás)	• teljesülő SO1 biztonsági cél (Jogosult hozzáférés), • helyesen működő SF2.1 biztonsági funkció (A hozzáférés ellenőrzés menedzselése), • helyesen működő SF2.2 biztonsági funkció (Biztonsági attribútum alapú hozzáférés ellenőrzés).
Értékelés	Az SSCD-PP „Részleges hozzáférés ellenőrzés” követelményét a MICARDO támogatja, az ITSEC értékelés pedig igazolja (a 14. feltétel betartása esetén): • csak az adminisztrátor tisztviselő hozhatja létre a felhasználó (aláíró) kezdeti PIN kódját, • csak az adminisztrátor vagy a felhasználó (aláíró) generálhatja saját magánkulcsát, • csak az adminisztrátor vagy a felhasználó (aláíró) exportálhatja a generált nyilvános kulcsot, • csak a felhasználó (aláíró) írhat alá saját magánkulcsával.
Következtetés	A MICARDO (a feltételek betartása esetén) **megfelel** az SSCD-PP „Részleges hozzáférés ellenőrzés” követelményének.
Feltétel:	14.

Biztonsági jellemzőkön alapuló hozzáférés ellenőrzés (FDP_ACF.1)	
Követelmény (CC SSCD-PP)	1. A BALE az általános és inicializáló biztonsági jellemzőkre (attribútumokra) alapulva juttassa érvényre az inicializálás biztonsági funkciót. A BALE juttassa érvényre a következő szabályokat annak eldöntésére, hogy egy ellenőrzött szubjektum és ellenőrzött objektum közötti művelet megengedett-e: • az aláírás-létrehozó adat (magánkulcs) akkor generálható, ha a „szerep" biztonsági jellemző „aláíró" vagy „adminisztrátor" értékre van állítva, valamint a „magán-nyilvános kulcspár kezelés" biztonsági jellemző „felhatalmazott" értékre van állítva. A BALE kifejezetten tagadja meg a szubjektumoknak az objektumokhoz való hozzáférését, a következő szabályok alapján: • az aláírás-létrehozó adat (magánkulcs) nem generálható, ha a „szerep" biztonsági jellemző „aláíró" vagy „adminisztrátor" értékre van állítva, valamint a „magán-nyilvános kulcspár kezelés" biztonsági jellemző „nem felhatalmazott" értékre van állítva. 2. A BALE az általános biztonsági jellemzőkre alapulva juttassa érvényre a nyilvános kulcs exportálás biztonsági funkciót. A BALE juttassa érvényre a következő szabályokat annak eldöntésére, hogy egy ellenőrzött szubjektum és ellenőrzött objektum közötti művelet megengedett-e: • az aláírás-ellenőrző adat (nyilvános kulcs) akkor exportálható, ha a „szerep" biztonsági jellemző „aláíró" vagy „adminisztrátor" értékre van állítva. 3. A BALE az általános biztonsági jellemzőkre alapulva juttassa érvényre a megszemélyesítés (perszonalizálás) biztonsági funkciót. A BALE juttassa érvényre a következő szabályokat annak eldöntésére, hogy egy ellenőrzött szubjektum és ellenőrzött objektum közötti művelet megengedett-e: • a hitelesítő adat (PIN kód) akkor hozható létre, ha a „szerep" biztonsági jellemző „adminisztrátor" értékre van állítva. 4. A BALE az általános és az aláírás-létrehozás biztonsági jellemzőkre alapulva juttassa érvényre az aláírás-létrehozás biztonsági funkciót. A BALE juttassa érvényre a következő szabályokat annak eldöntésére, hogy egy ellenőrzött szubjektum és ellenőrzött objektum közötti művelet megengedett-e: • egy hiteles aláíró alkalmazás által küldött aláírandó adatra elektronikus aláírás akkor készíthető, ha a „szerep" biztonsági jellemző „aláíró" értékre van állítva, valamint a „magánkulcs aktivizálás" biztonsági jellemző „igen" értékre van állítva. A BALE kifejezetten tagadja meg a szubjektumoknak az objektumokhoz való hozzáférését, a következő szabályok alapján: a.) egy **nem hiteles** aláíró alkalmazás által küldött aláírandó adatra elektronikus aláírás nem készíthető, ha a „szerep" biztonsági jellemző „aláíró" értékre van állítva, valamint a „magánkulcs aktivizálás" biztonsági jellemző „igen" értékre van állítva. b.) egy hiteles aláíró alkalmazás által küldött aláírandó adatra elektronikus aláírás nem készíthető, ha a „szerep" biztonsági jellemző „aláíró" értékre van állítva, valamint a „magánkulcs aktivizálás" biztonsági jellemző „**nem**" értékre van állítva.

Biztonsági jellemzőkön alapuló hozzáférés ellenőrzés (FDP_ACF.1) /folytatás/	
MICARDO tulajdonság	A MICARDO támogatja a felhasználói és adminisztrátori szerepkör szétválasztását. Egy BALE-ként használt MICARDO esetén az „aláíró” a „felhasználó”, míg az intelligens kártya megszemélyesítési folyamatában különleges jogosultságokkal rendelkező személy az „adminisztrátor”. Ilyen szerepkör megfeleltetés, valamint a 14. feltétel betartása esetén: • az aláíró kezdeti PIN kódját csak az „adminisztrátor” hozhatja létre, • az „aláíró” csak akkor generálhatja le saját magánkulcsát, ha ezt az adminisztrátor engedélyezi számára, • csak az „aláíró” vagy az „adminisztrátor” exportálhatja a nyilvános kulcsot, • csak az „aláíró” írhat alá magánkulcsával, miután az „adminisztrátor” ezt engedélyezte számára.
Ellenőrzött követelmények (MICARDO ITSEC tanúsítás)	• teljesülő SO1 biztonsági cél (Jogosult hozzáférés), • helyesen működő SF2.1 biztonsági funkció (A hozzáférés ellenőrzés menedzselése), • helyesen működő SF2.2 biztonsági funkció (Biztonsági attribútum alapú hozzáférés ellenőrzés).
Értékelés	Az SSCD-PP „Biztonsági jellemzőkön alapuló hozzáférés ellenőrzés” követelményét a MICARDO támogatja, az ITSEC értékelés pedig igazolja (a 14. feltétel betartása esetén): • amennyiben nem az adminisztrátor generálja a kulcspárokat, az „aláíró” csak akkor generálhatja le saját magánkulcsát, ha ezt az „adminisztrátor” engedélyezi számára, • amennyiben nem az adminisztrátor generálja a kulcspárokat csak az „aláíró” exportálhatja saját nyilvános kulcsát, • az „aláíró” kezdeti PIN kódját csak az „adminisztrátor” hozhatja létre, • csak az „aláíró” írhat alá magánkulcsával, de ő is csak azután, hogy az „adminisztrátor” ezt engedélyezte számára.
Következtetés	A MICARDO (a feltételek betartása esetén) **megfelel** az SSCD-PP „Biztonsági jellemzőkön alapuló hozzáférés ellenőrzés” követelményének.
Feltétel:	14.

Részleges maradvány információ védelem (FDP_RIP.1)	
Követelmény (CC SSCD-PP)	A BALE-nak biztosítania kell, hogy erőforrás visszavétel (deallokáció) után semmilyen korábbi információ tartalom ne legyen hozzáférhető az alábbi objektumokra nézve: • aláírás-létrehozó adat (magánkulcs), • hitelesítő adat (megadott PIN kód vagy jelszó), • hitelesítést ellenőrző adat (a PIN kód vagy jelszó kártyán tárolt képe).
MICARDO tulajdonság	A MICARDO garantálja, hogy egy erőforrás minden előző információ tartalma közvetlen törlésre kerüljön a következő objektumok deallokálása során: • valamennyi elemi és dedikált fájl, • a titkos kulcsok és egyéb titkok számítására használt felejtő memóriák.
Ellenőrzött követelmények (MICARDO ITSEC tanúsítás)	• teljesülő SO3 biztonsági cél (Memória védelem), • helyesen működő SF6.1 biztonsági funkció (Maradvány információ védelem).
Értékelés	Mivel a magánkulcsok, hitelesítő adatok és hitelesítést ellenőrző adatok hosszú távon elemi fájlokban, rövid távon pedig felejtő memóriákban tárolódnak, ezért a fent említett, és az ITSEC értékelés által ellenőrzött MICARDO tulajdonság /deallokálás utáni törlés/ biztosan vonatkozik rájuk.
Következtetés	A MICARDO **megfelel** az SSCD-PP „Részleges maradvány információ védelem” követelményének.
Feltétel:	---

A tárolt adatok sértetlenségének figyelése és beavatkozás (FDP_SDI.2)	
Követelmény (CC SSCD-PP)	A BALE biztosítsa az általa folyamatosan tárolt adatok közül az alábbiak sértetlenségének ellenőrzését: • aláírás-létrehozó adat (magánkulcs), • hitelesítést ellenőrző adat (a PIN kód vagy jelszó kártyán tárolt képe), • aláírás-ellenőrző adat (nyilvános kulcs) /amennyiben az aláíró a BALE-n tárolja/. A BALE biztosítsa az általa átmenetileg tárolt adatok közül az alábbiak sértetlenségének ellenőrzését: • aláírandó adat reprezentáns (lenyomatolt aláírandó adat). Mindkét fenti adatcsoportra, integritás hiba észlelése esetén a BALE: • akadályozza meg a módosult adatok használatát, egyúttal • értesítse az aláírót az integritás hibáról (hibaüzenet generálásával).
MICARDO tulajdonság	A MICARDO az intelligens kártyán elemi (EF) és dedikált (DF) fájlokban tárolt valamennyi felhasználói adatot folyamatosan figyeli a következő attribútumok alapján: • a minden fájl fejrészéhez csatolt ellenőrző összeg (CRC), • a fájlok adattartalmára számolt, s ehhez csatolt ellenőrző összeg (CRC). Adat integritás hiba észlelése esetén a kártya értesíti a felhasználót a hibáról. Fejrész ellenőrző összeg hiba esetén a fájlban tárolt felhasználói adathoz nem lehet többé hozzáférni.
Ellenőrzött követelmények (MICARDO ITSEC tanúsítás)	• teljesülő SO3 biztonsági cél (Memória védelem), • helyesen működő SF3.1 biztonsági funkció (A tárolt adatok sértetlenségének monitorozása, szükség esetén közbelépés).
Értékelés	A magán- és nyilvános kulcsokat, valamint a hitelesítő adatokat tartalmazó elemi fájlokra a fent említett, és az ITSEC értékelés által ellenőrzött MICARDO tulajdonság /CRC ellenőrző összegek folyamatos figyelése/ biztosan észleli az integritás hibákat. Integritás hiba észlelése esetén a MICARDO megakadályozza a módosult adatok használatát, egyúttal értesíti (hibaüzenet formájában) az aláírót az integritás hibáról. Következésképpen a MICARDO valamennyi, a BALE-ktől elvárt tulajdonsággal rendelkezik ebben a követelménycsoportban is.
Következtetés	A MICARDO **megfelel** az SSCD-PP „A tárolt adatok sértetlenségének figyelése és beavatkozás” követelményének.
Feltétel:	---

Az adat-csere sértetlensége (FDP_UIT.1)	
Követelmény (CC SSCD-PP)	1. A BALE legyen képes érvényre juttatni, hogy a nyilvános kulcs exportálás biztonsági funkció olyan módon továbbítsa a felhasználói adatokat (*nyilvános kulcsot*), mely megvédi a módosításból, és beszúrásból adódó hibáktól. A BALE legyen képes arra, hogy a felhasználói adatok vételekor megállapítsa, hogy történt-e módosítás vagy beszúrás. 2. A BALE legyen képes érvényre juttatni, hogy az aláírás-létrehozás biztonsági funkció olyan módon fogadja a felhasználói adatokat (*aláírandó adat reprezentánst*), mely megvédi a módosításból, törlésből és beszúrásból adódó hibáktól. A BALE legyen képes arra, hogy a felhasználói adatok vételekor megállapítsa, hogy történt-e módosítás, törlés vagy beszúrás.
MICARDO tulajdonság	A MICARDO képes megbízható csatornát kiépíteni, mely megvédi a host oldali alkalmazás és az intelligens kártya között kicserélt adatok hitelességét és sértetlenségét a továbbítás során (kriptográfiai ellenőrzőösszeg képzés alkalmazásával). Mind a nyilvános kulcs exportálásához, mind az aláírandó adat reprezentáns importálásához használható (és a 12. feltétel szerint használandó is) ez a megbízható csatorna (hitelességet és sértetlenséget biztosító titkos üzenetváltás).
Ellenőrzött követelmények (MICARDO ITSEC tanúsítás)	• teljesülő SO5 biztonsági cél (A továbbított adatok sértetlensége és hitelessége), • helyesen működő SF5.2 biztonsági funkció (Adat csere hitelesség és sértetlenség).
Értékelés	A 12 feltétel teljesítése esetén (melyet a MICARDO támogat) kiépülő megbízható csatornán a nyilvános kulcs és aláírandó adat reprezentáns) védve van a módosításból, törlésből és beszúrásból eredő hibákkal szemben.
Következtetés	A MICARDO (a feltételek betartása esetén) **megfelel** az SSCD-PP „Az adat-csere sértetlensége” követelményének.
Feltétel:	12.

A hitelesítési hiba kezelése (FIA_AFL.1)	
Követelmény (CC SSCD-PP)	A BALE legyen képes detektálni, ha ***[behelyettesítés: egy meghatározott szám]*** sikertelen, egymást követő hitelesítési kísérlet történt. A meghatározott számú vagy ennél több sikertelen hitelesítési kísérlet bekövetkezése esetén a BALE blokkolja a PIN kódot.
MICARDO tulajdonság	A MICARDO a sikertelen hitelesítési kísérletek megakadályozása érdekében az alábbi ellenintézkedéseket valósítja meg: • összehasonlítja a felhasználó által megadott jelszót (vagy PIN-t) egy a kártyán tárolt titkos referencia értékkel, • észleli, ha egy előre meghatározott számú (n) sikertelen hitelesítési kísérlet következett be, bármely jelszó alapú hitelesítési eljárásban, • sikeres hitelesítés esetén egy számláló értékét n-re állítja, • sikertelen hitelesítés esetén a fenti számláló értékét eggyel csökkenti, • ha a fenti számláló értéke 0 lesz, akkor a megfelelő jelszó (PIN kód) blokkolódik (s ilyenkor csak egy reset funkció állíthatja vissza a számláló kiindulási értékét a blokkolás feloldására), • a blokkolás jogosulatlan végrehajtása ellen ennek a reset funkciónak a hozzáférési szabálya véd (a 13. feltétel teljesítése esetén).
Ellenőrzött követelmények (MICARDO ITSEC tanúsítás)	• teljesülő SO1 biztonsági cél ((Jogosult hozzáférés), • helyesen működő SF1.2 biztonsági funkció (Jelszó alapú felhasználó hitelesítés).
Értékelés	A MICARDO támogatja az SSCD védelmi profil fenti elvárását.
Következtetés	A MICARDO (a feltételek betartása esetén) **megfelel** az SSCD-PP „A hitelesítési hiba kezelése” követelményének.
Feltétel:	13.

A felhasználói jellemzők meghatározása (FIA_ATD.1)	
Követelmény (CC SSCD-PP)	A BALE legyen képes kezelni az egyedi felhasználókhoz (aláíróhoz) tartozó biztonsági jellemzők következő listáját: PIN kód.
MICARDO v2.1 tulajdonság	A MICARDO képes kezelni a PIN kódot, mindkét szerepkörhöz tartozóan (így a felhasználóra, vagyis az aláíróra is).
Ellenőrzött követelmények (MICARDO ITSEC tanúsítás)	• teljesülő SO1 biztonsági cél ((Jogosult hozzáférés), • helyesen működő SF1.2 biztonsági funkció (Jelszó alapú felhasználó hitelesítés).
Értékelés	A követelmény teljesül.
Következtetés	A MICARDO **megfelel** az SSCD-PP „A felhasználói jellemzők meghatározása” követelményének.
Feltétel:	---

Az azonosítás időzítése (FIA_UID.1)	
Követelmény (CC SSCD-PP)	A BALE az aláíró azonosítása előtt csak az alábbiakat engedje meg: • egy megbízható útvonal létesítése a helyi felhasználó és a BALE között (az FTP_TRP.1-nek megfelelően), • egy megbízható csatorna létesítése a megbízható aláírás-létrehozó alkalmazás és a BALE között (az FTP_ITC.1-nek megfelelően). A BALE bármilyen további, általa közvetített tevékenységet csak akkor engedélyezzen, ha az aláíró már sikeresen azonosította magát[12].
MICARDO tulajdonság	A MICARDO különböző szempontokból menedzseli az egyes objektumokhoz való hozzáférést /hozzáférési szabályok, felhasználási cél, életciklus állapot, részletesebben lásd a 4.2, valamint az SF2 Hozzáférés ellenőrzés alfejezeteket/. A fájlokra, kulcsokra és jelszavakra egyaránt alkalmazható hozzáférési szabályok keretében a hozzáférés különböző feltételei határozhatók meg. Ezek a feltételek azt határozzák meg, hogy egy végrehajtandó parancs hozzáférhet-e egy adott objektumhoz. Lehetséges értékei között szerepel a következő is: • sikeres jelszó alapú felhasználói hitelesítés után. Ez azt jelenti, hogy a MICARDO támogatja az aláírással kapcsolatos parancsok felhasználói hitelesítéshez kötését (ezt el is várjuk a 14/5. feltételben). Mivel a felhasználói hitelesítés egyben a felhasználó azonosítását is eredményezi a MICARDO támogatja, hogy bármilyen (közte és a felhasználó/megbízható aláírás-létrehozó alkalmazás közötti megbízható útvonal/csatorna létesítését követő) általa közvetített, aláírással kapcsolatos tevékenységet csak akkor engedélyezzen, ha az aláíró már sikeresen azonosította magát.
Ellenőrzött követelmények (MICARDO ITSEC tanúsítás)	• teljesülő SO1 biztonsági cél ((Jogosult hozzáférés), • helyesen működő SF2.1 biztonsági funkció (A hozzáférés ellenőrzés menedzselése), • helyesen működő SF2.2 biztonsági funkció (Biztonsági attribútum alapú hozzáférés ellenőrzés),
Értékelés	A MICARDO támogatja a követelmény kielégítését. Amennyiben az aláírással kapcsolatos parancsok felhasználói hitelesítéshez vannak kötve /ezt várja el a 14/5. feltétel/, akkor az elvárás teljesül.
Következtetés	A MICARDO (a feltételek betartása esetén) **megfelel** az SSCD-PP „Az azonosítás időzítése” követelményének.
Feltétel:	14.

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

A hitelesítés időzítése (FIA_UAU.1)	
Követelmény (CC SSCD-PP)	A BALE az aláíró hitelesítése előtt csak az alábbiakat engedje meg: • az aláíró azonosítása (a FIA_UID.1-nek megfelelően), • egy megbízható útvonal létesítése a helyi felhasználó és a BALE között (az FTP_TRP.1-nek megfelelően), • egy megbízható csatorna létesítése a megbízható aláírás-létrehozó alkalmazás és a BALE között (az FTP_ITC.1-nek megfelelően). A BALE bármilyen további, általa közvetített tevékenységet csak akkor engedélyezzen, ha az aláíró már sikeresen hitelesítette magát[13].
MICARDO tulajdonság	Mint azt a FIA_UID.1 (Az azonosítás időzítése) követelmény tárgyalásánál kimutattuk, a MICARDO támogatja az aláírással kapcsolatos parancsok felhasználói hitelesítéshez kötését.
Ellenőrzött követelmények (MICARDO ITSEC tanúsítás)	• teljesülő SO1 biztonsági cél ((Jogosult hozzáférés), • helyesen működő SF2.1 biztonsági funkció (A hozzáférés ellenőrzés menedzselése), • helyesen működő SF2.2 biztonsági funkció (Biztonsági attribútum alapú hozzáférés ellenőrzés),
Értékelés	A MICARDO támogatja a követelmény kielégítését. Amennyiben az aláírással kapcsolatos parancsok felhasználói hitelesítéshez vannak kötve /ezt várja el a 14/5. feltétel/, akkor az elvárás teljesül.
Következtetés	A MICARDO (a feltételek betartása esetén) **megfelel** az SSCD-PP „Az azonosítás időzítése” követelményének.
Feltétel:	14.

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

A biztonsági funkciók viselkedésének kezelése (FMT_MOF.1)	
Követelmény (CC SSCD-PP)	A BALE legyen képes az aláírás-létrehozás funkció aktivizálását korlátozni, csak az aláíró számára elérhetővé téve azt.
MICARDO tulajdonság	Mint azt a FIA_UID.1 (Az azonosítás időzítése) követelmény tárgyalásánál kimutattuk, a MICARDO támogatja az aláírással kapcsolatos parancsok felhasználói hitelesítéshez kötését.
Ellenőrzött követelmények (MICARDO ITSEC tanúsítás)	• teljesülő SO1 biztonsági cél ((Jogosult hozzáférés), • helyesen működő SF2.1 biztonsági funkció (A hozzáférés ellenőrzés menedzselése), • helyesen működő SF2.2 biztonsági funkció (Biztonsági attribútum alapú hozzáférés ellenőrzés),
Értékelés	A MICARDO támogatja a követelmény kielégítését. A 14./4 feltétel teljesülése esetén aláírásra csak az „aláíró” aktivizálhatja magánkulcsát az inicializációs, perszonalizációs szakaszban, Amennyiben az aláírás-létrehozási funkció kiváltása felhasználói hitelesítéshez van kötve /ezt pedig a 14/5. feltétel várja el/, akkor a későbbiekben is csak az aláíró aktivizálhatja ezt.
Következtetés	A MICARDO (a feltételek betartása esetén) **megfelel** az SSCD-PP „A biztonsági funkciók viselkedésének kezelése” követelményének.
Feltétel:	14.

A biztonsági jellemzők kezelése (FMT_MSA.1)	
Követelmény (CC SSCD-PP)	A BALE legyen képes: • az „inicializálás” funkció „magán-nyilvános kulcspár kezelés” biztonsági jellemzőjének módosítási lehetőségét az adminisztrátorra korlátozni, • az „aláírás-létrehozás” funkció „magánkulcs működtetése (aláírás)” biztonsági jellemzőjének módosítási lehetőségét az aláíróra korlátozni.
MICARDO tulajdonság	A 14/1. feltétel betartása esetén csak az „adminisztrátor” adhatja meg a jogot az „aláíró”-nak kulcspár kezelésére. A 14/4. feltétel betartása esetén csak az „aláíró” képes az aláírás lehetőségét saját maga számára biztosítani (de ezt a lehetőséget nem tilthatja meg).
Ellenőrzött követelmények (MICARDO ITSEC tanúsítás)	• teljesülő SO1 biztonsági cél ((Jogosult hozzáférés), • helyesen működő SF2.1 biztonsági funkció (A hozzáférés ellenőrzés menedzselése), • helyesen működő SF2.2 biztonsági funkció (Biztonsági attribútum alapú hozzáférés ellenőrzés),
Értékelés	A MICARDO v2.1 közvetlenül nem támogatja a BALE-ra elvárt, a biztonsági jellemzők módosítási lehetőségére vonatkozó fenti követelményt. Ugyanakkor a MICARDO v2.1 által biztosított általános szerepkörök jogosultság elkülönítésével, valamint a 14. feltétel teljesítésével az elvárás lényegi része teljesíthető.
Következtetés	A MICARDO (a feltételek betartása esetén) **megfelel** az SSCD-PP „A biztonsági jellemzők kezelése” követelményének.
Feltétel:	14.

Biztonságos biztonsági jellemzők (FMT_MSA.2)	
Követelmény (CC SSCD-PP)	A BALE biztosítsa, hogy biztonsági jellemzőknek (attribútumnak) csak biztonságos értékek lesznek elfogadva.
MICARDO v2.1 tulajdonság	A MICARDO v2.1 filozófiája ellentétes a fenti elvárással. Sőt az inicializálási, perszonalizálási szakaszban (a külső, általános parancsokkal való vezérelhetőség érdekében) egyes biztonsági attribútumokat kifejezetten nem biztonságos értékűre kell átmenetileg állítani. */Például egy kulcs pár generálására a felhasználói kézikönyv az alábbi, egymást követő lépéseket javasolja:* *1. új könyvtár létrehozása az adatfájlok számára (DF, valamint megfelelő strukturális információkkal feltöltött EF-k),* *2. az új adatmezők feltöltése,* *3. a hozzáférési jogok módosítása (ezt követően a magánkulcs információkhoz nem lehetséges a hozzáférés),* *4. kulcs generálása,* *5. a nyilvános kulcs kiolvasása* *A felhasználói útmutató is felhívja a figyelmet arra, hogy amennyiben a fenti 3. lépés kimarad, a magánkulcs módosítható vagy olvasható marad!/* A MICARDO támogatja, hogy az aláíró magánkulcsot más célra ne lehessen felhasználni, de ezt (adminisztrátori jogosultsággal) külön be kell állítani.
Ellenőrzött követelmények (MICARDO ITSEC tanúsítás)	• teljesülő SO1 biztonsági cél ((Jogosult hozzáférés), • helyesen működő SF2.1 biztonsági funkció (A hozzáférés ellenőrzés menedzselése), • helyesen működő SF2.2 biztonsági funkció (Biztonsági attribútum alapú hozzáférés ellenőrzés),
Értékelés	Amennyiben az alábbi három feltétel együttesen teljesül, akkor az elvárás mögött meghúzódó veszélyeket sikerül elfogadható szintre csökkenteni: • az adminisztrátor és a felhasználó (aláíró) szerepkörök teljes szétválasztása (a 14. feltétel ezt tartalmazza), • minden biztonsági attribútum (az adminisztrátor által létrehozva, majd esetenként módosítva) az inicializálási, perszonalizálási fázis végére biztonságos értéket vesz fel, s így hagyja el a hitelesítés-szolgáltató védett környezetét (s a felhasználói környezetben ez a későbbiekben már nem változtatható meg) (a 14/5. feltétel épp ezt tartalmazza), • a hitelesítés-szolgáltató által működtetett, inicializálást, perszonalizálást végző, esetenként nem biztonságos attribútum beállításokat is működtető alkalmazásokat egy független értékelési eredmény alapján megbízható elektronikus aláírási termékként értékelik (az elektronikus aláírás törvény értelmében)./15. feltétel/
Következtetés	A MICARDO (a feltételek betartása esetén) **megfelel** az SSCD-PP „Biztonságos biztonsági jellemzők” követelményének.
Feltétel:	14. és 15.

Statikus jellemző inicializálás (FMT_MSA.3)	
Követelmény (CC SSCD-PP)	A BALE az „inicializálás” és az „aláírás-létrehozás” biztonsági funkciókra korlátozó alapértékeket szolgáltasson: az aláírás-létrehozó adat generálása után a „magánkulcs aktivizálása” (aláírás) biztonsági jellemzőt „nem” értékre állítsa. A BALE tegye lehetővé az adminisztrátor számára, hogy a fenti korlátozó (default) alapértéket felülírja a megszemélyesítés folyamán.
MICARDO tulajdonság	A MICARDO ezt a követelményt nem támogatja.
Ellenőrzött követelmények (MICARDO ITSEC tanúsítás)	• teljesülő SO1 biztonsági cél ((Jogosult hozzáférés), • helyesen működő SF2.1 biztonsági funkció (A hozzáférés ellenőrzés menedzselése), • helyesen működő SF2.2 biztonsági funkció (Biztonsági attribútum alapú hozzáférés ellenőrzés),
Értékelés	A MICARDO közvetlenül nem támogatja a BALE-ra elvárt fenti követelményt. A MICARDO által biztosított általános szerepkörök jogosultság elkülönítésével, valamint a 14. feltétel rezsim utasításainak betartásával az elvárás érdemi része ugyanakkor teljesíthető: • a fenti követelmény célja annak megakadályozása, hogy egy már kulcsokkal ellátott, de még nem az aláíró személyes felügyelete alá tartozó intelligens kártyával ne élhessenek vissza jogosulatlanul, • a 14/6. feltétel technikai vagy rezsim intézkedésekkel pont ennek megakadályozását várja el.
Következtetés	A MICARDO (a feltételek betartása esetén) **megfelel** az SSCD-PP „Statikus jellemző inicializálás” követelményének.
Feltétel:	14.

A biztonsági funkciók adatainak kezelése (FMT_MTD.1)	
Követelmény (CC SSCD-PP)	A BALE a hitelesítő adatok (PIN kód) módosításának lehetőségét az aláíróra korlátozza.
MICARDO tulajdonság	A MICARDO a felhasználóra korlátozza saját PIN kódjának (jelszavának) módosítási lehetőségét. (A cserét megvalósító „Change Reference Data” parancs sikers végrehajtásához szükség van a régi PIN kód helyes megadására) A 14. feltétel betartása esetén az „aláíró” a felhasználó lesz.
Ellenőrzött követelmények (MICARDO ITSEC tanúsítás)	• teljesülő SO1 biztonsági cél ((Jogosult hozzáférés), • helyesen működő SF1.2 biztonsági funkció (Jelszó alapú felhasználó hitelesítés).
Értékelés	A MICARDO teljesíti az elvárást, az ITSEC értékelés igazolja ezt.
Következtetés	A MICARDO (a feltételek betartása esetén) **megfelel** az SSCD-PP „A biztonsági funkciók adatainak kezelése” követelményének.
Feltétel:	14.

Biztonsági szerepkörök (FMT_SMR.1)	
Követelmény (CC SSCD-PP)	A BALE legyen képes az alábbi szerepek kezelésére: adminisztrátor, aláíró. A BALE legyen képes összekapcsolni a felhasználókat az egyes szerepekkel.
MICARDO tulajdonság	A MICARDO az alábbi szerepköröket támogatja: • adminisztrátor • felhasználó A 14. feltétel betartása esetén az „aláíró” a felhasználó lesz.
Ellenőrzött követelmények (MICARDO ITSEC tanúsítás)	• teljesülő SO1 biztonsági cél (Jogosult hozzáférés), • helyesen működő SF1.2 biztonsági funkció (Jelszó alapú felhasználó hitelesítés).
Értékelés	A MICARDO teljesíti az elvárást, az ITSEC értékelés igazolja ezt.
Következtetés	A MICARDO (a feltételek betartása esetén) **megfelel** az SSCD-PP „A biztonsági szerepkörök” követelményének.
Feltétel:	14.

Az absztrakt gép tesztelése (FPT_AMT.1)	
Követelmény (CC SSCD-PP)	A BALE ***[választás: a kezdeti rendszer indítás során; a normál működés során periodikusan; egy jogosult felhasználó kérelme esetén; más feltételek fellépésekor]*** hajtson végre egy olyan teszt-sorozatot, mely kimutatja, hogy helyesen működik a BALE alapját képező absztrakt gép.
Infineon tulajdonság	Az SLE66CX320P chip helyes működése csak bizonyos tartományon belül garantált. A chip minden művelet végrehajtásakor ellenőrzi, hogy a környezeti körülmények elhagyták-e ezt a garantált tartományt, (s csak a pozitív esetben hajtja végre azt). A chip önteszt szoftvere támogatja a helyes működés ellenőrzését: • a reset parancs kiadása után automatikusan lefutó inicializáló rutinok ellenőrzik a legfontosabb hardver elemeket (memóriák, CPU, stb.), • a normál üzemmódot tesztelő rutinok folyamatosan monitorozzák a helyes működést (pl. a tárolt adatok sértetlenségét). A chip hardver-vezérelt öntesztje nem indítható a felhasználói szoftverekből, az csak mintegy automatikus alap (háttér) ellenőrzésként áll rendelkezésre.
Ellenőrzött követelmények (Infineon ITSEC tanúsítás)	• helyesen működő SF1 biztonsági funkció (Működési állapot ellenőrzés).
MICARDO v2.1 tulajdonság	A MICARDO v2.1 operációs rendszernek nincs olyan parancsa, mellyel közvetlen hardver tesztelést lehetne kiváltani. Ugyanakkor a chip az általa feldolgozott parancsok visszatérési értékeiben jelzi, ha meghibásodott („MemoryFailureError”, UndefinedTechnicalProblem”, stb.). A host oldalról kiadható reset parancs pedig kiváltja a legszükségesebb hibaellenőrzési tesztrutinok futtatását. Az operációs rendszer SF3.1 biztonsági tulajdonsága pedig az egyik legveszélyesebb hardver hiba (a chip-ben tárolt adatok sértetlenségének elvesztése) folyamatos tesztelését vállalja magára.
Ellenőrzött követelmények (MICARDO ITSEC tanúsítás)	• helyesen működő SF3.1 biztonsági funkció (A tárolt adatok sértetlenségének monitorozása, szükség esetén közbelépés).

Az absztrakt gép tesztelése (FPT_AMT.1) /folytatás/	
Értékelés	A chip nem támogatja, hogy öntesztje alkalmazói programból vagy az operációs rendszerből meghívható legyen. Ezért a BALE alapját képező absztrakt gép helyes működése nem ellenőrizhető egy jogosult felhasználó konkrét kérelmére. Ugyanakkor a kezdeti rendszer indítás során (reset után), valamint bizonyos értelemben folyamatosan (a tárolt adatok sértetlenségének monitorozásával és a környezeti körülmények garantált tartományba esésének ellenőrzésével) az absztrakt gép (chip) teszteli önmagát, s hibajelzéssel (parancs visszatérési értékekkel) tájékoztatja a parancsot kiadó host oldali alkalmazást az esetleges meghibásodásról, vagy fizikai támadásról. Tekintettel arra, hogy az SSCD védelmi profil választható lehetőségeiből legalább egy teljesül, s figyelembe véve a hardver hiba esetén biztonságos állapotba kerülés MICARDO v2.1 által megvalósított tulajdonságát (SF3.1, A tárolt adatok sértetlenségének monitorozása, szükség esetén közbelépés) is, a követelmény kielégítettnek tekinthető.
Következtetés	A MICARDO v2.1 **megfelel** az SSCD-PP „Az absztrakt gép tesztelése” követelményének.
Feltétel:	---

A BALE kisugárzása (FPT_EMSEC.1)	
Követelmény (CC SSCD-PP)	A BALE ***[behelyettesítés: meghatározott korlátok között]*** akadályozza meg az aláírás-létrehozó adat (magánkulcs), valamint a hitelesítő adat (PIN kód) megismerését lehetővé tévő ***[behelyettesítés: kisugárzás típusok]*** kisugárzódását. A BALE garantálja, hogy a ***[behelyettesítés: felhasználók típusa]*** nem képes a külső interfészek kisugárzásából a magánkulcsot, illetve a PIN kódot megismerni.
Infineon tulajdonság	Az SLE66CX320P chip helyes működése csak bizonyos tartományon belül garantált. A chip minden művelet végrehajtásakor ellenőrzi, hogy a környezeti körülmények elhagyták-e ezt a garantált tartományt, (s csak a pozitív esetben hajtja végre azt).
Ellenőrzött követelmények (Infineon ITSEC tanúsítás)	• helyesen működő SF1 biztonsági funkció (Működési állapot ellenőrzés).
MICARDO v2.1 tulajdonság	A MICARDO véd minden ismert hardver támadás ellen, hatékonyan alkalmazva a hardver (Infineon chip) által biztosított valamennyi mechanizmust, annak érdekében, hogy ne lehessen az intelligens kártyán tárolt vagy feldolgozott adatokat (különösen a magán aláíró kulcsot és a PIN kódot) felfedni, vagy észrevétlenül módosítani. A MICARDO garantálja, hogy a kriptográfiai műveletek során aktivizált egyetlen kulcsot sem lehet felfedni, s nem lehet a feldolgozott adatokra se következtetni A kártyán tárolt titkos kulcsról az aláírási folyamat során sem lehet információt nyerni. A MICARDO kezeli az összes olyan hardver alapú (a chip által támogatott) biztonsági mechanizmust, mely felhasználható a rejtett csatornák elemzésének a megakadályozására (mint amilyen az egyszerű és a differenciál áramfelvételi támadás /SPA és DPA/). Az intelligens kártya valamennyi kriptográfiai művelete él a hardver mechanizmusok támogatásával.
Ellenőrzött követelmények (MICARDO ITSEC tanúsítás)	• teljesülő SO2 biztonsági cél (Ellenállás a fizikai támadásoknak), • teljesülő SO4 biztonsági cél (A kriptográfia műveletek biztonsága), • helyesen működő SF7.2 biztonsági funkció (Rejtett csatorna vizsgálat ellenőrzés).
Értékelés	A MICARDO meghatározott (áram feszültségre és óra jel frekvenciára vonatkozó) korlátok között megakadályozza a magánkulcs, valamint a hitelesítő adat megismerését lehetővé tévő [SPA és DPA által kihasználható kisugárzás típusok] kisugárzódását. Így még a magas támadó potenciállal rendelkező támadók sem képesek a külső interfészek kisugárzásából a magánkulcsot, illetve a PIN kódot megismerni.
Következtetés	A MICARDO **megfelel** az SSCD-PP „A BALE kisugárzása” követelményének.
Feltétel:	---

A biztonságos állapot megőrzése hiba esetén (FPT_FLS.1)	
Követelmény (CC SSCD-PP)	A BALE őrizzen meg egy biztonságos állapotot, ha a következő típusú hibák lépnek fel: ***[behelyettesítés: hiba típusok listája]***
MICARDO tulajdonság	A MICARDO **megőriz egy biztonságos állapotot**, a következő típusú hibák bekövetkezése esetén: • **egy parancs végrehajtása során bekövetkező átmeneti vagy folyamatos hardver hiba,** • **fizikai támadás.** A MICARDO úgy reagál a fenti hibák észlelésekor, hogy biztonság politikája ne sérüljön (pl. az intelligens kártya megnyitott munkaszakasza ne maradjon használható a továbbiakban). A MICARDO v2.1 operációs rendszer hardver alapú (a chip által támogatott) biztonsági funkciókat és az ezeknek megfelelő mechanizmusokat használ a hardver hibák monitorozására és a biztonságos állapot érvényre juttatására.
Ellenőrzött követelmények (MICARDO ITSEC tanúsítás)	• teljesülő SO2 biztonsági cél (Ellenállás a fizikai támadásoknak), • helyesen működő SF7.1 biztonsági funkció (Hardver hiba elleni védelem).
Értékelés	A MICARDO SF7.1 biztonsági funkciója éppen a fenti elvárást teljesíti (hardver hiba és fizikai támadás hiba típusokra).
Következtetés	A MICARDO **megfelel** az SSCD-PP „A biztonságos állapot megőrzése hiba esetén” követelményének.
Feltétel:	---

A fizikai támadások passzív észlelése (FPT_PHP.1)	
Követelmény (CC SSCD-PP)	A BALE félreérthetetlen módon detektálja a biztonsági funkciók kompromittálódását okozható fizikai manipulálásokat. A BALE legyen képes detektálni, hogy fizikai manipulálás történt a biztonsági funkció elemeire, vagy az azt megalapozó eszközökre.
Infineon tulajdonság	Az SLE66CX320P chip helyes működése csak bizonyos tartományon belül garantált. A chip minden művelet végrehajtásakor ellenőrzi, hogy a környezeti körülmények elhagyták-e ezt a garantált tartományt, (s csak a pozitív esetben hajtja végre azt).
Ellenőrzött követelmények (Infineon ITSEC tanúsítás)	• helyesen működő SF1 biztonsági funkció (Működési állapot ellenőrzés).
MICARDO v2.1 tulajdonság	A MICARDO megőriz egy biztonságos állapotot, a következő típusú hibák bekövetkezése esetén: • egy parancs végrehajtása során bekövetkező átmeneti vagy folyamatos hardver hiba, • **fizikai támadás.** A MICARDO v2.1 operációs rendszer hardver alapú (a chip által támogatott) biztonsági funkciókat és az ezeknek megfelelő mechanizmusokat használ a hardver hibák monitorozására és a biztonságos állapot érvényre juttatására.
Ellenőrzött követelmények (MICARDO ITSEC tanúsítás)	• teljesülő SO2 biztonsági cél (Ellenállás a fizikai támadásoknak), • helyesen működő SF7.1 biztonsági funkció (Hardver hiba elleni védelem).
Értékelés	A MICARDO félreérthetetlen módon detektálja a biztonsági funkciók kompromittálódását okozható fizikai manipulálásokat. A MICARDO képes detektálni, hogy fizikai manipulálás történt a biztonsági funkció elemeire, vagy az azt megalapozó eszközökre.
Következtetés	A MICARDO **megfelel** az SSCD-PP „A fizikai támadások passzív észlelése” követelményének.
Feltétel:	---

A fizikai támadásokkal szembeni ellenálló képesség (FPT_PHP.3)	
Követelmény (CC SSCD-PP)	A BALE álljon ellen a ***[behelyettesítés: biztonsági funkció eszközök/ elemek listája]***-ra irányuló ***[behelyettesítés: fizikai manipulációs forgatókönyvek]***-nek olyan automatikus reagálással, ami megakadályozza a BALE biztonsági politikájának megsértését.
Infineon tulajdonság	Az SLE66CX320P chip helyes működése csak bizonyos tartományon belül garantált. A chip minden művelet végrehajtásakor ellenőrzi, hogy a környezeti körülmények elhagyták-e ezt a garantált tartományt, (s csak a pozitív esetben hajtja végre azt).
Ellenőrzött követelmények (Infineon ITSEC tanúsítás)	• helyesen működő SF1 biztonsági funkció (Működési állapot ellenőrzés).
MICARDO v2.1 tulajdonság	A MICARDO megőriz egy biztonságos állapotot, a következő típusú hibák bekövetkezése esetén: • egy parancs végrehajtása során bekövetkező átmeneti vagy folyamatos hardver hiba, • **fizikai támadás.** A MICARDO **úgy reagál a fenti hibák észlelésekor, hogy biztonság politikája ne sérüljön** (pl. az intelligens kártya megnyitott munkaszakasza ne maradjon használható a továbbiakban). A MICARDO v2.1 operációs rendszer hardver alapú (a chip által támogatott) biztonsági funkciókat és az ezeknek megfelelő mechanizmusokat használ a hardver hibák monitorozására és a biztonságos állapot érvényre juttatására.
Ellenőrzött követelmények (MICARDO ITSEC tanúsítás)	• teljesülő SO2 biztonsági cél (Ellenállás a fizikai támadásoknak), • helyesen működő SF7.1 biztonsági funkció (Hardver hiba elleni védelem).
Értékelés	A MICARDO ellenáll a ***chip-jére*** irányuló ***(áram feszültség és óra jel frekvencia manipulálásán alapuló támadásoknak***) olyan automatikus reagálással, ami megakadályozza biztonsági politikájának megsértését.
Következtetés	A MICARDO **megfelel** az SSCD-PP „A fizikai támadásokkal szembeni ellenálló képesség” követelményének.
Feltétel:	---

A biztonsági funkciók tesztelése (FPT_TST.1)	
Követelmény (CC SSCD-PP)	A BALE ***[választás: a kezdeti rendszer indítás során; a normál működés során periodikusan; egy jogosult felhasználó kérelme esetén; más feltételek fellépésekor]*** hajtson végre egy olyan teszt-sorozatot, mely kimutatja, hogy biztonsági funkciói helyesen működnek. A BALE biztosítsa, hogy az arra feljogosított felhasználók képesek legyenek a biztonsági funkció adatok sértetlenségének ellenőrzésére. A BALE biztosítsa, hogy az arra feljogosított felhasználók képesek legyenek az általa tárolt végrehajtható kódok sértetlenségét ellenőrizni.
Infineon tulajdonság	Az SLE66CX320P chip helyes működése csak bizonyos tartományon belül garantált. A chip minden művelet végrehajtásakor ellenőrzi, hogy a környezeti körülmények elhagyták-e ezt a garantált tartományt, (s csak a pozitív esetben hajtja végre azt). A chip önteszt szoftvere támogatja a helyes működés ellenőrzését: • a reset parancs kiadása után automatikusan lefutó inicializáló rutinok ellenőrzik a legfontosabb hardver elemeket (memóriák, CPU, stb.), • a normál üzemmódot tesztelő rutinok folyamatosan monitorozzák a helyes működést (pl. a tárolt adatok sértetlenségét). A chip hardver-vezérelt öntesztje nem indítható a felhasználói szoftverekből, az csak mintegy automatikus alap (háttér) ellenőrzésként áll rendelkezésre.
Ellenőrzött követelmények (Infineon ITSEC tanúsítás)	• helyesen működő SF1 biztonsági funkció (Működési állapot ellenőrzés).
MICARDO v2.1 tulajdonság	A MICARDO v2.1 operációs rendszernek nincs olyan parancsa, mellyel közvetlen hardver tesztelést lehetne kiváltani. Ugyanakkor a chip az általa feldolgozott parancsok visszatérési értékeiben jelzi, ha meghibásodott („MemoryFailureError”, UndefinedTechnicalProblem”, stb.). A host oldalról kiadható reset parancs pedig kiváltja a legszükségesebb hibaellenőrzési tesztrutinok futtatását. Az operációs rendszer SF3.1 biztonsági tulajdonsága pedig az egyik legveszélyesebb hardver hiba (a chip-ben tárolt adatok sértetlenségének elvesztése) folyamatos tesztelését magára vállalja.
Ellenőrzött követelmények (MICARDO ITSEC tanúsítás)	• helyesen működő SF3.1 biztonsági funkció (A tárolt adatok sértetlenségének monitorozása, szükség esetén közbelépés).

A biztonsági funkciók tesztelése (FPT_TST.1) /folytatás/	
Értékelés	A MICARDO ***a kezdeti rendszer indítás során (reset után egy általános inicializáló teszt rutint elindítva), valamint normál működése során (minden parancs feldolgozása során az ehhez szükséges hardver és tárolt adatelemeket ellenőrizve)*** végrehajt egy olyan teszt-sorozatot, mely kimutatja, hogy biztonsági funkciói helyesen működnek. A MICARDO indirekt módon biztosítja, hogy az arra feljogosított felhasználók képesek a biztonsági funkció adatok (attribútumok) sértetlenségének ellenőrzésére /azáltal, hogy bármely típusú attribútum (hozzáférési szabály, felhasználási cél, életciklus állapot) sérülése esetén az attribútumokra számított ellenőrző összeg hibát mutat, s ez az érintett objektumhoz való hozzáférést azonnal és véglegesen elérhetetlenné teszi/. A MICARDO nem tárol semmilyen végrehajtható kódot, így annak sértetlenség ellenőrzésének támogatása jelen esetben értelmetlen elvárás.
Következtetés	A MICARDO **megfelel** az SSCD-PP „A biztonsági funkciók tesztelése” követelményének.
Feltétel:	---

Megbízható csatorna (FTP_ITC.1) /A tanúsítvány-létrehozó alkalmazás, illetve az aláírás-létrehozó alkalmazás felé./	
Követelmény (CC SSCD-PP)	1. A BALE biztonsági funkciói biztosítsanak egy olyan kommunikációs csatornát a BALE és egy távoli megbízható informatikai termék ***(a tanúsítvány generáló alkalmazás)*** között, mely logikailag különbözik a többi kommunikációs csatornától, egyúttal biztosítja végpontjainak garantált azonosítását és a továbbított adatok illetéktelen felfedés és módosítás elleni védelmét. A BALE engedje meg, hogy a megbízható csatornán való kommunikációt ***[választás: a BALE, a távoli informatikai termék]*** kezdeményezze. A BALE ***vagy a távoli informatikai termék (a tanúsítvány generáló alkalmazás)*** ezen a biztonságos csatornán kezdeményezzen kommunikációt az alábbi esetekhez: • aláírás-ellenőrző adat (nyilvános kulcs) exportálása (a tanúsítvány-létrehozó alkalmazás felé), 2. A BALE biztonsági funkciói biztosítsanak egy olyan kommunikációs csatornát a BALE és egy távoli megbízható informatikai termék ***(az aláírás-létrehozó alkalmazás)*** között, mely logikailag különbözik a többi kommunikációs csatornától, egyúttal biztosítja végpontjainak garantált azonosítását és továbbított adatok illetéktelen felfedés és módosítás elleni védelmét. A BALE engedje meg, hogy a megbízható csatornán való kommunikációt ***a távoli informatikai termék (az aláírás-létrehozó alkalmazás)*** kezdeményezze. A BALE ***vagy a távoli informatikai termék (az aláírás-létrehozó alkalmazás)*** ezen a biztonságos csatornán kezdeményezzen kommunikációt az alábbi esetekhez: • aláírandó adat reprezentáns fogadása (az aláírás-létrehozó alkalmazástól).

Megbízható csatorna (FTP_ITC.1) /folytatás/ /A tanúsítvány-létrehozó alkalmazás, illetve az aláírás-létrehozó alkalmazás felé./	
MICARDO tulajdonság	A MICARDO képes megbízható csatornát kiépíteni, melyen keresztül az intelligens kártya szolgáltatásait felhívó programok (köztük a tanúsítvány-létrehozó alkalmazás és az aláírás-létrehozó alkalmazás) biztonságosan kommunikálhatnak vele, mivel a továbbítás során megvédi az alkalmazások és az intelligens kártya között kicserélt adatok: • bizalmasságát (rejtjelezéssel), • hitelességét és sértetlenségét (kriptográfiai ellenőrzőösszeg képzéssel). Mind a nyilvános kulcs exportálásához, mind az aláírandó adat reprezentáns importálásához használható (és a 12. feltétel szerint használandó is) ez a megbízható csatorna (bizalmasságot, hitelességet és sértetlenséget biztosító titkos üzenetváltás). A MICARDO elvi felépítése miatt, mindkét fenti esetben a távoli informatikai terméknek (a tanúsítvány generáló alkalmazásnak, illetve az aláírás-létrehozó alkalmazásnak) kell kezdeményeznie a megbízható csatorna kiépítését.
Ellenőrzött követelmények (MICARDO ITSEC tanúsítás)	• teljesülő SO5 biztonsági cél (A továbbított adatok sértetlensége és hitelessége), • helyesen működő SF5.1 biztonsági funkció (Adat csere bizalmasság), • helyesen működő SF5.2 biztonsági funkció (Adat csere hitelesség és sértetlenség).
Értékelés	A 12. feltétel teljesítése esetén (melyet a MICARDO támogat) kiépülő megbízható csatorna biztosítja végpontjainak garantált azonosítását és a továbbított adatok (nyilvános kulcs és aláírandó adat reprezentáns) illetéktelen felfedés és módosítás elleni védelmét. A megbízható csatornán való kommunikáció külső kezdeményezésének kötöttsége nem mond ellen az elvárásnak, csak szűkíti annak választási lehetőségét (a MICARDO nem képes kezdeményezni).
Következtetés	A MICARDO (a feltételek betartása esetén) **megfelel** az SSCD-PP „Megbízható csatorna” követelményének.
Feltétel:	12.

Megbízható útvonal (FTP_TRP.1) /A helyi felhasználó és a BALE között./	
Követelmény (CC SSCD-PP)	A BALE biztonsági funkciói biztosítsanak egy olyan kommunikációs útvonalat a BALE 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 BALE engedje meg, hogy a megbízható útvonalon való kommunikációt ***[választás: a BALE, a helyi felhasználók]*** kezdeményezze. A BALE követelje meg ennek a biztonságos útvonalnak a használatát az alábbi esetekben ***[választás: kezdeti felhasználói hitelesítés, [behelyettesítés: más szolgáltatások, melyekhez a megbízható útvonal megkövetelt]]***.
MICARDO tulajdonság	A MICARDO képes megbízható útvonalat kiépíteni, melyen keresztül az intelligens kártyával a helyi felhasználók (az aláíró és az adminisztrátor) biztonságosan kommunikálhatnak, mivel a továbbítás során megvédi a helyi felhasználók és az intelligens kártya között kicserélt adatok: • bizalmasságát (rejtjelezéssel), • hitelességét és sértetlenségét (kriptográfiai ellenőrzőösszeg képzéssel). Mind a kezdeti felhasználói hitelesítéshez (PIN kód vagy jelszó megadáshoz), mind a hitelesítési adatok (PIN kód vagy jelszó) cseréjéhez használható (és a 12. feltétel szerint használandó is) ez a megbízható útvonal (bizalmasságot, hitelességet és sértetlenséget biztosító titkos üzenetváltás). A MICARDO elvi felépítése miatt a helyi felhasználónak (pontosabban a nevében eljáró host oldali alkalmazásnak) kell kezdeményeznie a megbízható útvonal kiépítését.
Ellenőrzött követelmények (MICARDO ITSEC tanúsítás)	• teljesülő SO5 biztonsági cél (A továbbított adatok sértetlensége és hitelessége), • helyesen működő SF5.1 biztonsági funkció (Adat csere bizalmasság), • helyesen működő SF5.2 biztonsági funkció (Adat csere hitelesség és sértetlenség).

Megbízható útvonal (FTP_TRP.1) /folytatás/ /A helyi felhasználó és a BALE között./	
Értékelés	A 12. feltétel teljesítése esetén (melyet a MICARDO támogat) kiépülő megbízható útvonal biztosítja végpontjainak garantált azonosítását és a továbbított adatok (PIN kód vagy jelszó) illetéktelen felfedés és módosítás elleni védelmét. A megbízható útvonalon való kommunikáció külső kezdeményezésének kötöttsége nem mond ellen az elvárásnak, csak szűkíti annak választási lehetőségét (a MICARDO nem képes kezdeményezni). A MICARDO-nak (a 12. feltétel szerint) az alábbi esetekben kell megkövetelnie a biztonságos útvonal használatát: • kezdeti felhasználói hitelesítés, • a hitelesítési adatok cseréje.
Következtetés	A MICARDO (a feltételek betartása esetén) **megfelel** az SSCD-PP „Megbízható útvonal” követelményének.
Feltétel:	12.

Az alábbi táblázat az egyes biztonsági követelmények teljesülésének feltételeit foglalja össze.

Funkcionális biztonsági követelmények	A teljesülést elősegítő feltételek
FCS_CKM.1 Kriptográfiai kulcs generálás	5., 6.
FCS_CKM.4 Kriptográfiai kulcs megsemmisítés	8.
FCS_COP.1 Kriptográfiai eljárás	14.
FDP_ACC.1 Részleges hozzáférés ellenőrzés	14.
FDP_ACF.1 Biztonsági jellemzőkön alapuló hozzáférés ellenőrzés	14.
FDP_RIP.1 Részleges maradvány információ védelem	---
FDP_SDI.2 A tárolt adatok sértetlenségének figyelése és beavatkozás	---
FDP_UIT.1 Az adatcsere sértetlensége	12
FIA_AFL.1 A hitelesítési hiba kezelése	13
FIA_ATD.1 A felhasználói jellemzők meghatározása	---
FIA_UID.1 Az azonosítás időzítése	14
FIA_UAU.1 A hitelesítés időzítése	14
FMT_MOF.1 A biztonsági funkciók viselkedésének kezelése	14.
FMT_MSA.1 A biztonsági jellemzők kezelése	14.
FMT_MSA.2 Biztonságos biztonsági jellemzők	14., 15.
FMT_MSA.3 Statikus jellemző inicializálás	14.
FMT_MTD.1 A biztonsági funkciók adatainak kezelése	14.
FMT_SMR.1 Biztonsági szerepkörök	14.
FPT_AMT.1 Az absztrakt gép tesztelése	---
FPT_EMSEC.1 A BALE kisugárzása	---
FPT_FLS.1 A biztonságos állapot megőrzése hiba esetén	---
FPT_PHP.1 A fizikai támadások passzív észlelése	---
FPT_PHP.3. A fizikai támadásokkal szembeni ellenálló képesség	---
FPT_TST.1 A biztonsági funkciók tesztelése	---
FTP_ITC.1 Megbízható csatorna	12.
FTP_TRP.1 Megbízható útvonal	12.

6.2 A MICARDO megfelelése az SSCD védelmi profil garanciális biztonsági követelményeinek

Az ITSEC garanciális szintjei közvetlenül megfeleltethetőek a CC /Közös szempontrendszer/ értékelési garancia szintjeinek, az alábbi módon:

ITSEC	CC
E0	EAL 1
E1	EAL 2
E2	EAL 3
E3	EAL 4
E4	**EAL 5**
E5	EAL 6
E6	EAL 7

A táblázat vastag betűkkel jelzett sorából adódik a MICARDO v2.1 megfelelése az EAL4-es garancia szintű SSCD védelmi profilnak (minthogy az egyes EAL szintek hierarchikusak, azaz a nagyobb szintek mindig tartalmazzák az alacsonyabb szintek összes komponensét).

A MICARDO intelligens kártya megfelel a 3-as típusú BALE-re vonatkozó EAL4-es garancia szintű védelmi profilnak /Protection Profile – Secure Signature-Creation Device Type 3, version: 1.05, EAL4/.

A 3-as típusú BALE-re készült, garanciális biztonság szempontjából még szigorúbb változat (EAL4+) néhány olyan garanciális komponens kielégítését is elvárja, melyet az EAL4 még nem. Ezek közül pl. az életciklus támogatására megkövetelt ALC_DVS.2 /A biztonsági intézkedések elégségessége/ csak EAL6-tól (illetve ITSEC E5-től) megkövetelt elvárás. Erre a követelményre nem terjedt ki az ITSEC értékelés, ezért a garanciális biztonság szempontjából szigorúbb változatnak (EAL4+) való megfelelőség nem mondható ki.

7. A Tanúsítási jelentés eredménye és érvényességi feltételei

7.1 A Tanúsítási jelentés eredménye

Az SLE66CX320P mikrochip-ből
és a MICARDO operációs rendszerből álló
intelligens kártya
/Infineon Technologies AG, Germany, ORGA Kartensysteme GmbH, Germany/

tanúsítás tárgyát képező verziója

/chip:	SLE66CX320P / m1421b25,
operációs rendszer:	v 2.1 64/32 R1.0/

a tanúsítás érvényességi feltételeinek[14] együttes teljesülése esetén

ALKALMAS

minősített aláírások létrehozására,

mint

3-as típusú biztonságos aláírás-létrehozó eszköz.

[14] Lásd a 7.2 “Az eredmények érvényességi feltételei” alfejezet 1.-17 feltételeit.

7.2 Az eredmények érvényességi feltételei

Az SLE66CX320P mikrochip-ből és a MICARDO v2.1 operációs rendszerből álló (MICARDO) intelligens kártya egy bonyolult kriptográfiai eszköz, melyet fejlesztői úgy terveztek, hogy minél általánosabb feltételek között legyen használható, s a felhasználói igények minél szélesebb körét legyen képes kielégíteni. Ennek megfelelően számos biztonsági tulajdonság konfigurálható be, illetve ki rajta.

Amennyiben a MICARDO intelligens kártyát minősített aláírások létrehozására kívánják felhasználni, olyan biztonsági követelményeknek kell megfelelni, melyek a felhasználhatóságot korlátozzák, különböző feltételek betartását követelik meg.

Tovább bonyolítja a helyzetet, hogy a MICARDO intelligens kártya nem támogat kártyán tárolt végrehajtható kódokból álló alkalmazásokat, az alkalmazásokat kizárólag a host oldalról kiadott, szabványos (és az operációs rendszer által támogatott, értelmezett és a chip segítségével végrehajtott) parancsok megfelelő sorozatával lehet megvalósítani. Ez a filozófiai megközelítés bizonyos szempontból növeli a felhasználhatóság rugalmasságát, ugyanakkor számos biztonsági veszélyt is okoz, mivel
a host oldalról akár nem biztonságos konfigurálások is beállíthatók, elérhetők. Ezen veszélyek megnyugtató kivédése (legalább a felhasználói fázisra) további szigorításokat, extra feltételeket kíván meg.

Az alábbiakban összefoglaljuk azokat a feltételeket, melyek **együttes** betartása feltétele a MICARDO intelligens kártya BALE-ként való felhasználásának.

7.2.1 Általános érvényességi feltételek

Az alábbi feltételek minden felhasználási mód esetén (tehát a fejlesztő-gyártó cég által igen általánosra tervezett felhasználási kör egészében) szükségesek a megbízható és biztonságos működéshez.

1. A MICARDO intelligens kártya szolgáltatásait igénybe vevő adminisztrátorok és felhasználók (aláírók) jól képzettek és megbízhatóak.

2. A MICARDO intelligens kártya szolgáltatásait igénybe vevő adminisztrátorok és felhasználók betartják a különböző útmutatók **(**döntően a MICARDO Public Chip Card Operating System v2.1 User Manual**)** által előírt, alábbi kötelező tevékenységeket:
   - a tulajdonosok titokban tartják saját PIN kódjukat,
   - az aláírók PIN kód hosszúsága legalább 6 digit legyen,
   - a PIN kódokat nem szabad megjeleníteni a terminálon adatbevitel közben,

3. A külvilág és az intelligens kártya közötti bizalmas adatcsere esetén titkos üzenetváltást kell megvalósítani (a parancsra és válaszára megvalósított MAC képzéssel és kódolással).

4. A külvilágban tárolt (hitelesítéshez vagy titkosításhoz használt) kulcsok titkosságáért a felhasználók felelősek. Számukra a következők erősen ajánlottak:
   - a kulcsokat tartalmazó adatterületeket védeni kell az illetéktelen kiolvasás és módosítás ellen,
   - a kulcsokat kompromittálódásuk esetén azonnal cserélni vagy blokkolni kell ,
   - kulcsok továbbítása az intelligens kártyára mindig titkos üzenettel történjen.

7.2.2 Az ITSEC tanúsítások érvényességi feltételei

Az alábbi feltételek ahhoz elengedhetetlenek, hogy a MICARDO v2.1 intelligens kártya megfeleljen az ITSEC E4-es biztonsági szintjének.

5. A digitális aláírással kapcsolatos kriptográfiai funkcionalitást az alábbi algoritmusra kell korlátozni: **RSA (1024 bites kulcsméret, PKCS #1-es aláírás formátum, SHA-1 lenyomatképzés)**[15].

6. A MICARDO és a külvilág közötti titkos üzenetváltáshoz a **Triple DES** algoritmust alkalmazzák **(**a MICARDO által támogatott 112 bites kulcsméretben).

7.2.3 A biztonságos aláírás-létrehozó eszközként történő használhatóság kiegészítő feltételei

Egy minősített aláírásokat létrehozó aláírónak a MICARDO v2.1 felhasználása során az alábbi kiegészítő feltételeket is be kell tartania:

7. A BALE-ként használt MICARDO intelligens kártyának csak egy felhasználója lehet, az aláíró[16].

8. A minősített aláírások létrehozására használt magánkulcsot érvényességének lejárta után az első lehetséges alkalommal törölni kell[17].

9. A minősített aláírások létrehozására használt magánkulcs hozzáférési szabályait úgy kell beállítani a perszonalizálás folyamatában, hogy a későbbiekben azzal a felhasználó (aláíró) csak aláírni tudjon. (Ne lehessen titkosításra /pontosabban dekódolásra/ vagy hitelesítésre felhasználni.)

10. A minősített aláírások létrehozására használt magánkulcsot ne lehessen menteni.

[15] Mert az ITSEC értékelés csak erre az algoritmusra vonatkozott, bár a chip támogatja a DSA aláíró algoritmust is.
[16] A MICARDO v2.1 képes több (vég)felhasználót is kezelni egy kártyán.
[17] Amennyiben új tanúsítvány kérelme vagy más célból az aláíró eszközével megjelenik a hitelesítés-szolgáltatónál, az adminisztrátor felelőssége (mert csak neki van jogosultsága rá) a kártyán lévő, már érvénytelen magánkulcsok fizikai megsemmisítése (törlése).

11. A minősített aláírások létrehozására használt magánkulccsal csak minősített aláírást szabad létrehozni. (Így nem szabad fokozott biztonságú aláírás-létrehozására felhasználni.)

12 Bizalmasságot, hitelességet és sértetlenséget biztosító titkos üzenetváltást kell biztosítani (a Triple DES algoritmus felhasználásával) a következő esetekben:
- az aláírandó adatreprezentáns intelligens kártyára küldésekor (aláírás céljából),
- a nyilvános kulcs intelligens kártyáról való fogadásakor (tanúsítványba foglalás céljából).
- kezdeti felhasználói hitelesítéskor (a PIN kód vagy a jelszó megadásához),
- a hitelesítési adatok (PIN kód vagy jelszó) cseréjéhez.

13 A biztonsági attribútumok inicializálásakor biztosítani kell az alábbiakat:
- A retry counter alapértéke 3 legyen.
- A retry counter reset-elési funkciójához csak az adminisztrátornak legyen joga.

14. Egy BALE-ként használt MICARDO esetén az adminisztrátor és felhasználó (aláíró) szerepkörök szétválasztásával, valamint az inicializálási, perszonalizálási folyamatoknál alkalmazott programok és rezsim szabályok együttműködésével biztosítani kell a következőket:
    1. az „aláíró” vagy az „adminisztrátor” generálja az aláírói kulcspárt, ennek felhasználását pedig az „adminisztrátor” engedélyezze,
    2. a folyamat során az „adminisztrátor” végrehajt egy páronkénti megfelelőség tesztet (az aláíráshoz generált nyílt – magánkulcs pár összetartozásának ellenőrzését), és csak sikeres eredmény esetén adható ki tanúsítvány, illetve maga a BALE,
    3. az „aláíró” vagy az „adminisztrátor” exportálja a legenerált nyilvános kulcsot tanúsítvány készítés céljából,
    4. csak az „aláíró” aktivizálhatja magánkulcsát (aláírásra),
    5. a sikeres folyamat végén a felhasználónak (aláírónak) átadott intelligens kártyára teljesül, hogy minden biztonsági attribútum biztonságos értéket vesz fel, s így hagyja el a hitelesítés-szolgáltató védett környezetét (a felhasználói környezetben ez a későbbiekben már nem változtatható meg)[18]

[18] Egy lehetséges (de nem kizárólagos) példa az alábbi:
Az adminisztrátor és a leendő felhasználó (aláíró) együttes jelenlétében:
- az adminisztrátor előzetesen inicializálta az aláíró (felhasználó) kezdeti PIN kódját,
- az adminisztrátor átadja a felhasználónak az intelligens kártyát és megadja a kezdeti PIN kód értékét is,
- a felhasználó (aláíró) azonnal lecseréli saját PIN kódját,
- a felhasználó legenerálja saját (aláírói) kulcspárját,
- a felhasználó exportálja a legenerált nyilvános kulcsot,
- az adminisztrátor elvégezteti a páronkénti megfelelőség tesztet (sikertelenség esetén a folyamat megszakad),
- az adminisztrátor tanúsítvány kérelmet állít ki és küld el az adott nyilvános kulcsra,
- a (hitelesítés-szolgáltatótól) visszakapott tanúsítványt az adminisztrátor rátölti a kártyára,
- az adminisztrátor a „magánkulcs aktivizálás” biztonsági jellemzőt „igen” értékre állítja (aktiválva a magánkulcsot tartalmazó fájlt),
- minden további biztonsági attribútumot az adminisztrátor által felügyelt program biztonságosra állít be,

/Azon elvárás, hogy minden biztonsági attribútum biztonságos értéket vesz fel, magában foglalja az alábbi követelményeket is:

- a PIN kódokat megfelelő hozzáférési szabályokkal védve, biztonságosan tárolják az intelligens kártyán,
- valamennyi digitális aláírással kapcsolatos parancs végrehajtása csak sikeres jelszó alapú felhasználói azonosítás és hitelesítés után legyen lehetséges (a megfelelő fájlok „sikeres jelszó alapú felhasználói hitelesítés után" hozzáférési feltétel beállításával)./

6. technikai vagy rezsim intézkedésekkel biztosítani kell, hogy egy már kulcsokkal ellátott, de még nem az aláíró személyes felügyelete alá tartozó intelligens kártyával harmadik személy ne élhessen vissza jogosulatlanul.

15. A hitelesítés-szolgáltató által működtetett, inicializálást, perszonalizálást végző, esetenként nem biztonságos attribútum beállításokat is működtető alkalmazásra egy a fejlesztőktől független, elektronikus aláírás termékek biztonsági értékelésére/tanúsítására felhatalmazott szervezet értékelési eredménye állapítsa meg, hogy az alkalmazás kielégíti a 7. - 10., valamint a 12. - 14. feltételeket.[19]

16. Az aláíró csak megbízható aláírás-létrehozó alkalmazást használhat.

17. A Tanúsítvány csak a jelenlegi verzióra érvényes
/chip: SLE66CX320P / m1421b25, operációs rendszer: v 2.1 64/32 R1.0/

Új chip verzió esetén mind a chip-re, mind az operációs rendszerre új tanúsítás szükséges.

- az adminisztrátor átadja az aláírónak a kártyát.

[19] A 15. feltétel indoklása:
A MICARDO intelligens kártya nem támogat kártyán tárolt végrehajtható kódokból álló alkalmazásokat, az alkalmazásokat kizárólag a host oldalról kiadott, szabványos (és az operációs rendszer által támogatott, értelmezett és a chip segítségével végrehajtott) parancsok megfelelő sorozatával lehet megvalósítani.
Ez a filozófiai megközelítés bizonyos szempontból növeli a felhasználhatóság rugalmasságát, ugyanakkor számos biztonsági veszélyt is okoz, mivel a host oldalról akár nem biztonságos konfigurálások is beállíthatók, elérhetők. Még az elektronikus aláírásról szóló 2001. évi XXXV. törvény 1. sz. mellékletében a biztonságos aláírás-létrehozó eszközre vonatkozó igen általános követelmények is sérülhetnek, nemcsak az SSCD védelmi profil elvárásai:

- az aláírás készítéséhez használt aláírás-létrehozó adat titkossága is sérülhet
- az aláírás-létrehozó adat jogosulatlan felhasználókkal szembeni védelme sem biztosított.

/Például egy kulcs pár generálására a felhasználói kézikönyv az alábbi, egymást követő lépéseket javasolja:

1. új könyvtár létrehozása az adatfájlok számára (DF, valamint megfelelő strukturális információkkal feltöltött EF-k),
2. az új adatmezők feltöltése,
3. a hozzáférési jogok módosítása (ezt követően a magánkulcs információkhoz nem lehetséges a hozzáférés),
4. kulcs generálása,
5. a nyilvános kulcs kiolvasása

A felhasználói útmutató is felhívja a figyelmet arra, hogy amennyiben a fenti 3. lépés kimarad, a magánkulcs módosítható vagy olvasható marad!/
A fenti (igen súlyos) veszélyek megnyugtató kivédése indokolja a szolgáltató által használt alkalmazásra vonatkozó szigorító feltételt.

Amennyiben csak az operációs rendszer változik, elég egy olyan új, az operációs rendszerre vonatkozó tanúsítás, mely a régi chip verziót megnevezi.
Mindkét fenti esetben szükséges az új verzió BALE-ként való felhasználhatóságát egy erre kijelölt hazai tanúsító szervezettel ismételten tanúsíttatni.

8. Felhasznált 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+

ITSEC: Information Technology Security Evaluation Criteria, version 1.2 (1991)

ITSEM: Information Technology Security Evaluation Manual, version 1.0 (1993)

8.2 A tanúsítási jelentéshez figyelembe vett egyéb dokumentumok

Kérelem /a tanúsítás elvégzésére/

Kérdőív a tanúsítás kérelmezéséhez

BSI-DSZ-ITSEC-0175-2002 Certification
/Smart Card IC SLE66CX320P / m1421b25/

BSI-DSZ-ITSEC-0175-2002 Certification Report
/Smart Card IC SLE66CX320P / m1421b25/

TUVIT-DSZ-ITSEC-9126-2001 Certification
/MICARDO Public Version 2.1 64/32 R1.0/

TUVIT-DSZ-ITSEC-9126-2001 Certification Report
/Smart Card Operating System MICARDO Public Version 2.1 64/32 R1.0/

ORGA: MICARDO Public Chip Card Operating System v2.1 User Manual

9. Rövidítések

ACE	Advenced Crypto Engine
BALE	Biztonságos aláírás-létrehozó eszköz
BSI	Bundesamt für Sicherheit in der Informationtechnik
CC	Common Criteria
CEN	European Comittee for Standardization
CPU	Central Processing Unit
CRC	Cyclic Redundancy Check
DES	Data Encryption Standard /FIPS PUB 46-3, FIPS PUB 74, FIPS PUB 81/
DF	Dedicated file
DPA	Differencial Power Attack
DSA	Digital Signature Algorithm /FIPS PUB 186-2/
EAL	Evaluation Assurance Level
EEPROM	Electrically Erasable Programmable Read Only Memory
EF	Elementary file
IEC	International Electrotechnical Comission
IRAM	Internal Random Access Memory
ISO	International Organization for Standardization
ITSEC	Information Technology Security Evaluation Criteria
ITSEM	Information Technology Security Evaluation Manual
MAC	Message Authentication Code
MED	Memory Encryption and Decryption unit
MF	Master file
MMU	Memory Management Unit
PIN	Personal Identification Number
PKCS	Public Key Cryptographic Standards
PKCS #1	RSA Cryptography Standard
PP	Protection Profile
RAM	Random Access Memory
ROM	Read Only Memory
RMS	Resource Management System
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)
STS	Self Test Software
Triple-DES	/FIPS PUB 46-3, ANSI X9.52/
XRAM	eXtended Random Access Memory