Tanúsítási jelentés

Hung-TJ-011-2003

**A P8WE5032v0G mikrochip-ből,
STARCOS SPK 2.3 v 7.0 operációs rendszerből,
valamint a
StarCert v 2.2 digitális aláírás alkalmazásból
álló
intelligens kártya
mint**

biztonságos aláírás-létrehozó eszköz

**/Philips Semiconductors GmbH, Germany,
Giesecke & Devrient GmbH, Germany/**

Tartalom

1. Bevezetés *5*

1.1 A tanúsítási jelentés tárgya **5**

1.2 A tanúsítási jelentés feladata **6**

1.3 A tanúsítási jelentés hatóköre **6**

1.4 A tanúsítási jelentés szerkezete **6**

2. Egy 3-as típusú BALE-re vonatkozó CC követelmények az SSCD védelmi profil szerint *8*

2.1 Egy 3-as típusú BALE biztonsági környezete **8**

2.1.1 A biztonságra irányuló veszélyek 8

A fizikai környezet sebezhetőségének kihasználása 8

A magánkulcs letárolása, lemásolása 8

Az aláírás-létrehozás adatok származtatása 8

Az aláírás-létrehozó adat kiszivárgása 8

Az elektronikus aláírás hamisítása 9

Az elektronikus aláírások letagadása 9

Az aláírás-ellenőrző adatok hamisítása 9

Az aláírandó adat reprezentánsának meghamisítása 9

Visszaélés a BALE aláírás-létrehozó funkciójával 9

2.1.2 Érvényre juttatandó biztonsági szabályok 9

Szakértő támadók 9

Minősített tanúsítvány 9

A rendszer teljes életciklusára kiterjedő biztonság 10

A BALE, mint biztonságos aláírás-létrehozó eszköz 10

2.2 Egy 3-as típusú BALE biztonsági céljai **10**

Fizikai kisugárzás elleni védelem 10

Aláírás-létrehozó / aláírás-ellenőrző adatpárok generálása 10

Az életciklus biztonsága 10

Az aláírás-létrehozó adatok titkossága 10

Az aláírás-ellenőrző és az aláírás-létrehozó adat közötti megfelelés 10

Az aláírás-ellenőrző adat hitelességének biztosítása 11

A módosítás detektálása 11

A fizikai módosítással szembeni ellenállás 11

Az aláírás-létrehozó adatok egyedisége 11

Az aláírandó adat-reprezentáns sértetlenségének ellenőrzése 11

Az aláírás előállítási funkció csak a törvényes aláírónak áll rendelkezésre 11

Az elektronikus aláírás kriptográfiai biztonsága 11

2.3 Egy 3-as típusú BALE funkcionális biztonsági követelményei **12**

2.4. Egy 3-as típusú BALE garanciális biztonsági követelményei **13**

3. A STARCOS speciális tulajdonságai *14*

4. A STARCOS operációs rendszerre és a StarCert digitális aláírás alkalmazásra vonatkozó ITSEC tanúsítvány eredményeinek összefoglalása *17*

4.1 Az ITSEC értékelés eredményei **17**

4.2 Megvédett értékek **17**

4.2.1 Objektumok 17
4.2.2 Alanyok (szubjektumok) 17
4.2.3 Hozzáférés típusok (az alanyok és objektumok között) 18

4.3 A környezetre vonatkozó feltételezések 19
4.3.1 A teljes életciklus biztonságára vonatkozó feltételezések (AE1) 19
4.3.2 A (külső) kulcsok sértetlenségére és minőségére vonatkozó feltételezések (AE2) 19
4.3.3 A felhasználásra módjára vonatkozó feltételezések (AE3) 20
4.3.4 A felhasználás környezeti biztonságára vonatkozó feltételezések (AE4) 21
4.3.5 Az intelligens kártya hardverére (chip) vonatkozó feltételezések (AE5) 22

4.4 Kivédett fenyegetések 23
T1 A kártyatulajdonos aláírói magánkulcsának jogosulatlan felfedése vagy módosítása 23
T2 Visszaélés az aláírás funkcióval 23
T3 A kártyatulajdonos adatainak meghamisítása 23

4.5 Teljesített biztonsági célok 23
SO1 A kártyatulajdonos aláírói magánkulcsának védelme 23
SO2 A digitális aláírás funkció jogosulatlan használatának megakadályozása 23
SO6 A kulcsgenerálás minősége 24
SO7 Biztonságos digitális aláírás szolgáltatása 24
SO8 A biztonság potenciális megsértésére való reagálás 24

4.6 A biztonságot érvényre juttató funkciók (biztonsági funkciók) 25
Azonosítás és hitelesítés (IA) 25
IA1: Az emberi felhasználó hitelesítése 25
IA2: A hitelesítő adat cseréje 25
IA3: A hitelesítő adat blokkolása 25
IA4: A blokkolt hitelesítő adat feloldása és cseréje 25
Hozzáférés ellenőrzés (AC) 25
AC1: A parancsokhoz való hozzáférés ellenőrzése 25
AC2: A felfedés hozzáférés ellenőrzése 27
AC3: Blokkolt állapot 27
Naplózás (AU) 27
AU1: Információ a blokkolt állapotról 27
AU2: Információ a kártyatulajdonos hitelesítésének blokkoltságáról 27
Objektum újrahasználat (OR) 27
OR1: Érzékeny adatok törlése az átmeneti tárolókban 27
Adat csere (DX) 28
DX1: Kulcs generálása és exportálása 28
DX2: Digitális aláírás létrehozása 28

5. A mikrochip-re vonatkozó ITSEC tanúsítvány eredményeinek összefoglalása ... 30

5.1 Az ITSEC értékelés eredményei 30

5.2 A mikrochip alkotó elemei 30
5.2.1 A P8WE5032v0G mikrochip hardver alkotó elemei 30
5.2.2 A P8WE5032v0G mikrochip förmver alkotó elemei 31
5.2.3 A P8WE5032v0G mikrochip szoftver alkotó eleme 31

5.3 A mikrochip legfontosabb tulajdonságai (biztonsági funkciók) 31
Véletlenszám generátor (F1): 31
Triple-DES társprocesszor (F2) 31
RSA megvalósítás beépített aritmetikai alapfunkciókkal (F3) 32
Működési állapot ellenőrzés (F4) 32
A fizikai manipuláció elleni védelem (F5) 32
Az üzemmód és a konfiguráció védelme (F6) 32

6. A STARCOS intelligens kártya megfelelése az SSCD védelmi profil követelményeinek 33

6.1 A STARCOS intelligens kártya megfelelése az SSCD védelmi profil funkcionális biztonsági követelményeinek 33

6.2 A STARCOS megfelelése az SSCD védelmi profil garanciális biztonsági követelményeinek 69

7. A Tanúsítási jelentés eredménye és érvényességi feltételei 70

7.1 A Tanúsítási jelentés eredménye 70

7.2 Az eredmények érvényességi feltételei 71

7.2.1 Általános érvényességi feltételek 71

7.2.2 Az ITSEC tanúsítások érvényességi feltételei 71

7.2.3 A biztonságos aláírás-létrehozó eszközként történő használhatóság kiegészítő feltételei 71

8. Felhasznált dokumentumok 74

8.1 Termékmegfelelőségi követelményeket tartalmazó dokumentumok 74

8.2 A tanúsítási jelentéshez figyelembe vett egyéb dokumentumok 74

9. Rövidítések 75

1. Bevezetés

1.1 A tanúsítási jelentés tárgya

Jelen tanúsítási jelentés tárgya egy olyan intelligens kártya, mely egy P8WE5032v0G mikrochip-et, egy ebbe ágyazott STARCOS SPK 2.3 v 7.0 operációs rendszert, valamint egy StarCert v 2.2 digitális aláírás alkalmazást tartalmaz (a későbbiekben erre a termékre "**STARCOS**" vagy „**STARCOS 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 STARCOS 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 STARCOS intelligens kártyára vonatkozó értékelési és tanúsítási eredmények (a mikrochip-re, valamint az operációs rendszerre és különböző alkalmazásaira 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 STARCOS 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 STARCOS egyéb tulajdonságaira (pl. titkosításra való felhasználhatóságára).

1.4 A tanúsítási jelentés szerkezete

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

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 juttatandó biztonsági szabályok), biztonsági célok, funkcionális és garanciális követelmények/ (2. fejezet).
- A STARCOS intelligens kártya néhány különleges tulajdonsága (3. fejezet).
- A STARCOS operációs rendszerre és a StarCert digitális aláírás alkalmazásra vonatkozó ITSEC tanúsítvány eredményei (4. fejezet).
- A STARCOS mikrochip-jére vonatkozó ITSEC tanúsítvány eredményei (5. fejezet).
- Az SSCD védelmi profil követelményeinek kimutatása a STARCOS 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 STARCOS 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 garanciaösszetevőit.

Garanciaosztályok	Garanciacsaládok és garanciaösszetevők az EAL 4 /**EAL4+**/ szintű értékelésénél
A konfiguráció menedzselése	ACM_AUT.1 A konfigurációmenedzselés részleges automatizálása
	ACM_CAP.4 A szoftver telepítést támogató és elfogadó eljárások
	ACM_SCP.2 A problémakövető konfigurációmenedzselés lefedettsége
Kiszállítás és üzemeltetés	ADO_DEL.2 A módosítások észlelése
	ADO_IGS.1 Hardver-telepítés, szoftver-telepítés, beindítás eljárásai
Fejlesztés	ADV_FSP.2 Teljesen meghatározott külső interfészek
	ADV_HLD.2 Felsőszintű tervezést érvényesítő biztonság
	ADV_IMP.2 Az értékelés tárgya biztonsági funkcióinak kivitelezése /csak EAL5-től megkövetelt/[6]
	ADV_LLD.1 Az alsószintű 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**[7]**/**
	ALC_LCD.1 A fejlesztő által meghatározott életciklus-modell
	ALC_TAT.1 Jól meghatározott fejlesztőeszközök
Vizsgálatok	ATE_COV.2 A lefedettség elemzése
	ATE_DPT.1 A felsőszintű terv(ezés) vizsgálata
	ATE_FUN.1 Funkcionális vizsgálat
	ATE_IND.2 Független vizsgálat – mintán
A sebezhetőség felmérése	**AVA_MSU.3 A nem-biztonságos állapotok elemzése és vizsgálata /csak EAL6-tól megkövetelt**[8]**/**
	AVA_SOF.1 Az értékelés tárgya biztonsági funkciónak erősségértékelése
	AVA_VLA.4 Keményen ellenálló /csak EAL6-tól megkövetelt[9]**/**

[6] EAL4-re: ADV_IMP.1 Az értékelés tárgya biztonsági funkciói kivitelezésének alkészlete
[7] EAL4-re: ALC_DVS.1 A biztonsági intézkedések azonosítása
[8] EAL4-re: AVA_MSU.2 Az elemzés érvényesítése
[9] EAL4-re: AVA_VLA.2 A sebezhetőség független elemzése

3. A STARCOS speciális tulajdonságai

A STARCOS legfontosabb tulajdonságait a 4.2 - 4.6 alfejezetek részletezik.
Az alábbiakban csak azokat a jellemzőit emeljük ki, melyek megkülönböztetik más intelligens kártyáktól, s melyek jelen tanúsítás szempontjából lényegbe vágóak.

A STARCOS intelligens kártya fő alkotóelemei az alábbiak:
- "Philips P8WE 5032 V0G" chip /ez nem képezte részét az értékelésnek/,
- "STARCOS SPK2.3 v 7.0" operációs rendszer,
- "StarCert v 2.2" aláíró alkalmazás.

A STARCOS intelligens kártya (‚mint az értékelés tárgya) tartalmazta az alábbiakat:
- a kártyán tárolt összes (végrehajtható) szoftver,
- az aláírás alkalmazás valamennyi (nem végrehajtható) adata.

A STARCOS intelligens kártya (mint az értékelés tárgya) az alábbi funkcionalitást biztosítja:
1. az aláírás alkalmazás létrehozása (feltöltés) a kártyán, az első perszonalizálás során,
2. aláírói kulcspárok generálása a kártyán,
3. digitális aláírások létrehozása,
4. a digitális aláírások számára a biztonság garantálása,

A STARCOS intelligens kártya egyéb funkcionalitásokat is támogat(hat), de ez nem volt tárgya az értékelésnek:
1. az aláírás alkalmazás egyéb funkciói (köztük az aláírás ellenőrzése és az SSL hitelesítés és dekódolás funkciói),
2. az aláírás alkalmazáson kívül más alkalmazások funkcionalitása,
3. az intelligens kártya egyéb, nem alkalmazás specifikus funkciói.

A STARCOS intelligens kártya aláírás alkalmazásán (StarCert v2.2) kívüli egyéb alkalmazások adataira nézve:
- ezek is a kártya (más) fájljaiban és könyvtáraiban tárolódnak,
- nem hajtja végre ezeket (mint kódot) az intelligens kártya,
- nem tárgyai az értékelésnek (és tanúsításnak).

A STARCOS intelligens kártya StarCert v2.2 aláírás alkalmazása a STARCOS SPK2.3-ban implementált kriptográfiai algoritmusok közül kizárólag az RSA (aláíró) algoritmust és az SHA-1 (lenyomat készítő) algoritmust használja (a chip és az operációs rendszer által támogatott DSA aláíró algoritmust nem).

A STARCOS különböző perszonalizálási modelleket támogat. A megszemélyesítés végrehajtható központosítva egy hitelesítés-szolgáltatónál, decentralizálva egy perszonalizálás-szolgáltatónál (tipikusan egy decentralizált regisztrációs szervezetnél), vagy akár a felhasználó (aláíró) saját körletében. A kezdeti perszonalizálás során a STARCOS intelligens kártyát egy perszonalizációs PIN kód védi.

A STARCOS intelligens kártyának a következő konfigurálási opciói vannak:

- adattovábbítási protokoll (T=1 vagy T=0/T=1)

  Az első opció csak a T=1 protokollt támogatja, míg a második mindkettőt. Ez utóbbi esetben az alkalmazandó protokollban a kártya és az interfész eszköz előzetesen megegyezik egymással minden munkaszakasz (session) kezdetén, s ezt az adott munkaszakaszon belül nem változtaják meg.
- az aláírói kulcspárok maximális száma

  A kártyatulajdonos aláírói kulcspárjainak maximális száma korlátozott. Ez a szám legalább 1 és feljebb 3 lehet. A három opció (tehát amikor pontosan 1, legfeljebb 2, vagy legfeljebb 3 aláírói kulcspárral rendelkezhet a kártyatulajdonos) közüli választás semmilyen hatást nem gyakorol a kártya többi tulajdonságára. Ha 2 vagy 3 aláírói kulcspár van a kártyán, akkor azok közül ugyan választani kell, de minden kulcspárnak teljesen megegyező tulajdonságai és hozzáférési szabályai vannak, ezért a különböző kulcspárok viselkedése azonos.
- a kártyatulajdonos sikeres hitelesítését követő aláírások számának korlátozása

  Két lehetséges korlátozás van:
  - *1 (minden aláírás-létrehozás megkíván egy sikeres hitelesítést a kártyatulajdonostól),*
  - *nincs korlátozva az intelligens kártya oldaláról.*

  Ez utóbbi opciót speciális biztonsági környezetre (pl. egy hitelesítés-szolgáltató által való felhasználásra) tervezték.
- globális PIN kód

  Az aláírástól függetlenül, a StarCert v2.2 alkalmazás az SSL protokollt is támogatja a host és az intelligens kártya közötti kommunikáció hitelesítésére és titkosítására/dekódolására. Az SSL számára két különböző kulcspár van biztosítva, melyet kívülről vihetnek be az alkalmazásnak. A globális PIN kód ezt az SSL hitelesítési és dekódolási funkcionalitást védi az illetéktelen hozzáféréstől. A globális PIN funkcionalitást az inicializálás során kell aktivizálni és beállítani,ezek később már nem változtathatóak.

  A globális PIN kód a hitelesítés és a dekódolás titkos kulcsainak hozzáférését véheti, egymástól függetlenül. Tehát 4 lehetséges globális PIN kód opció van (nincs aktivizálva, csak az SSL hitelesítéshez kell megadni, csak az SSL dekódoláshoz kell megadni, mindkettőhöz szükséges megadni).

  (A globális PIN kód mechanizmusa teljesen különáll az aláírás funkcionalitásától, arra semmilyen hatást nem gyakorol.),

A STARCOS intelligens kártya hitelesítési mechanizmusa a következő tulajdonságokkal rendelkezik:

- Az intelligens kártyát egy úgynevezett transzport PIN kóddal szállítják le felhasználójának (a kártyatulajdonosnak). Ez a transzport PIN kód 5 digites.
- A kártyatulajdonosnak ezt a transzport PIN kódot le kell cserélnie az első hitelesítéskor, egy legalább 6 digitből álló PIN kódra. Az intelligens kártya ezt követően csak legalább 6 digitből álló PIN kódokat fogad el (nem lehet sikeresen rövidebbre cserélni)

A fenti tulajdonságok biztosítják, hogy még abban az esetben is, amikor a kártyatulajdonos legenerált aláírói kulcspárral (kulcspárokkal) kapja meg kártyáját, biztos lehet abban, hogy azokat még soha senki nem használta fel aláírásra (hisz ez csak sikeres hitelesítés után lett volna lehetséges, amihez előbb egy legalább 6 hosszú

PIN kódra kellett volna cserélni a transzport PIN kódot, amit már nem lehetne többé rövidebbre visszacserélni.)

A digitális aláírás létrehozásánál a STARCOS választható módon az alábbi két feltöltő (padding) módszert támogatja:
- PKCS#1 v1.5 (pszeudó véletlenekkel való teljes feltöltés),
- ISO/IEC 9796 part2 (véletlen számokkal való kiegészítő feltöltés)[10].

A digitális aláírás létrehozásánál a STARCOS választható módon az alábbi két lenyomatoló függvényt támogatja:
- SHA-1,
- RIPEMD-160[11].

A StarCert v 2.2 digitális aláírás alkalmazás képes SSL protokoll fogadásával hitelesítést és dekódolást (a kártyára küldött titkosított adatok dekódolásával) képes megvalósítani. Erre két külön kulcs van fenntartva, melyet kívülről kell a kártyára importálni. A host oldali aláíró alkalmazással kialakított megbízható csatorna kiépítéséhez Triple-DES kulcsok generálódnak (112 bites munkaszakasz kulcsok (session keys).
Ez a funkció (az úgynevezett "titkos üzenetváltás" (Secure Messaging)) nem volt megvizsgálva az értékelés során, de létezését maga a tanúsítási jelentés is megemlíti, illetve leírja.

[10] Ezek közül csak a PKCS#1 v1.5 lesz elfogadható minősített aláírásokhoz (lásd 3. feltétel).
[11] Mindkettő elfogadott minősített aláírásokhoz.

4. A STARCOS operációs rendszerre és a StarCert digitális aláírás alkalmazásra vonatkozó ITSEC tanúsítvány eredményeinek összefoglalása

A STARCOS SPK 2.3 v 7.0 intelligens kártya operációs rendszert, valamint a ráépülő StarCert v 2.2 digitális aláírás alkalmazást egy informatikai termékek (ITSEC és CC szerinti) értékelésére Németországban akkreditált laboratórium[12] megvizsgálta, értékelte és tesztelte egy termékspecifikus (a STARCOS-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 STARCOS termék) legfontosabb részleteit is.

4.2 Megvédett értékek

4.2.1 Objektumok

Az alábbi objektumok állnak védelem alatt:

- aláírás alkalmazás,
- a kártyatulajdonos aláírói magánkulcsa(i),
- a kártyatulajdonos hitelesítő adata (PIN kód),
- a kártyatulajdonos reset kódja (PUK kód),
- a kártyatulajdonos tanúsítványa(i),
- a gyökér hitelesítés-szolgáltató nyilvános kulcsa,
- az aláírás ellenőrzéséhez használható egyéb adatok,
- a kártyatulajdonos nyilvános kulcsa(i)

4.2.2 Alanyok (szubjektumok)

Az alábbi alanyokat különböztetjük meg:

- kártyatulajdonos,
- valaki más (mindenki más a kártyatulajdonoson és a potenciális támadón kívül),
- potenciális támadó.

[12] a T-Systems ISS GmbH

4.2.3 Hozzáférés típusok (az alanyok és objektumok között)

Az alábbi hozzáférési típusokat különböztetjük meg:

Az aláírás alkalmazáshoz való hozzáférés típusok:

- megnyitás,
- bezárás.

A kártyatulajdonos aláírói magánkulcsa(á/ai)hoz való hozzáférés típusok:

- generálás,
- felhasználás aláírás-létrehozásra.

A kártyatulajdonos hitelesítő adatához (PIN kód) való hozzáférés típusok:

- felhasználás a kártyatulajdonos hitelesítésére,
- módosítás,
- blokkolás,
- blokkolás feloldása.

A kártyatulajdonos reset kódjához (PUK kód) való hozzáférés típusok:

- felhasználás hitelesítésére,
- blokkolás.

A kártyatulajdonos tanúsítvány(á/ai)hoz való hozzáférés típusok:

- olvasás,
- felhasználás aláírás ellenőrzésre,
- kiegészítés.

A gyökér hitelesítés-szolgáltató nyilvános kulcsához való hozzáférés típusok:

- olvasás,
- felhasználás aláírás ellenőrzésre.

Az aláírás ellenőrzéséhez használható egyéb adatokhoz való hozzáférés típusok:

- olvasás,
- felhasználás aláírás ellenőrzésre.

A kártyatulajdonos nyilvános kulcs(á/ai)hoz való hozzáférés típusok:

- generálás,
- olvasás,
- felhasználás aláírás ellenőrzésre.

4.3 A környezetre vonatkozó feltételezések

A STARCOS intelligens kártya értékelési eredményei csak különböző feltételezések mellett érvényesek.
A feltételezések egy része az operációs rendszer és alkalmazás alapját képező hardverrel szemben támaszt elvárásokat (a STARCOS intelligens kártya értékelése - költséghatékonysági szempontokból - a chip-re vonatkozó korábbi értékelés és tanúsítás eredményeit elfogadva, azokra mint külső feltételezésekre hivatkozik, s nem ismétli meg ezek vizsgálatát, ellenőrzését.) Ezen feltételezések teljesülését a következő fejezetben (a chip-re vonatkozó értékelési és tanúsítási eredmények áttekintésével) mi is kimutatjuk.
A feltételezések egy másik részének teljesülését a gyártásra vagy a működtetésre vonatkozó szabályok betartása biztosítja. Ezek a feltételezések beépülnek jelen tanúsítási jelentés érvényességi feltételei közé is.
A STARCOS intelligens kártya értékelésénél meghatározott környezeti feltételezések egyikéről pedig kimutatjuk, hogy az intelligens kártya egy (abban az értékelésben nem vizsgált) tulajdonságának aktivizálása esetén a feltételezésre nincs szükség.

4.3.1 A teljes életciklus biztonságára vonatkozó feltételezések (AE1)

A STARCOS intelligens kártya elsősorban működtetési szakaszában hivatott biztonsági céljait elérni. Ehhez külső támogatás szükséges, a megelőző életciklus szakaszokból:

(AE1.1): Az intelligens kártya gyártási, inicializálási és perszonalizálási szakaszaiban alkalmazott folyamatok biztonságosak.

(AE1.2): Mind a hitelesítés-szolgáltató, mind a perszonalizálást végző munkahely megőrzi a kártyatulajdonost hitelesítő információk bizalmasságát.

4.3.2 A (külső) kulcsok sértetlenségére és minőségére vonatkozó feltételezések (AE2)

(AE2.1): A környezet garantálja a gyökér hitelesítés-szolgáltató eszközt hitelesítő kulcspárjára[13] az alábbiakat:
1. a kulcspár és a kriptográfiai algoritmus kriptográfiai minőségét (erősségét),
2. a magánkulcs bizalmasságát,
3. a nyilvános kulcs hitelességét (elsősorban az eredetét).

(AE2.2): A környezet garantálja a hitelesítés-szolgáltatók (a SigG által akkreditált technikai összetevők kölcsönös hitelesítésére szolgáló) eszközt hitelesítő kulcspárjára[14] az alábbiakat:
1. a kulcspár és a kriptográfiai algoritmus kriptográfiai minőségét (erősségét),
2. a magánkulcs bizalmasságát,
3. a nyilvános kulcs hitelességét (elsősorban az eredetét), amennyiben az intelligens kártyán tárolódik,
4. a nyilvános kulcs hitelességét (elsősorban az eredetét) a hitelesítő tanúsítványban.

[13] Ilyen hazai viszonyok között nincs.
[14] Ilyen hazai viszonyok között nincs.

(AE2.3): A környezet garantálja a SigG akkreditált interfész eszközt hitelesítő kulcspárjára[15] az alábbiakat:
1. a kulcspár és a kriptográfiai algoritmus kriptográfiai minőségét (erősségét),
2. a magánkulcs bizalmasságát,
3. a nyilvános kulcs hitelességét (elsősorban az eredetét).

(AE2.4): A környezet garantálja az intelligens kártya hitelesítő kulcspárjára az alábbiakat:
1. a kulcspár kriptográfiai minőségét (erősségét),
2. a nyilvános kulcs hitelességét (elsősorban az eredetét) abban az eszköz hitelesítő tanúsítványban[16], melyet a hitelesítés-szolgáltató a SigG akkreditált technikai összetevők kölcsönös hitelesítése érdekében generált, s mely az intelligens kártyán tárolódik..

(AE2.5): A környezet garantálja a gyökér hitelesítés-szolgáltató (tanúsítványt) aláíró kulcspárjára az alábbiakat:
1. a kulcspár és a kriptográfiai algoritmus kriptográfiai minőségét (erősségét),
2. a magánkulcs bizalmasságát,
3. a nyilvános kulcs hitelességét (elsősorban az eredetét).

(AE2.6): A környezet garantálja a hitelesítés-szolgáltatók (tanúsítványt) aláíró kulcspárjára az alábbiakat:
1. a kulcspár és a kriptográfiai algoritmus kriptográfiai minőségét (erősségét),
2. a magánkulcs bizalmasságát,
3. a nyilvános kulcs hitelességét (elsősorban az eredetét) a (kártyatulajdonos aláíró kulcsát tartalmazó) tanúsítványban.

(AE2.7): A környezet garantálja a kártyatulajdonos nyilvános kulcsának hitelességét (elsősorban az eredetét) a hitelesítés-szolgáltató által kibocsátott tanúsítványban.

4.3.3 A felhasználásra módjára vonatkozó feltételezések (AE3)

(AE3.1): A kártyatulajdonosnak az intelligens kártyát kellően biztonságosan kell használnia, mely az alábbiakat foglalja magában:
1. a kártyatulajdonosnak biztonságosan kell tárolnia és kezelnie kártyáját, hogy megvédje a helytelen használattól és manipulálástól,
2. a kártyatulajdonos csak olyan aláírandó adatokra aktivizálja a digitális aláírás funkciót, melynek sértetlenségét vagy hitelességét garantálni kell,
3. a kártyatulajdonos őrizze meg az aláíró alkalmazáshoz tartozó hitelesítő adatainak (PIN és PUK kódok) bizalmasságát.
4. a kártyatulajdonos rendszeresen cserélje az aláíró alkalmazáshoz tartozó PIN kódját,

[15] Ilyen hazai viszonyok között nincs.
[16] Ilyen hazai viszonyok között nincs.

5. a kártyatulajdonosnak tudnia kell, hogy az általa használt interfész eszköz SigG akkreditált-e, s ha igen, akkor nyilvános vagy hivatali/otthoni-e[17],
6. a kártyatulajdonos csak hivatali/otthoni interfész eszközzel használja az aláírás alkalmazást. Kiegészítő aláíró kulcspár generálása CA/RA körletekben is sor kerülhet. Ilyen esetekben az aláíró alkalmazás kulcsgeneráló funkcióját csak egy CA/RA-n belüli interfész eszközzel lehet használni.

(AE3.2): A fenti szabályokról a kártyatulajdonost a tanúsítványt és/vagy a kártyát kibocsátó szolgáltató tájékoztatja.

4.3.4 A felhasználás környezeti biztonságára vonatkozó feltételezések (AE4)

(AE4.1): A kártyatulajdonos a StarCert aláírás alkalmazást kizárólag SigG-nek megfelelő interfész eszközzel használja[18].

(AE4.2): A STARCOS intelligens kártya környezete garantálja az alábbiakat:

1. A hivatali/otthoni interfész eszköz egy olyan informatikai rendszerhez kapcsolódik, mely csak olyan üzenetet, vagy üzenetből képzett lenyomatolási értéket küld az intelligens kártyának, melyet az aláíró alá akar írni.
2. a korlátlan aláírás-létrehozás konfigurációja esetén az informatikai rendszer többi összetevője
   - vagy korlátozza az egy sikeres kártyatulajdonos hitelesítés után létrehozható digitális aláírások számát egy rögzített számra (s ezt elérve csak újabb sikeres hitelesítés után lehet további digitális aláírásokat létrehozni),
   - vagy korlátozza azt az időtartamot, amíg digitális aláírásokat lehet létrehozni (s ennek lejártával csak újabb sikeres hitelesítés után lehet további digitális aláírásokat létrehozni).
3. A hivatali/otthoni interfész eszköz megőrzi a kártyatulajdonos hitelesítő információinak (PIN és PUK kódok) bizalmasságát.
4. A környezet megőrzi a hivatali/otthoni interfész eszköz és az intelligens kártya között továbbított adatok bizalmasságát és sértetlenségét[19].
5. Amennyiben az intelligens kártya hitelesített állapotban van, s ezt a tényt továbbítja a hivatali/otthoni interfész eszköznek, akkor ez az eszköz ennek megfelelően reagáljon, s ezt az információt transzparens módon továbbítsa a felhasználó felé[20].
6. Amennyiben a PIN vagy PUK kódok megadásánál a maximálisan megengedett téves hitelesítési kísérlet bekövetkezik, és az intelligens kártya ezt a tényt továbbítja a hivatali/otthoni interfész eszköznek (megfelelő hibakód generálásával), akkor ez az eszköz ennek megfelelően reagáljon, s ezt az információt transzparens módon továbbítsa a felhasználó felé[21].

[17] Ez a feltétel hazai viszonyok között nem alkalmazható.
[18] Ez a feltétel hazai viszonyok között nem alkalmazható.
[19] Ez a feltétel ellentmond az SSCD védelmi profil megbízható útvonal és csatorna követelményeinek. /Ezen feltétel szerint a StarCert v2.2 alkalmazás csak olyan biztonságos környezetben használható, mely megvédi az intelligens kártya és az interfész eszköz között továbbított adatok bizalmasságát és sértetlenségét, míg az SSCD védelmi profil elvárja, hogy a BALE támogassa a bizalmasság és sértetlenség technikai eszközökkel történő megvédését./ Erre a kérdésre a későbbiekben még kitérünk.
[20] Ez a feltétel hazai viszonyok között nem alkalmazható.
[21] Ez a feltétel hazai viszonyok között nem alkalmazható.

(AE4.3): A kártyatulajdonos aláíró kulcspárjának generálásakor (akár a kártyatulajdonos, akár a CA/RA generálja ezt) a hitelesítés-szolgáltatónak ellenőriznie kell a kártyatulajdonos által használt intelligens kártya SigG akkreditáltságát[22].

4.3.5 Az intelligens kártya hardverére (chip) vonatkozó feltételezések (AE5)

(AE5.1): Az intelligens kártya hardvere ellenáll a fizikai támadásoknak, a következő értelemben:

1. megvédi az intelligens kártyát a módosításoktól
2. garantálja a kártyatulajdonos magánkulcs(á/ai)nak, valamint a kártya hitelesítő magánkulcsának a bizalmasságát a fizikai támadásokkal szemben.

(AE5.2): Az intelligens kártya hardvere biztonsági mechanizmusokat valósít meg annak érdekében, hogy megakadályozza vagy korlátozza azt az illetéktelen információ áramlást, mely a hardver tervezésből adódó jellegzetességeinek a megfigyeléséből adódna.

(AE5.3): Az intelligens kártya hardvere biztonsági mechanizmusokat valósít meg a biztonság potenciális megsértésének detektálására. A hardver a következő eseményekre reagál:

- (túl) alacsony/magas órafrekvencia,
- (túl) alacsony/magas feszültség,
- (túl) alacsony/magas hőmérséklet.

A fenti események valamelyikének detektálása esetén az intelligens kártya reset-elődik, s mindaddig ebben az állapotában marad, míg a fizikai körülmények a biztonság potenciális megsértését jelzik.

[22] Ez a feltétel hazai viszonyok között nem alkalmazható.

4.4 Kivédett fenyegetések

Az ITSEC értékelés megerősítette, hogy a STARCOS intelligens kártya (a 4.3 pontban felsorolt feltételezések mellett) kivédi az alábbi fenyegetéseket.

T1 A kártyatulajdonos aláírói magánkulcsának jogosulatlan felfedése vagy módosítása

T1.1: A kártyatulajdonos aláírói magánkulcsának jogosulatlan felfedése.

T1.2: A kártyatulajdonos aláírói magánkulcsának jogosulatlan módosítása.

T2 Visszaélés az aláírás funkcióval

T2.1: Visszaélés a digitális aláírás létrehozás funkciójával a kártyatulajdonos engedélye nélkül.

T3 A kártyatulajdonos adatainak meghamisítása

T3.1: A kártyatulajdonostól származó üzenet olyan meghamisítása, hogy az üzenet fogadója nem képes ennek észlelésére.
T3.2: Egy bizonyos üzenet kártyatulajdonostól való származásának állítása oly módon, hogy ezt a kártyatulajdonos nem képes megcáfolni.

4.5 Teljesített biztonsági célok

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

SO1 A kártyatulajdonos aláírói magánkulcsának védelme

A STARCOS védje meg a kártyatulajdonos aláírói magánkulcsának bizalmasságát és sértetlenségét az alábbi két szempontból:

(SO1.1): A STARCOS akadályozza meg az aláírói magánkulcsának bármilyen fajta felfedését az intelligens kártyán.
(SO1.2): A STARCOS akadályozza meg az aláírói magánkulcsának bármilyen fajta módosítását az intelligens kártyán.

SO2 A digitális aláírás funkció jogosulatlan használatának megakadályozása

A STARCOS kizárólag a kártyatulajdonos számára tegye elérhetővé a digitális aláírás funkcióját, az alábbi szempontok szerint:

(SO2.1): A STARCOS csak egy tudás alapú sikeres hitelesítés után tegye elérhetővé a digitális aláírás funkcióját a kártyatulajdonos számára.
(SO2.2): Egymást követő sikertelen hitelesítéseket a STARCOS-nak jogosulatlan hozzáférési kísérletként kell értelmeznie, s ilyen esetben az aláírás funkcióját elérhetetlenné kell tennie.
(SO2.3): A hitelesítési adatot a STARCOS intelligens kártyán kell tárolni, s azt onnan ne lehessen felfedni.

SO6 A kulcsgenerálás minősége

A STARCOS intelligens kártya által generált valamennyi kulcs kriptográfiai minőség szempontjából erős legyen. Az erős kriptográfiai minőséget az alábbiak jellemzik:

(SO6.1): Az aláírói kulcspárok generálását egy biztonságos folyamattal kell megvalósítani (az életciklus bármelyik szakaszában következik is ez be.)
(SO6.2): A generált aláírói kulcspárok nagyon nagy valószínűséggel egyediek és kriptográfiailag erősek legyenek.
(SO6.3): Az aláírói magánkulcsot lehetetlen legyen kiszámolni nyilvános párjából.

SO7 Biztonságos digitális aláírás szolgáltatása

Ez a fő biztonsági cél a következőket várja el:

(SO7.1): A STARCOS intelligens kártya biztosítson egy olyan digitális aláírási funkciót, mely az interfész eszköz (host oldal) által átadott adatokra az általa tárolt aláírói magánkulcs felhasználásával egy digitális aláírást készít.
(SO7.2): A digitális aláírást készítő funkció oly módon működjön, hogy a kártyatulajdonos aláírói magánkulcsának birtoklása nélkül, senki sem legyen képes digitális aláírást generálni.

SO8 A biztonság potenciális megsértésére való reagálás

A STARCOS intelligens kártyának képesnek kell lennie egy véglegesen lezárt állapotba (terminate state) kerülésre. Ebbe az állapotba kerülve, az intelligens kártyának visszafordíthatatlanul blokkolódnia kell, s a későbbiekben egyetlen alkalmazás sem futhat rajta. A STARCOS intelligens kártyának az elindítás folyamán érzékelnie kell ezt az állapotot, s ilyenkor végtelen ciklusba kell kerülnie. A véglegesen lezárt állapotba kerülést nyilvánvalóvá kell tenni az interfész eszköz, illetve a felhasználó számára is.

4.6 A biztonságot érvényre juttató funkciók (biztonsági funkciók)

Az ITSEC értékelés megerősítette az alábbi biztonsági funkciók helyes működését.

Azonosítás és hitelesítés (IA)

IA1: Az emberi felhasználó hitelesítése

Az IA1 biztonsági funkciónak az alábbi három alfunkciója van:
- hitelesíti a kártyatulajdonost (a PIN és a PIK mechanizmusokkal),
- alapértelmezésben (az intelligens kártya resetelése és deaktiválása után, az aláírás alkalmazás megnyitásakor és bezárásakor, hitelesítési hiba esetén, ismétlődő hitelesítési hiba esetén, a hitelesítés lejártával) a kártyatulajdonoson és a támadón kívüli alanyt ("valaki más") azonosít,
- észleli és azonosítja a potenciális támadót (potenciális támadás észlelésekor).

IA2: A hitelesítő adat cseréje

Ez a biztonsági funkció lehetővé teszi a kártyatulajdonosnak, hogy lecserélje PIN kódját.

IA3: A hitelesítő adat blokkolása

Ez a biztonsági funkció ismételt hitelesítési hiba esetén megakadályozza a PIN kód további próbálgatását.

IA4: A blokkolt hitelesítő adat feloldása és cseréje

Ez a biztonsági funkció a PUK kód helyes megadása esetén lehetővé teszi a kártyatulajdonos számára hogy blokkolt PIN kódját felszabadítsa, egyúttal lecserélje.

Hozzáférés ellenőrzés (AC)

AC1: A parancsokhoz való hozzáférés ellenőrzése

Ez a biztonsági funkció egy s szubjektum számára engedélyezi az o objektumhoz való acn(s,o) típusú hozzáférést, ahogy a következő táblázat mutatja:

Objektum	Szubjektum		
	"kártyatulajdonos"	"valaki más"	"potenciális támadó"
"aláírás alkalmazás"	megnyitás, bezárás	megnyitás, bezárás	-
"a kártyatulajdonos aláírói magánkulcsa(i)"	generálás, felhasználás aláírás-létrehozásra	-	-
"a kártyatulajdonos hitelesítő adata (PIN kód)"	módosítás, blokkolás, a blokkolás feloldása	felhasználás a kártyatulajdonos hitelesítésére, blokkolás	-
"a kártyatulajdonos reset kódja (PUK kód)"	-	felhasználás hitelesítésére, blokkolás	-
"a kártyatulajdonos tanúsítványa(i)"	olvasás, felhasználás aláírás ellenőrzésre, kiegészítés	olvasás, felhasználás aláírás ellenőrzésre	-
"a gyökér hitelesítés-szolgáltató nyilvános kulcsa"	olvasás, felhasználás aláírás ellenőrzésre	olvasás, felhasználás aláírás ellenőrzésre	-
"az aláírás ellenőrzéséhez használható egyéb adatok"	olvasás, felhasználás aláírás ellenőrzésre	olvasás, felhasználás aláírás ellenőrzésre	-
"a kártyatulajdonos nyilvános kulcsa(i)"	generálás olvasás, felhasználás aláírás ellenőrzésre	olvasás, felhasználás aláírás ellenőrzésre	-

Engedélyezési tábla

A fenti engedélyezés mellett ez a biztonsági funkció egy s szubjektum számára kifejezetten megakadályozza az o objektumhoz való acn(s,o) típusú hozzáférést, ahogy a következő táblázat mutatja:

Objektum	Szubjektum		
	"kártyatulajdonos"	"valaki más"	"potenciális támadó"
"aláírás alkalmazás"	-	-	megnyitás, bezárás
"a kártyatulajdonos aláírói magánkulcsa(i)"	-	generálás, felhasználás aláírás-létrehozásra	-
"a kártyatulajdonos hitelesítő adata (PIN kód)"	felhasználás a kártyatulajdonos hitelesítésére	módosítás, a blokkolás feloldása	felhasználás a kártyatulajdonos hitelesítésére módosítás, a blokkolás feloldása
"a kártyatulajdonos reset kódja (PUK kód)"	felhasználás hitelesítésére, blokkolás	-	felhasználás hitelesítésére, blokkolás
"a kártyatulajdonos tanúsítványa(i)"	-	kiegészítés	olvasás, felhasználás aláírás ellenőrzésre, kiegészítés
"a gyökér hitelesítés-szolgáltató nyilvános kulcsa"	módosítás	módosítás	olvasás, módosítás, felhasználás aláírás ellenőrzésre
"az aláírás ellenőrzéséhez használható egyéb adatok"	módosítás, kiegészítés	módosítás, kiegészítés	olvasás, módosítás, kiegészítés, felhasználás aláírás ellenőrzésre
"a kártyatulajdonos nyilvános kulcsa(i)"	-	generálás	generálás, olvasás, felhasználás aláírás ellenőrzésre

Tiltó tábla

AC2: A felfedés hozzáférés ellenőrzése

Ez a biztonsági funkció megakadályozza a kártyatulajdonos aláírói magánkulcs(á/ai)nak felfedését. A kártyatulajdonos is csak digitális aláírás létrehozása érdekében képes aktivizálni. A magánkulcsot felhasználása során (a digitális aláírás létrehozása közben) ez a funkció megvédi a felfedéstől még a DPA és az SPA típusú támadások ellen is.

AC3: Blokkolt állapot

Ez a biztonsági funkció megakadályozza a potenciális támadót, az intelligens kártya bármely funkcionalitásának használatától.
A "valaki más" szubjektum képes a TERMINATE CARD USAGE parancs kiadásával a STARCOS intelligens kártyát egy véglegesen lezárt állapotba (terminate state) juttatnia. Ezzel az intelligens kártya visszafordíthatatlanul blokkolódik, egyetlen alkalmazás sem futtatható rajta a későbbiekben. A STARCOS intelligens kártya az elindítás folyamán érzékeli ezt az állapotot, s ilyenkor végtelen ciklusba kerülve megakadályoz bármilyen más parancs végrehajtását.

Naplózás (AU)

AU1: Információ a blokkolt állapotról

Ez a biztonsági funkció a felhasználót tájékoztatja arról, hogy az intelligens kártya véglegesen blokkolt állapotba került, s a továbbiakban nem használható.

AU2: Információ a kártyatulajdonos hitelesítésének blokkoltságáról

Ez a biztonsági funkció az interfész eszközt (tipikusan a kártyaolvasót) tájékoztatja arról, hogy a kártyatulajdonos hitelesítése (PIN kódjával vagy PUK kódjával) blokkolódott. (Ezt a helyzetet az interfész eszköznek, illetve a host oldali alkalmazásnak a felhasználó számára is meg kell jelenítenie.)

Objektum újrahasználat (OR)

OR1: Érzékeny adatok törlése az átmeneti tárolókban

Ez a biztonsági funkció biztosítja, hogy az átmenetileg használt memóriatartományokból kitörlődik a kártyatulajdonos magánkulcsa, PIN kódja és PUK kódja, még az aláírás alkalmazás lezárása előtt (s így egy más alkalmazás semmiképp nem férhet hozzá).

Adat csere (DX)

DX1: Kulcs generálása és exportálása

A DX1.1 kulcs generálási alfunkció az aszimmetrikus kulcspárok generálását végzi. A kártyatulajdonos több aláírói kulcspárral is rendelkezhet. Minden újonnan generált kulcspárra nézve a kártya mindaddig a perszonalizálási szakaszban marad, míg a nyilvános kulcs összetevőre a hitelesítés-szolgáltató tanúsítványt nem készít, s az fel nem kerül a kártyára. Ezután kerül csak az adott kulcspár működtetésre (aláírásra) alkalmas állapotba. Egy új kulcspár generálása viszont nem befolyásolja egy a kártyán már létező másik aláírói kulcspár életciklusát. Egy már létező kulcspár lecserélésre nincs mód (csak újat lehet generálni). A STARCOS intelligens kártyán összesen generálható kulcspárok számát (m) a kártyagyártó állítja be a kártya inicializálásakor. A különböző kulcspárokat egy paraméterrel (i) lehet megkülönböztetni (i = 1,…m)
A DX1.2 nyilvános kulcs olvasási alfunkció lehetővé teszi a kártyán generált nyilvános kulcsok hitelesítésére (aláírására) használt kulcspár nyilvános összetevőjének (PK.ICC.AUT) kiolvasását, valamint az (ennek magánkulcs párjával, azaz a SK.ICC.AUT kulccsal) aláírt, s így hitelesített aláírói nyilvános kulcsok (PK_i.CH.DS[23]) kiolvasását is.

DX2: Digitális aláírás létrehozása

Ez a biztonsági funkció egy digitális aláírás funkcionalitást biztosít. Segítségével a kártyatulajdonos az intelligens kártyára továbbított aláírandó adatot (valamelyik SK_i.CH.DS) magánkulcsával aláírja, majd az aláírást visszaküldi az interfész eszköznek. Amennyiben a kártyán több aláírói magánkulcs van, az aláírónak választania kell közülük.
A STARCOS konfigurációjától függően (lásd a 3. fejezet harmadik konfigurációs opcióit) egy sikeres hitelesítést követően az intelligens kártya vagy csak egy digitális aláírás létrehozását teszi lehetővé, vagy többet is.
A STARCOS intelligens kártya az aláírandó dokumentum lenyomatolásának mindhárom alábbi változatát támogatja:

- a host oldali alkalmazás képzi a teljes lenyomatot (hash-értéket), s ezt küldi a kártyára aláírásra,
- a host oldali alkalmazás az aláírandó dokumentum egy részéről képez csak egy közbülső lenyomatot, s ezt a maradék dokumentummal együtt küldi át a kártyára végleges lenyomatolásra és aláírásra,
- a host oldali alkalmazás a teljes aláírandó dokumentumot küldi át a kártyára teljes lenyomatolásra és aláírásra.

(A digitális aláírás funkció úgy működik, hogy az intelligens kártyán tárolt és a digitális aláíráshoz felhasznált magánkulcs(ok)ra nem lehet következtetni a digitális aláírás képzéséből. Egyúttal a felhasznált magánkulcs nem következtethető ki az aláírásból, s a titkos magánkulcsot nem birtoklók nem is generálhatnak vele készült aláírást.)

[23] A kulcsokra STARCOS jelölésrendszerében alkalmazott betűpár hármasban:
az első helyen szereplő betűpár a kulcs összetevőjét jelzi (PK: nyilvános, SK: magán kulcsösszetevő),
a második betűpár a tulajdonost jelöli (ICC: a kártya saját kulcsa, CH: a kártyatulajdonos kulcsa),
a harmadik betűpár pedig a kulcs felhasználhatóságát jelöli (DS: aláírásra használható kulcs, AUT: más kulcsok hitelesítésére használható kulcs). (Az első betűpár indexelhető is.)

5. A mikrochip-re vonatkozó ITSEC tanúsítvány eredményeinek összefoglalása

5.1 Az ITSEC értékelés eredményei

A P8WE5032v0G mikrochip értékelését végző laboratórium[24], illetve a tanúsítást kiállító BSI[25] 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 alkotó elemei

Bár a mikrochip értékelési eredményeit a STARTCOS SPK 2.3 v 7.0 operációs rendszer és StarCert v 2.2 digitális aláírás alkalmazás együttes értékelésénél és tanúsításánál figyelembe vették és beépítették, a BALE követelményeknek való teljes megfelelés kimutatásánál a későbbiekben szükség lesz néhány hardver-specifikus értékelési eredményre (ellenőrzött biztonsági funkcióra).
Ezért röviden áttekintjük a mikrochip összetevőit és fő biztonsági funkcióit.

A vizsgált intelligens kártya alapját a Philips P8WE5032v0G mikrochip-je biztosítja.

5.2.1 A P8WE5032v0G mikrochip hardver alkotó elemei

- b-bites (80C51 típusú) központi feldolgozó egység (CPU)
- memóriák:
  - RAM (256 + 2048 bájt)
  - ROM (32 Kbájt felhasználói + tesztelésre)
  - EEPROM (32 Kbájt, benne 32 byte biztonsági területtel)
- Triple-DES társprocesszor /Triple-DES algoritmus gyors számítására/
- FameX társprocesszor /aritmetikai számítások gyors végrehajtására/
- megszakító modul
- fizikai véletlenszám generátor
- belső óra,
- áramköri modul biztonsági érzékelőkkel és biztonsági logikával
- I/O interfész
- UART

[24] debis Systemhaus Information Security Services GmbH.
[25] A német informatika biztonsági értékelési/tanúsítási sémában központi szerepet betöltő tanúsító szervezet.

5.2.2 A P8WE5032v0G mikrochip förmver alkotó elemei

Az alábbi förmver elemek (az IC dedikált teszt szoftvere) a teszt ROM-ban helyezkednek el, csak a teszt üzemmódban elérhető módon:

- teszt operációs rendszer
- teszt rutinok az áramkör különböző blokkjaihoz
- kontroll flag-ek az EEPROM biztonsági területének állapotaihoz
- a biztonságkritikus tesz műveletek illegális végrehajtását megakadályozó logika

5.2.3 A P8WE5032v0G mikrochip szoftver alkotó eleme

Az alábbi szoftver elemek a felhasználói ROM-ban helyezkednek el:

- operációs rendszer (nem volt része a mikrochip alap értékelésének és tanúsításának)
- alkalmazás (nem volt része a mikrochip alap értékelésének és tanúsításának)

A P8WE5032v0G mikrochip alábbi biztonsági tulajdonságait érintette az előzetes értékelés, majd az ezt követő (német séma alapján végzett) tanúsítás. Ennek eredményeit a STARTCOS SPK 2.3 v 7.0 operációs rendszer és StarCert v 2.2 digitális aláírás alkalmazás együttes értékelése és tanúsítása - mint kiindulási alapot – figyelembe vette.

5.3 A mikrochip legfontosabb tulajdonságai (biztonsági funkciók)

A microchip az alábbiakban részletezett biztonsági funkciók segítségével valósítja meg biztonsági céljait.

Véletlenszám generátor (F1):

A mikrochip-ben egy valódi, fizikai véletlen jelenségen alapuló véletlenszám generátor van, mely a „működési állapot ellenőrzés” biztonsági funkció által garantált határok között stabilan működik. A véletlenszám generátor folyamatosan 1 bájtos véletlenszámokat generál. Minden bájt legalább 7 bitnyi entrópiával rendelkezik. A beágyazott szoftvernek (alkalmazás) legalább 4800 belső órajelet kell várnia két egymást követő véletlen bájt kiolvasása közben.

Triple-DES társprocesszor (F2)

A mikrochip ezen biztonsági funkciója a beágyazott szoftver számára biztosítja a Triple-DES titkosítás és dekódolás funkcionalitást.
A mikrochip hardver társprocesszora szabványos Triple-DES titkosítást hajt végre, 112 bites kulcsméret mellett. A titkosítási algoritmus megvalósítása garantálja, hogy a Triple-DES műveletek során a külsőleg is megfigyelhető jelekből (viselkedésből) nem lehet következtetni sem a nyílt, sem a kulcs adatokra. Ez egyaránt vonatkozik az áramfelvétel különbségére irányuló (DPA), valamint a műveletek időigényén alapuló (TA) támadásokra.

RSA megvalósítás beépített aritmetikai alapfunkciókkal (F3)

A mikrochip támogatást nyújt nagy egész számok moduláris műveleteihez. Az aritmetikai funkciók az aszimmetrikus kriptográfiai algoritmusok (pl. az RSA) gyorsítására használhatók. Az intelligens kártya beágyazott szoftverének kell kiválasztania a társprocesszor megfelelő funkcióját, majd kell megadnia az aritmetikai függvények változóit. Ez a biztonsági funkció a szabványos RSA kriptográfiai algoritmus megvalósítását támogatja, 1024-es kulcsméret mellett.

Működési állapot ellenőrzés (F4)

Ez a biztonsági funkció az alábbi alfunkciókat tartalmazza:
- a feszültség és az óra frekvencia szűrése,
- a feszültség, az óra frekvencia és a hőmérséklet folyamatos figyelemmel kísérése (monitorozása) érzékelőkkel, valamint az EEPROM-ba írási folyamat áramerősségének és a program végrehajtásának az ellenőrzése.

Amennyiben a működési paraméterek ellenőrzése konfigurálva van (azaz az érzékelők bekapcsolt állapotban vannak), s valamelyik paraméter elhagyja a megengedett tartományt, az aktuális program futása törlődik egy CPU reset hatására.
A felhasználóhoz való szállítás előtt a mód-kapcsolót teszt üzemmódról felhasználói üzemmódra állítják. A felhasználói üzemmódban a mikrochip működése közben automatikusan eléri az érzékelőket, melyek ilyenkor mindig bekapcsolt állapotban vannak, s még az alkalmazásból sem lehet kikapcsolni őket.

A fizikai manipuláció elleni védelem (F5)

A mikrochip megvédi a manipulálástól alábbi komponenseit:
- hardver,
- a ROM-ban tárolt teszt szoftvere,
- az intelligens kártya ROM-ban és EEPROM-ban tárolt alkalmazói szoftvere,
- EEPROM-ban és RAM-ban tárolt alkalmazói adatok,
- az EEPROM biztonsági szegmensében tárolt konfigurációs adatok,
- üzemmód-kapcsoló.

A védelem a mikrochip konstrukcióján alapul, mely megnehezíti a manipulálást.

Az üzemmód és a konfiguráció védelme (F6)

Ez a biztonsági funkció a mikrochip két üzemmódja (teszt üzemmód és felhasználói üzemmód) segítségével hozzáférés ellenőrzést biztosít. Az alábbi 3 alfunkciót tartalmazza:
- azonosítás
  Teszt üzemmódban a mikrochip azonosítja az adminisztrátort, felhasználói üzemmódban pedig a felhasználót (kártyatulajdonost).
- hozzáférés védelem
  Teszt üzemmódban a teszt szoftver futtatható, de a beágyazott szoftver nem, felhasználói üzemmódban a beágyazott szoftver futtatható, de a teszt szoftver nem.
- üzemmód kapcsoló
  A mikrochip kezdeti állapota a teszt üzemmód. Ez átállítható felhasználói üzemmódba, de ezután a teszt üzemmód már nem érhető el többé.

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

6.1 A STARCOS intelligens kártya 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.]***
STARCOS tulajdonság	A STARCOS képes: • az **RSA** digitális aláírás algoritmushoz kulcsokat generálni, • **Triple-DES** kulcsokat generálni a kártyatulajdonos hitelesítési adatainak védelmét biztosító megbízható útvonal kiépítéséhez (session key). A STARCOS képes 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 STARCOS képes 112 bites **Triple-DES** kulcsok (session key) előállítására az alábbi módszerrel: • a microchip hardver véletlenszám generátora által előállított véletlen számokat egy kiegészítő, szoftver-alapú eljárás stabilizálja.
Ellenőrzött követelmények (STARCOS ITSEC tanúsítás)	• teljesülő SO6 biztonsági cél (A kulcsgenerálás minősége) • helyesen működő DX1 biztonsági funkció (Kulcs generálása és exportálása)

Kriptográfiai kulcs generálás (FCS_CKM.1) /folytatás/	
Értékelés	Az RSA (legalább 1020 bitméret mellett) minősített aláíráshoz elfogadott algoritmus. A STARCOS képes a megfelelő méretű (1024 bites) RSA kulcsok szabványos generálására. Következésképp a STARCOS 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 STARCOS képes 112 bites triple-DES kulcsok biztonságos generálására. Következésképpen a STARCOS képes a megbízható csatorna és útvonal kiépítéséhez szükséges titkosító és kriptográfiai ellenőrzőösszeg számító algoritmus kulcsainak generálására.
Következtetés	A STARCOS **megfelel** az SSCD-PP „Kriptográfiai kulcs generálás” követelményének.
Feltételek:	---

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.]***
STARCOS tulajdonság	A STARCOS: • automatikusan törli (aktív felülírással) a titkos kulcsok és egyéb titkok számítására használt felejtő memóriákat (bennük a munkaszakasz kulcsokat és az aláíró magánkulcsot) még az aláírás alkalmazás lezárása előtt.
Ellenőrzött követelmények (STARCOS ITSEC tanúsítás)	• teljesülő SO1 biztonsági cél (A kártyatulajdonos aláírói magánkulcsának védelme), • helyesen működő OR1 biztonsági funkció (Érzékeny adatok törlése az átmeneti tárolókban).
Értékelés	A munkaszakasz kulcsok, illetve a digitális aláírásra átmenetileg felejtő memóriába másolt magánkulcs másolatok automatikusan törlődnek, még az aláíró alkalmazás lezárása előtt. Az ITSEC értékelés azt is igazolta, hogy a törlés a tárolt kulcsértékek fizikailag visszafordíthatatlan megsemmisítésével (aktív felülírásával) jár. Következésképpen a BALE képes tárolt kulcsértékeinek fizikailag visszafordíthatatlan, szabványos megsemmisítésére.
Következtetés	A STARCOS **megfelel** az SSCD-PP „Kriptográfiai kulcs megsemmisítés” követelményének.
Feltétel:	---

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].***
STARCOS tulajdonság	A STARCOS: • 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 8/1. és a 8/8. feltételt), • támogatja az **RSA** digitális aláírás algoritmust (*1024 bit közötti kulcsmérettel, és szabványos PKCS#1-es formátumban*),
Ellenőrzött követelmények (STARCOS ITSEC tanúsítás)	• teljesülő SO6 biztonsági cél (A kulcsgenerálás minősége), • teljesülő SO7 biztonsági cél (Biztonságos digitális aláírás szolgáltatása), • helyesen működő DX1 biztonsági funkció (Kulcs generálása és exportálása), • helyesen működő DX2 biztonsági funkció (Digitális aláírás létrehozása).
Értékelés	A STARCOS képes egy minősített aláíráshoz elfogadott szabványos kriptográfiai algoritmus végrehajtásával (RSA, 1024 bites kulcsmérettel, PKCS#1 aláírási formátummal, PKCS#1 v1.5 feltöltő móddal, SHA-1 vagy RIPEMD-160 lenyomatoló függvénnyel) az alábbi feladatokat ellátni: • a magánkulcs/nyilvános kulcs megfelelésének bizonyítása, • az aláírandó adatok digitális aláírása.
Következtetés	A STARCOS (a feltételek betartása esetén) **megfelel** az SSCD-PP „Kriptográfiai eljárás” követelményének.
Feltételek:	3. és 8.

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.
STARCOS tulajdonság	A STARCOS támogatja a felhasználói és adminisztrátori szerepkör szétválasztását. Egy BALE-ként használt STARCOS esetén az „aláíró” a „felhasználó”, míg az intelligens kártya megszemélyesítési folyamatában különleges jogosultságokkal rendelkező személy az „adminisztrátor”. Ilyen szerepkör megfeleltetés, valamint a 8. 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 (STARCOS ITSEC tanúsítás)	• teljesülő SO1 biztonsági cél (A kártyatulajdonos aláírói magánkulcsának védelme), • teljesülő SO2 biztonsági cél (A digitális aláírás funkció jogosulatlan használatának megakadályozása), • helyesen működő IA1 biztonsági funkció (Az emberi felhasználó hitelesítése), • helyesen működő IA2 biztonsági funkció (A hitelesítő adat cseréje), • helyesen működő AC1 biztonsági funkció (A parancsokhoz való hozzáférés ellenőrzése).

Részleges hozzáférés ellenőrzés (FDP_ACC.1) /folytatás/	
Értékelés	Az SSCD-PP „Részleges hozzáférés ellenőrzés” követelményét a STARCOS támogatja, az ITSEC értékelés pedig igazolja (a 8. feltétel betartása esetén): • csak az adminisztrátor tisztviselő hozhatja létre a felhasználó (aláíró) kezdeti (5 digit hosszú transzport) PIN kódját, • csak az adminisztrátor vagy a felhasználó (aláíró) generálhatja a kártyatulajdonos aláírói magánkulcsát, • csak az adminisztrátor vagy a felhasználó (aláíró) exportálhatja a fenti módon generált magánkulcs nyilvános kulcs párját, • csak a felhasználó (aláíró) cserélheti le az (5 digit hosszú) transzport PIN kódot az általa használandó (legalább 6digit hosszú) PIN kódjával, • csak a felhasználó (aláíró) írhat alá saját magánkulcsával (miután a legalább 6 digit hosszú PIN kódjával hitelesítette magát).
Következtetés	A STARCOS (a feltételek betartása esetén) **megfelel** az SSCD-PP „Részleges hozzáférés ellenőrzés” követelményének.
Feltétel:	8.

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/	
STARCOS tulajdonság	A STARCOS támogatja a felhasználói és adminisztrátori szerepkör szétválasztását. Egy BALE-ként használt STARCOS esetén az „aláíró” a „felhasználó”, míg az intelligens kártya megszemélyesítési folyamatában különleges jogosultságokkal rendelkező személy az „adminisztrátor”. Ilyen szerepkör megfeleltetés, valamint a 8. feltétel betartása esetén: 1'. Aláírói kulcspár(oka)t a kezdeti perszonalizálás szakaszában csak a perszonalizációs PIN kódot ismerő "adminisztrátor" vagy "felhasználó" generálhat (attól függően, hogy ez a perszonalizálás egy központosított hitelesítés-szolgáltatónál, decentralizált regisztrációs szervezetnél, vagy a felhasználó saját körletében történik meg). Az SSCD védelmi profil által elvárt "magán-nyilvános kulcspár kezelés” biztonsági jellemző "felhatalmazott” értékre állítás a STARCOS esetében a perszonalizációs PIN kód helyes megadásával helyettesíthető (ennek helytelen megadása esetén az egész perszonalizálás, tehát a kulcsgenerálás is kifejezetten tiltva van). 2'. A legenerált aláírói kulcspárok nyilvános kulcs részét exportálását csak az adminisztrátor (amennyiben ő végzi a kulcsgenerálást) vagy a felhasználó végezheti, sikeres hitelesítés után. 3'. A felhasználó kezdeti hitelesítő kódját (transzport PIN kód) csak az adminisztrátor hozhatja létre a perszonalizálás szakaszában. 4'. Az SSCD védelmi profil 4. pontban megfogalmazott fenti elvárásai úgy összegezhetők, hogy csak az „aláíró” írhasson alá (még a kulcsgenerálást helyette elvégző adminisztrátor se!), és az aláíró is csak akkor, ha ez külön engedélyezve van számára (a „magánkulcs aktivizálás” biztonsági jellemző „igen” értékre állításával), s az aláírandó adatok egy hiteles aláíró alkalmazástól jönnek. A STARCOS intelligens kártya a konkrétan megnevezett biztonsági tulajdonságokat nem kezeli, de az elvárások érdemi részét teljesíti az alábbi módon: • csak az aláíró írhat alá, miután az 5 digites transzport PIN kódot lecseréli saját, legalább 6 digites PIN kódjára (s a transzport kulcs 5 hosszúsága egyértelműen garantálja számára, hogy senki /még az adminisztrátor sem/ nem írt még alá kulcsával, • az aláírandó adatok hiteles aláíró alkalmazástól való származását a host oldal és a STARCOS között kiépülő megbízható csatorna (lásd FTP_ITC.1 követelmény) elvárása biztosítja, • aláírni pedig az aláíró sem tud, még mielőtt az 5 digites transzport PIN kódot le nem cseréli egy legalább 6 digites PIN kódra.
Ellenőrzött követelmények (STARCOS ITSEC tanúsítás)	• teljesülő SO1 biztonsági cél (A kártyatulajdonos magánkulcsának védelme), • teljesülő SO2 biztonsági cél (A digitális aláírás funkció jogosulatlan használatának megakadályozása), • helyesen működő IA.1 biztonsági funkció (Az emberi felhasználó hitelesítése), • helyesen működő IA.2 biztonsági funkció (A hitelesítő adat cseréje), • helyesen működő AC.1 biztonsági funkció (A parancsokhoz való hozzáférés ellenőrzés).

Biztonsági jellemzőkön alapuló hozzáférés ellenőrzés (FDP_ACF.1) /folytatás/	
Értékelés	Az SSCD-PP „Biztonsági jellemzőkön alapuló hozzáférés ellenőrzés” követelményét a STARCOS támogatja, az ITSEC értékelés pedig igazolja (a 8. feltétel betartása esetén): • amennyiben nem az adminisztrátor generálja a kulcspárokat, az „aláíró” csak akkor generálhatja le saját magánkulcsát, ha ezt az „adminisztrátor” (a transzport PIN átadásával) engedélyezi számára, • amennyiben nem az adminisztrátor generálja a kulcspárokat csak az „aláíró” exportálhatja saját nyilvános kulcsát (a transzport PIN kód hosszabbra cserélésével), • az „aláíró” kezdeti (transzport) PIN kódját csak az „adminisztrátor” hozhatja létre, • csak az „aláíró” írhat alá magánkulcsával, és is csak azután, hogy ennek lehetőségét aktivizálta (a transzport PIN kód hosszabbra cserélésével).
Következtetés	A STARCOS (a feltételek betartása esetén) **megfelel** az SSCD-PP „Biztonsági jellemzőkön alapuló hozzáférés ellenőrzés” követelményének.
Feltétel:	8.

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).
STARCOS tulajdonság	A STARCOS garantálja, hogy az átmenetileg használt memóriatartományokból kitörlődik a kártyatulajdonos magánkulcsa, PIN kódja és PUK kódja, még az aláírás alkalmazás lezárása előtt, s így egy más alkalmazás semmiképp nem férhet hozzá.
Ellenőrzött követelmények (STARCOS ITSEC tanúsítás)	• teljesülő SO1 biztonsági cél (A kártyatulajdonos aláírói magánkulcsának védelme), • helyesen működő OR1 biztonsági funkció (Érzékeny adatok törlése az átmeneti tárolókban).
Értékelés	Mivel a magánkulcsokat, hitelesítő adatokat és hitelesítést ellenőrző adatokat átmenetileg tároló felejtő memóriákat még az aláírás alkalmazás lezárása előtt aktívan felülírják, ezért ezen erőforrások deallokálás (alkalmazás lezárás) utáni törlése biztosított.
Következtetés	A STARCOS **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).
STARCOS tulajdonság	A STARCOS az intelligens kártyán tárolt valamennyi felhasználói adat sértetlenségét folyamatosan figyeli. Adat integritás hiba észlelése esetén a kártya értesíti a felhasználót a hibáról. egyúttal megakadályozza a módosult adatok használatát.
Ellenőrzött követelmények (STARCOS ITSEC tanúsítás)	• teljesülő SO8 biztonsági cél (A biztonság potenciális megsértésére való reagálás), • helyesen működő AC3 biztonsági funkció (Blokkolt állapot).
Értékelés	Az SSCD-PP fenti követelményében kivétel nélkül felhasználói adatok szerepelnek. A felhasználói adatokra pedig az ITSEC értékelés által ellenőrzött STARCOS biztonsági funkció (AC3) biztosan észleli az integritás hibákat. Integritás hiba észlelése esetén a STARCOS megakadályozza a módosult adatok használatát, egyúttal értesíti (hibaüzenet formájában) az aláírót az integritás hibáról. Következésképpen a STARCOS valamennyi, a BALE-ktől elvárt tulajdonsággal rendelkezik ebben a követelménycsoportban is.
Következtetés	A STARCOS **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.
STARCOS tulajdonság	A STARCOS **képes SSL hitelesítési és dekódolási funkcionalitását aktivizálni,** s ezzel egy megbízható csatornát kiépíteni az aláírás-létrehozó alkalmazással. Ezen a csatornán az alkalmazás és az intelligens kártya között kicserélt adatok bizalmassága, hitelessége és **sértetlensége** egyaránt megvédhető. Mind a nyilvános kulcs exportálásához, mind az aláírandó adat reprezentáns importálásához használható (és az 5. feltétel szerint használandó is) ez a megbízható csatorna. Az adattovábbítás során bekövetkező módosítás vagy beszúrás elrontja a továbbított adat sértetlenségét, így az SSL hitelesítési és dekódolási funkció képes észlelésére és jelzésére. Az aláírás-létrehozó funkció azt is képes jelezni, ha egyáltalán nem kapja meg a számára továbbítandó aláírandó adat reprezentánst (következésképpen erre az adatra a törlés is kimutatható.
Ellenőrzött követelmények (STARCOS ITSEC tanúsítás)	A STARCOS SPK 2.3 v 7.0 ITSEC értékelése nem vizsgálta a termék fenti /SSL alapján megvalósított megbízható csatorna/ funkcionalitás helyes megvalósítását, bár megemlítette létezését. Egy másik termék /a STARCOS SPK 2.4 operációs rendszer tachográf kártya alkalmazással/ ITSEC értékelése (melynek garanciaszintje szintén megfelelően magas -E3- volt) ugyanakkor már vizsgálta és tanúsította ezt a funkcionalitást is. A fejlesztőktől származó nyilatkozat szerint a két termék "ugyanazt a megbízható csatornát használja a "biztonságos adatcsere" funkción keresztül".
Értékelés	Az 5. feltétel teljesítése esetén (melyet a STARCOS támogat) kiépülő megbízható csatorna biztosítja végpontjainak garantált azonosítását és a továbbított adatok (nyilvános kulcs és aláírandó adat reprezentáns) illetéktelen módosítás elleni védelmét.
Következtetés	A STARCOS (a feltételek betartása esetén) **megfelel** az SSCD-PP „Az adat-csere sértetlensége” követelményének.
Feltétel:	5.

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.
STARCOS tulajdonság	A STARCOS 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 (**3**) sikertelen hitelesítési kísérlet következett be, bármely jelszó alapú hitelesítési eljárásban, • sikeres hitelesítés esetén egy számláló értékét **3**-ra 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 /PUK kód megadása/ állíthatja vissza a számláló **3**-as kiindulási értékét a blokkolás feloldására), • a blokkolás feloldását is csak háromszor lehet elrontani, a PUK kód **3**. helytelen megadása az aláírás alkalmazás végleges, visszafordíthatatlan blokkolását okozza.
Ellenőrzött követelmények (STARCOS ITSEC tanúsítás)	• teljesülő SO2 biztonsági cél (A digitális aláírás funkció jogosulatlan használatának megakadályozása), • teljesülő SO8 biztonsági cél (A biztonság potenciális megsértésére való reagálás), • helyesen működő IA1 biztonsági funkció (Az emberi felhasználó hitelesítése), • helyesen működő IA2 biztonsági funkció (A hitelesítő adat cseréje), • helyesen működő IA3 biztonsági funkció (A hitelesítő adat blokkolása), • helyesen működő IA4 biztonsági funkció (A blokkolt hitelesítő adat feloldása és cseréje), • helyesen működő AC3 biztonsági funkció (Blokkolt állapot).
Értékelés	A STARCOS támogatja az SSCD védelmi profil fenti elvárását.
Következtetés	A STARCOS (a feltételek betartása esetén) **megfelel** az SSCD-PP „A hitelesítési hiba kezelése” követelményének.
Feltétel:	---

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.
STARCOS tulajdonság	A STARCOS képes kezelni a PIN kódot, mindkét szerepkörhöz tartozóan (így a felhasználóra, vagyis az aláíróra is).
Ellenőrzött követelmények (STARCOS ITSEC tanúsítás)	• teljesülő SO2 biztonsági cél (A digitális aláírás funkció jogosulatlan használatának megakadályozása), • helyesen működő IA1 biztonsági funkció (Az emberi felhasználó hitelesítése).
Értékelés	A követelmény teljesül.
Következtetés	A STARCOS **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[26].
STARCOS tulajdonság	A STARCOS intelligens kártya a StarCert v2.2 digitális aláírás alkalmazás valamennyi aláírással kapcsolatos funkcióját (kulcsgenerálás, nyilvános kulcs exportálás, digitális aláírás-létrehozás, stb.) csak azt követően engedélyezi, hogy az aláíró (PIN kódja megadásával) sikeresen azonosította (és egyben hitelesítette) magát.
Ellenőrzött követelmények (STARCOS ITSEC tanúsítás)	• teljesülő SO2 biztonsági cél (A digitális aláírás funkció jogosulatlan használatának megakadályozása), • helyesen működő IA1 biztonsági funkció (Az emberi felhasználó hitelesítése), • helyesen működő AC1 biztonsági funkció (A parancsokhoz való hozzáférés ellenőrzése).
Értékelés	A STARCOS támogatja a követelmény kielégítését.
Következtetés	A STARCOS **megfelel** az SSCD-PP „Az azonosítás időzítése” követelményének.
Feltétel:	---

[26] 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[27].
STARCOS tulajdonság	A STARCOS intelligens kártya a StarCert v2.2 digitális aláírás alkalmazás valamennyi aláírással kapcsolatos funkcióját (kulcsgenerálás, nyilvános kulcs exportálás, digitális aláírás-létrehozás, stb.) csak azt követően engedélyezi, hogy az aláíró (PIN kódja megadásával) sikeresen (azonosította és egyben) hitelesítette magát.
Ellenőrzött követelmények (STARCOS ITSEC tanúsítás)	• teljesülő SO2 biztonsági cél (A digitális aláírás funkció jogosulatlan használatának megakadályozása), • helyesen működő IA1 biztonsági funkció (Az emberi felhasználó hitelesítése), • helyesen működő AC1 biztonsági funkció (A parancsokhoz való hozzáférés ellenőrzése).
Értékelés	A STARCOS támogatja a követelmény kielégítését.
Következtetés	A STARCOS **megfelel** az SSCD-PP „Az azonosítás időzítése” követelményének.
Feltétel:	---

[27] 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.
STARCOS tulajdonság	A kártyatulajdonos birtokában lévő kártyára /mint azt a FIA_UID.1 (Az azonosítás időzítése) követelmény tárgyalásánál kimutattuk/, a STARCOS támogatja az aláírással kapcsolatos parancsok felhasználói hitelesítéshez kötését. Amennyiben az aláíráshoz szükséges kulcsokat még az intelligens kártya tulajdonosához juttatása előtt generálja az adminisztrátor, akkor az aláírás-létrehozás funkció aktivizálását a következők akadályozzák meg: • egy aláíró kulccsal aláírni csak az 5 digites transzport PIN kód legalább 6 digitesre való lecserélése után lehet, • az aláíró első aláírása előtt ellenőrzi (a 8/5. vagy 8/7. feltétel betartása esetén), hogy a neki átadott transzport PIN kód hossza valóban 5 digit-e.
Ellenőrzött követelmények (STARCOS ITSEC tanúsítás)	• teljesülő SO2 biztonsági cél (A digitális aláírás funkció jogosulatlan használatának megakadályozása), • helyesen működő IA1 biztonsági funkció (Az emberi felhasználó hitelesítése), • helyesen működő IA2 biztonsági funkció (A hitelesítő adat cseréje), • helyesen működő AC1 biztonsági funkció (A parancsokhoz való hozzáférés ellenőrzése).
Értékelés	A STARCOS támogatja a követelmény kielégítését: • amennyiben az aláíráshoz szükséges kulcsokat az aláíró már készen kapja, leellenőrizheti (a transzport PIN kód hosszán) hogy korábban még nem írtak az adott kulccsal alá (s csak ekkor veszi át), • minden más esetben csak a kártya tulajdonos sikeres hitelesítése után aktivizálható a digitális aláírás funkció.
Következtetés	A STARCOS (a feltételek betartása esetén) **megfelel** az SSCD-PP „A biztonsági funkciók viselkedésének kezelése” követelményének.
Feltétel:	8.

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.
STARCOS tulajdonság	A STARCOS nem kezel sem „magán-nyilvános kulcspár kezelés” sem "magánkulcs működtetése" biztonsági jellemzőt. Ugyanakkor a fenti elvárás mindkét érdemi része teljesül, hiszen: • az adminisztrátor a transzport PIN kód legenerálásával és átadásával adja meg a jogot a kártyabirtokosnak a kulcspár generálására (amennyiben még nem generálta le helyette), • a 8/5. vagy 8/7. feltétel betartása esetén pedig az aláíró (kártyatulajdonos) az 5 digites transzport PIN kód legalább 6 digites PIN kódra való lecserélésével teremti meg az aláíró funkció aktivizálásának lehetőségét (s ezt helyette senki más nem teheti meg észrevétlenül).
Ellenőrzött követelmények (STARCOS ITSEC tanúsítás)	• teljesülő SO2 biztonsági cél (A digitális aláírás funkció jogosulatlan használatának megakadályozása), • helyesen működő IA1 biztonsági funkció (Az emberi felhasználó hitelesítése), • helyesen működő AC1 biztonsági funkció (A parancsokhoz való hozzáférés ellenőrzése).
Értékelés	A STARCOS közvetlenül nem támogatja a BALE-ra elvárt, a biztonsági jellemzők módosítási lehetőségére vonatkozó fenti követelményt. Ugyanakkor a STARCOS által biztosított adminisztrátori és felhasználói szerepkör elválasztásával, a transzport és felhasználói PIN kód hosszak különbözőségének kikényszerítésével és az aláírás funkció aktivizálás jogosultság ellenőrzésével (a 8. feltétel betartása esetén) az elvárás lényege teljesül.
Következtetés	A STARCOS (a feltételek betartása esetén) **megfelel** az SSCD-PP „A biztonsági jellemzők kezelése” követelményének.
Feltétel:	8.

Biztonságos biztonsági jellemzők (FMT_MSA.2)	
Követelmény (CC SSCD-PP)	A BALE biztosítsa, hogy biztonsági jellemzőknek (attribútumnak) csak biztonságos értékek lesznek elfogadva.
STARCOS tulajdonság	A STARCOS StarCert digitális aláírás alkalmazás minimalizálja a biztonsági jellemzők használatát: • nincs algoritmus és kulcsméretet befolyásoló biztonsági tulajdonság (mert csak a biztonságos RSA algoritmust valósítja meg 1024-es kulcsmérettel), • nincs "magán-nyilvános kulcspár kezelés" sem "magánkulcs működtetése" biztonsági jellemző (ezeket kényszerpályák, illetve rezsim intézkedések helyettesítik). Csak biztonságos értékek közül lehet választani: • az SHA-1 és RIPEMD-160 lenyomatoló függvény kiválasztásakor (mindkettő biztonságos), • az adattovábbítási protokoll és az aláírói kulcsok maximális száma konfigurálási opcióik kiválasztásakor. Az alábbi konfigurálási opcióik közötti választást pedig a 6. és 7. feltételekben meghatározott szabályok szerint helyesen (biztonságosan) kell megadni az inicializálás szakaszában, s később ez a biztonságos érték nem módosítható: • a kártyatulajdonos sikeres hitelesítését követő aláírások számára vonatkozó korlát (értéke 0 /nincs korlátozás/, ha egy hitelesítés-szolgáltató megbízható környezetében használják az intelligens kártyát, illetve 1 /a korlátozás csak 1 aláírást enged meg egy hitelesítés után/, • a globális PIN kóddal az SSL mindkét funkcionalitását (hitelesítés és dekódolás) védeni kell.
Ellenőrzött követelmények (STARCOS ITSEC tanúsítás)	• teljesülő SO2 biztonsági cél (A digitális aláírás funkció jogosulatlan használatának megakadályozása), • helyesen működő IA1 biztonsági funkció (Az emberi felhasználó hitelesítése), • helyesen működő AC1 biztonsági funkció (A parancsokhoz való hozzáférés ellenőrzése).

Értékelés	Amennyiben az alábbi két feltétel együttesen teljesül, akkor az elvárás teljesül:
	• a kártyatulajdonos sikeres hitelesítését követő aláírások számára vonatkozó korlát értéke az alábbi legyen:
	  • 0 /nincs korlátozás/, ha egy hitelesítés-szolgáltató megbízható környezetében használják az intelligens kártyát, illetve
	  • 1 /a korlátozás csak 1 aláírást enged meg egy hitelesítés után/, /a 6. feltétel ezt tartalmazza/,
	• az inicializálás szakaszában a STARCOS-t úgy kell konfigurálni, hogy az globális PIN kóddal védje az SSL mindkét funkcionalitását (hitelesítés és dekódolás). /7. feltétel/

Következtetés	A STARCOS (a feltételek betartása esetén) **megfelel** az SSCD-PP „Biztonságos biztonsági jellemzők" követelményének.
Feltétel:	6. és 7.

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.
STARCOS tulajdonság	A STARCOS közvetlenül nem támogatja a BALE-ra elvárt fenti követelményt, a mögötte meghúzódó érdemi elvárást viszont igen.
Ellenőrzött követelmények (STARCOS ITSEC tanúsítás)	• teljesülő SO2 biztonsági cél (A digitális aláírás funkció jogosulatlan használatának megakadályozása), • helyesen működő IA1 biztonsági funkció (Az emberi felhasználó hitelesítése), • helyesen működő AC1 biztonsági funkció (A parancsokhoz való hozzáférés ellenőrzése).
Értékelés	A STARCOS közvetlenül nem támogatja a BALE-ra elvárt fenti követelményt, a mögötte meghúzódó érdemi elvárást viszont igen. 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. Amennyiben az aláíráshoz szükséges kulcsokat még az intelligens kártya tulajdonosához juttatása előtt generálja az adminisztrátor, akkor az aláírás-létrehozás funkció aktivizálását a következők akadályozzák meg: • egy aláíró kulccsal aláírni csak az 5 digites transzport PIN kód legalább 6 digitesre való lecserélése után lehet, • az aláíró első aláírása előtt ellenőrzi (a 8/5. vagy 8/7 feltétel betartása esetén), hogy a neki átadott transzport PIN kód hossza valóban 5 digit-e.
Következtetés	A STARCOS (a feltételek betartása esetén) **megfelel** az SSCD-PP „Statikus jellemző inicializálás” követelményének.
Feltétel:	8.

A biztonsági funkciók adatainak kezelése (FMT_MTD.1)	
Követelmény (CC SSCD-PP)	A BALE a hitelesítő adatok (PIN kód) módosításának lehetőségét az aláíróra korlátozza.
STARCOS tulajdonság	A STARCOS a felhasználóra korlátozza saját PIN kódjának (jelszavának) módosítási lehetőségét. (A cserét megvalósító parancs sikeres végrehajtásához szükség van a régi PIN kód helyes megadására) A 8. feltétel betartása esetén az „aláíró” a felhasználó lesz.
Ellenőrzött követelmények (STARCOS ITSEC tanúsítás)	• teljesülő SO2 biztonsági cél (A digitális aláírás funkció jogosulatlan használatának megakadályozása), • helyesen működő IA2 biztonsági funkció (A hitelesítő adat cseréje), • helyesen működő IA3 biztonsági funkció (A hitelesítő adat blokkolása), • helyesen működő IA2 biztonsági funkció (A blokkolt hitelesítő adat feloldása és cseréje).
Értékelés	A STARCOS teljesíti az elvárást, az ITSEC értékelés igazolja ezt.
Következtetés	A STARCOS (a feltételek betartása esetén) **megfelel** az SSCD-PP „A biztonsági funkciók adatainak kezelése” követelményének.
Feltétel:	8.

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.
STARCOS tulajdonság	A STARCOS az alábbi szerepköröket támogatja: • adminisztrátor • felhasználó A 8. feltétel betartása esetén az „aláíró” a felhasználó lesz.
Ellenőrzött követelmények (STARCOS ITSEC tanúsítás)	• teljesülő SO2 biztonsági cél (A digitális aláírás funkció jogosulatlan használatának megakadályozása), • helyesen működő AC1 biztonsági funkció (A parancsokhoz való hozzáférés ellenőrzése).
Értékelés	A STARCOS teljesíti az elvárást, az ITSEC értékelés igazolja ezt.
Következtetés	A STARCOS (a feltételek betartása esetén) **megfelel** az SSCD-PP „A biztonsági szerepkörök” követelményének.
Feltétel:	8.

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.
Philips microchip tulajdonság	A P8WE5032v0G chip teszt üzemmódjában közvetlenül is támogatja, hogy az adminisztrátor kimutathassa az alapját képező absztrakt gép helyes működését. A P8WE5032v0G chip felhasználói üzemmódjában a helyes működés 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 (Philips ITSEC tanúsítása)	• helyesen működő F4 biztonsági funkció (Működési állapot ellenőrzés), • helyesen működő F5 biztonsági funkció (A fizikai manipuláció elleni védelem).
STARCOS tulajdonság	A STARCOS operációs rendszernek nincs olyan parancsa, mellyel közvetlen hardver tesztelést lehetne kiváltani. Ugyanakkor a chip az általa feldolgozott parancsok visszatérési értékeiben jelzi, ha meghibásodott, illetve blokkolt állapotba kerül. A host oldalról kiadható reset parancs pedig kiváltja a legszükségesebb hibaellenőrzési tesztrutinok futtatását.
Ellenőrzött követelmények (STARCOS ITSEC tanúsítás)	• teljesülő SO8 biztonsági cél (a biztonság potenciális megsértésére való reagálás), • helyesen működő AC3 biztonsági funkció (Blokkolt állapot).

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) vagy blokkolt állapotba kerüléssel 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 blokkolt állapotba kerülés STARCOS által megvalósított tulajdonságát (AC3 biztonsági funkció: Blokkolt állapot) is, a követelmény kielégítettnek tekinthető.
Következtetés	A STARCOS **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.
Philips microchip tulajdonság	A P8WE5032v0G 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 (Philips ITSEC tanúsítás)	• helyesen működő F4 biztonsági funkció (Működési állapot ellenőrzés), • helyesen működő F5 biztonsági funkció (A fizikai manipuláció elleni védelem).
STARCOS tulajdonság	A STARCOS véd minden ismert hardver támadás ellen, hatékonyan alkalmazva a hardver (Philips 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 STARCOS garantálja, hogy a kriptográfiai műveletek során generált vagy 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 STARCOS kezeli az összes olyan hardver alapú (a chip által támogatott) biztonsági mechanizmust, mely felhasználható a rejtett csatornák elemzésének a megakadályozására (mint amilyen a differenciál áramfelvételi támadás /SPA/ vagy az időréseket megfigyelő támadások /TA/). Az intelligens kártya valamennyi kriptográfiai művelete él a hardver mechanizmusok támogatásával.
Ellenőrzött követelmények (STARCOS ITSEC tanúsítás)	• teljesülő SO6 biztonsági cél (A kulcsgenerálás minősége), • teljesülő SO7 biztonsági cél (Biztonságos digitális aláírás szolgáltatása), • teljesülő SO8 biztonsági cél (A biztonság potenciális megsértésére való reagálás), • helyesen működő DX1 biztonsági funkció (Kulcs generálása és exportálása), • helyesen működő DX2 biztonsági funkció (Digitális aláírás létrehozása).

Értékelés	A STARCOS meghatározott (áram feszültségre és óra jel frekvenciára, valamint hőmérsékletre vonatkozó) korlátok között megakadályozza a magánkulcs, valamint a hitelesítő adat megismerését lehetővé tévő [DPA és TA 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 STARCOS **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]***
STARCOS tulajdonság	A STARCOS **megőriz egy biztonságos állapotot**, a következő típusú hibák bekövetkezése esetén: • **egy parancs végrehajtása során bekövetkező átmeneti vagy folyamatos hardver hiba,** • fizikai támadás. A STARCOS úgy reagál a fenti hibák észlelésekor, hogy biztonság politikája ne sérüljön (pl. az intelligens kártya megnyitott munkaszakasza ne maradjon használható a továbbiakban, komoly hiba vagy támadás esetén pedig blokkolt állapotba kerül). A STARCOS 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 (STARCOS ITSEC tanúsítás)	• teljesülő SO8 biztonsági cél (a biztonság potenciális megsértésére való reagálás), • helyesen működő AC3 biztonsági funkció (Blokkolt állapot).
Értékelés	A STARCOS AC3 biztonsági funkciója éppen a fenti elvárást teljesíti (hardver hiba és fizikai támadás hiba típusokra).
Következtetés	A STARCOS **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.
Philips microchip tulajdonság	A P8WE5032v0G 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 (Philips ITSEC tanúsítás)	• helyesen működő F4 biztonsági funkció (Működési állapot ellenőrzés), • helyesen működő F5 biztonsági funkció (A fizikai manipuláció elleni védelem).
STARCOS tulajdonság	A STARCOS megőriz egy biztonságos állapotot, a következő típusú hibák bekövetkezése esetén: • egy parancs végrehajtása során bekövetkező átmeneti vagy folyamatos hardver hiba, • **fizikai támadás.** A STARCOS 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 (STARCOS ITSEC tanúsítás)	• teljesülő SO8 biztonsági cél (a biztonság potenciális megsértésére való reagálás), • helyesen működő AC3 biztonsági funkció (Blokkolt állapot).
Értékelés	A STARCOS félreérthetetlen módon detektálja a biztonsági funkciók kompromittálódását okozható fizikai manipulálásokat. A STARCOS képes detektálni, hogy fizikai manipulálás történt a biztonsági funkció elemeire, vagy az azt megalapozó eszközökre.
Következtetés	A STARCOS **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.
Philips microchip tulajdonság	A P8WE5032v0G chip képes ellenállni a következő fizikai manipulációs forgatókönyvek (olyan automatikus reagálással, ami megakadályozza a BALE biztonsági politikájának megsértését): • **buszra kapcsolódás egy memória cella tartalmának megmérése vagy módosítása céljából,** • **egy belső áramkör módosítása,** • **a ROM-ban, EEPROM-ban, RAM-ban vagy az egyszer programozható memóriákban tárolt adatok módosítása, olyan környezeti feltételek megteremtésével, melyek elhagyják a chip biztonságos működési tartományát (mindezt akkor, mikor a chip nem futtat programot).**
Ellenőrzött követelmények (Philips ITSEC tanúsítás)	• helyesen működő F4 biztonsági funkció (Működési állapot ellenőrzés), • helyesen működő F5 biztonsági funkció (A fizikai manipuláció elleni védelem).
STARCOS tulajdonság	A STARCOS megőriz egy biztonságos állapotot, a következő típusú hibák bekövetkezése esetén: • egy parancs végrehajtása során bekövetkező átmeneti vagy folyamatos hardver hiba, • **fizikai támadás.** A STARCOS **úgy reagál a fenti támadások (**fizikai manipulációs forgatókönyvek) **észlelésekor, hogy biztonság politikája nem sérül** (pl. úgy, hogy az intelligens kártya megnyitott munkaszakasza ne maradjon használható a továbbiakban, vagy blokkolt állapotba kerüléssel).
Ellenőrzött követelmények (STARCOS ITSEC tanúsítás)	• teljesülő SO8 biztonsági cél (a biztonság potenciális megsértésére való reagálás), • helyesen működő AC3 biztonsági funkció (Blokkolt állapot).
Értékelés	A STARCOS ellenáll a *chip-jére* irányuló ***("buszra kapcsolódás egy memória cella tartalmának megmérése vagy módosítása céljából", "egy belső áramkör módosítása", "a ROM-ban, EEPROM-ban, RAM-ban vagy az egyszer programozható memóriákban tárolt adatok módosítása szélsőséges környezeti feltételek megteremtésével" forgatókönyveken alapuló támadásoknak***) olyan automatikus reagálással, ami megakadályozza biztonsági politikájának megsértését.
Következtetés	A STARCOS **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.
Philips microchip tulajdonság	A P8WE5032v0G chip teszt üzemmódjában közvetlenül is támogatja, hogy az adminisztrátor végrehajtson egy olyan teszt-sorozatot, mely kimutatja biztonsági funkciói helyes működését. A P8WE5032v0G chip felhasználói üzemmódjában a helyes működés 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 (pl. FameX hiba, XRAM hiba), • 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 (Philips ITSEC tanúsítás)	• helyesen működő F4 biztonsági funkció (Működési állapot ellenőrzés), • helyesen működő F5 biztonsági funkció (A fizikai manipuláció elleni védelem).
STARCOS tulajdonság	A STARCOS operációs rendszernek nincs olyan parancsa, mellyel közvetlen hardver tesztelést lehetne kiváltani. Ugyanakkor a chip az általa feldolgozott parancsok visszatérési értékeiben jelzi, ha meghibásodott, illetve blokkolt állapotba kerül. A host oldalról kiadható reset parancs pedig kiváltja a legszükségesebb hibaellenőrzési tesztrutinok futtatását.
Ellenőrzött követelmények (STARCOS ITSEC tanúsítás)	• teljesülő SO8 biztonsági cél (a biztonság potenciális megsértésére való reagálás), • helyesen működő AC3 biztonsági funkció (Blokkolt állapot).

A biztonsági funkciók tesztelése (FPT_TST.1) /folytatás/	
Értékelés	A STARCOS ***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 STARCOS indirekt módon biztosítja, hogy az arra feljogosított felhasználók képesek a biztonsági funkció adatok (attribútumok) sértetlenségének ellenőrzésére /azáltal, hogy bármely típusú attribútum sérülése esetén az attribútumokra számított ellenőrző összeg hibát mutat, s ez az érintett objektumhoz való hozzáférést azonnal és véglegesen elérhetetlenné teszi/. A STARCOS indirekt módon biztosítja, hogy az arra feljogosított felhasználók képesek a végrehajtható kódok sértetlenségének ellenőrzésére /azáltal, hogy a fájlokban tárolt adatokra vonatkozó ellenőrzőösszeg képzés a végrehajtható kódokat tartalmazó fájlokra is teljesül/.
Következtetés	A STARCOS **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./	
STARCOS tulajdonság	A STARCOS **képes az általa generált nyilvános kulcsot aláírni** (saját hitelesítő aláíró kulcsával), s ezzel egy megbízható csatornát kiépíteni a tanúsítvány-létrehozó alkalmazással (mely a hitelesítő-szolgáltatónál ellenőrizheti az aláírás **hitelességé**t. A STARCOS **képes SSL hitelesítési és dekódolási funkcionalitását aktivizálni,** s ezzel egy megbízható csatornát kiépíteni az aláírás-létrehozó alkalmazással. Ezen a csatornán az alkalmazás és az intelligens kártya között kicserélt adatok bizalmassága, hitelessége és **sértetlensége** egyaránt megvédhető. Mind a nyilvános kulcs exportálásához, mind az aláírandó adat reprezentáns importálásához használható (és az 5. feltétel szerint használandó is) ez a megbízható csatorna (hitelességet és sértetlenséget biztosító megbízható adatcsere). A STARCOS 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 (STARCOS ITSEC tanúsítás)	A STARCOS SPK 2.3 v 7.0 ITSEC értékelése nem vizsgálta a termék fenti /SSL alapján megvalósított titkos üzenetváltás/ funkcionalitás helyes megvalósítását, bár megemlítette létezését. Egy másik termék /a STARCOS SPK 2.4 operációs rendszer tachográf kártya alkalmazással/ ITSEC értékelése (melynek garanciaszintje szintén megfelelően magas -E3- volt) ugyanakkor már vizsgálta és tanúsította ezt a funkcionalitást is. A fejlesztőktől származó nyilatkozat szerint a két termék "ugyanazt a megbízható csatornát használja a "biztonságos adatcsere" funkción keresztül".
Értékelés	Az 5. feltétel teljesítése esetén (melyet a STARCOS támogat) kiépülő megbízható csatorna biztosítja végpontjainak garantált azonosítását és a továbbított adatok (nyilvános kulcs és aláírandó adat reprezentáns) illetéktelen módosítás elleni védelmét. A megbízható csatornán való kommunikáció külső kezdeményezésének kötöttsége nem mond ellen az elvárásnak, csak szűkíti annak választási lehetőségét (a STARCOS nem képes kezdeményezni).
Következtetés	A STARCOS (a feltételek betartása esetén) **megfelel** az SSCD-PP „Megbízható csatorna” követelményének.
Feltétel:	5.

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]]***.
STARCOS tulajdonság	A STARCOS **képes SSL hitelesítési és dekódolási funkcionalitását aktivizálni,** s ezzel egy 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, • hitelességét és • sértetlenségét. Mind a kezdeti felhasználói hitelesítéshez (PIN kód vagy jelszó megadáshoz), mind a hitelesítési adatok (PIN kód vagy jelszó) cseréjéhez használható (és az 5. feltétel szerint használandó is) ez a megbízható útvonal (bizalmasságot, hitelességet és sértetlenséget biztosító titkos üzenetváltás). A STARCOS elvi felépítése miatt a helyi felhasználónak kell kezdeményeznie a megbízható útvonal kiépítését.
Ellenőrzött követelmények (STARCOS ITSEC tanúsítás)	A STARCOS SPK 2.3 v 7.0 ITSEC értékelése nem vizsgálta a termék fenti /SSL alapján megvalósított titkos üzenetváltás/ funkcionalitás helyes megvalósítását, bár megemlítette létezését. Egy másik termék /a STARCOS SPK 2.4 operációs rendszer tachográf kártya alkalmazással/ ITSEC értékelése (melynek garanciaszintje szintén megfelelően magas -E3- volt) ugyanakkor már vizsgálta és tanúsította ezt a funkcionalitást is. A fejlesztőktől származó nyilatkozat szerint a két termék "ugyanazt a megbízható csatornát használja a "biztonságos adatcsere" funkción keresztül".

Megbízható útvonal (FTP_TRP.1) /folytatás/ /A helyi felhasználó és a BALE között./	
Értékelés	Az 5. feltétel teljesítése esetén (melyet a STARCOS 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 STARCOS nem képes kezdeményezni). A STARCOS-nak (az 5. feltétel szerint) az alábbi esetekben kell megkövetelnie a biztonságos útvonal használatát: • kezdeti felhasználói hitelesítés, • a hitelesítési adatok cseréje.
Következtetés	A STARCOS (a feltételek betartása esetén) **megfelel** az SSCD-PP „Megbízható útvonal” követelményének.
Feltétel:	5.

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

Funkcionális biztonsági követelmények	A teljesülést elősegítő feltételek
FCS_CKM.1 Kriptográfiai kulcs generálás	---
FCS_CKM.4 Kriptográfiai kulcs megsemmisítés	---
FCS_COP.1 Kriptográfiai eljárás	3., 8.
FDP_ACC.1 Részleges hozzáférés ellenőrzés	8.
FDP_ACF.1 Biztonsági jellemzőkön alapuló hozzáférés ellenőrzés	8.
FDP_RIP.1 Részleges maradvány információ védelem	---
FDP_SDI.2 A tárolt adatok sértetlenségének figyelése és beavatkozás	---
FDP_UIT.1 Az adatcsere sértetlensége	5.
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	---
FMT_MOF.1 A biztonsági funkciók viselkedésének kezelése	8.
FMT_MSA.1 A biztonsági jellemzők kezelése	8.
FMT_MSA.2 Biztonságos biztonsági jellemzők	6., 7.
FMT_MSA.3 Statikus jellemző inicializálás	8.
FMT_MTD.1 A biztonsági funkciók adatainak kezelése	8.
FMT_SMR.1 Biztonsági szerepkörök	8.
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	5.
FTP_TRP.1 Megbízható útvonal	5.

6.2 A STARCOS 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 STARCOS 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 STARCOS intelligens kártya kielégíti a 3-as típusú BALE-re vonatkozó EAL4-es garancia szintű védelmi profil /Protection Profile – Secure Signature-Creation Device Type 3, version: 1.05, EAL4/ **valamennyi követelményét.**

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

A P8WE5032v0G mikrochip-ből
és a STARCOS SPK 2.3 v 7.0 operációs rendszerből, valamint a
StarCert v 2.2 digitális aláírás alkalmazásból álló
intelligens kártya
/Philips Semiconductors GmbH, Germany,
Giesecke & Devrient GmbH, Germany/

a tanúsítás érvényességi feltételeinek[28] együttes teljesülése esetén

ALKALMAS

minősített aláírások létrehozására,

mint

3-as típusú biztonságos aláírás-létrehozó eszköz.

[28] Lásd a 7.2 “Az eredmények érvényességi feltételei” alfejezet 1.-10 feltételeit.

7.2 Az eredmények érvényességi feltételei

A P8WE5032v0G mikrochip-ből és a STARCOS SPK 2.3 v 7.0 operációs rendszerből, valamint a StarCert v 2.2 digitális aláírás alkalmazásból álló (STARCOS) 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 STARCOS intelligens kártyát minősített aláírások létrehozására kívánják felhasználni, olyan biztonsági követelményeknek kell megfelelni, melyek a felhasználhatóságot korlátozzák, különböző feltételek betartását követelik meg.

Az alábbiakban összefoglaljuk azokat a feltételeket, melyek **együttes** betartása feltétele a STARCOS intelligens kártya biztonságos aláírás-létrehozó eszközként 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 STARCOS intelligens kártya szolgáltatásait igénybe vevő adminisztrátorok és felhasználók (aláírók) jól képzettek és megbízhatóak.

2. A STARCOS intelligens kártya szolgáltatásait igénybe vevő adminisztrátorok és felhasználók titokban tartják saját PIN kódjukat.

7.2.2 Az ITSEC tanúsítások érvényességi feltételei

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

Nincs ilyen feltétel.

7.2.3 A biztonságos aláírás-létrehozó eszközként történő használhatóság kiegészítő feltételei

Egy minősített aláírásokat létrehozó aláírónak a STARCOS felhasználása során az alábbi kiegészítő feltételeket is be kell tartania:

3. A digitális aláírással kapcsolatos kriptográfiai funkcionalitást az alábbi feltöltő (padding) algoritmusra kell korlátozni: PKCS#1-es v 1.5

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

5. Bizalmasságot, hitelességet és sértetlenséget biztosító titkos üzenetváltást kell biztosítani (az SSL protokoll aktivizálásával, 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.

6. A kártyatulajdonos sikeres hitelesítését követő aláírások számára vonatkozó korlátot a következőképpen kell konfigurálni:
   - értéke 0 /nincs korlátozás/, ha egy hitelesítés-szolgáltató megbízható környezetében használják az intelligens kártyát, illetve
   - értéke 1 /a korlátozás csak 1 aláírást enged meg egy hitelesítés után/, amennyiben egy magánszemély használja aláírási célból az intelligens kártyát.

7. A globális PIN kódot úgy kell konfigurálni, hogy az SSL mindkét funkcionalitását (hitelesítés és dekódolás) védje.

8. Egy BALE-ként használt STARCOS esetén az adminisztrátor és felhasználó (aláíró) szerepkörök szétválasztásával, valamint az inicializálási, perszonalizálási folyamatoknál alkalmazott programok és rezsim szabályok együttműködésével biztosítani kell a következőket:

   Amennyiben az adminisztrátor generálja az aláírói kulcspár(oka)t:
   1. A generálási folyamat során az „adminisztrátor” hajtson végre egy páronkénti megfelelőség tesztet (az aláíráshoz generált nyilvános – magánkulcs pár összetartozásának ellenőrzését), és csak sikeres eredmény esetén kérhető a nyilvános kulcsra tanúsítvány.
   2. Az „adminisztrátor” biztonságosan (az 5. feltételt betartva, megbízható csatornán keresztül) exportálja a legenerált nyilvános kulcsot tanúsítvány készítés céljából.
   3. A hitelesítés-szolgáltató által elkészített tanúsítványt az adminisztrátor továbbítsa az intelligens kártyának.
   4. Az „adminisztrátor” az 5 digites transzport PIN kód átadásával (nem feltétlenül személyesen, de mindenképp egy biztonságos átadási eljárás keretében) engedélyezze a felhasználó számára az aláírási funkció aktivizálását, s egyúttal (ha még nincs az összes legenerálható kulcspár legenerálva) a további aláírói kulcspárok generálását.
   5. A felhasználó ellenőrizze le a kapott transzport PIN kód hosszúságát, s csak akkor fogadja el, ha az 5 digites. Ekkor az első kártyával kapcsolatos tevékenysége a PIN kód lecserélése legyen, egy legalább 6 digitből álló saját PIN kódra.

Amennyiben a felhasználó generálja saját aláírói kulcspárj(á/ai)t:

6. Az „adminisztrátor” az 5 digites transzport PIN kód átadásával (nem feltétlenül személyesen, de mindenképp egy biztonságos átadási eljárás keretében) engedélyezze a felhasználó számára az aláírói kulcspárok generálását, valamint az aláírási funkció későbbi aktivizálását.
7. A felhasználó ellenőrizze le a kapott transzport PIN kód hosszúságát, s csak akkor fogadja el a kártyát, ha a PIN kód 5 digites. Ebben az esetben az első kártyával kapcsolatos tevékenysége a PIN kód lecserélése legyen, egy legalább 6 digitből álló saját PIN kódra.
8. Ezt követően a felhasználó generálja le magának aláírói kulcs(á/ai)t, s a folyamat során hajtson végre egy páronkénti megfelelőség tesztet (az aláíráshoz generált nyilvános – magánkulcs pár összetartozásának ellenőrzését). Csak sikeres eredmény esetén kérhető a nyilvános kulcsra tanúsítvány.
9. A felhasználó biztonságosan (az 5. feltételt betartva, megbízható csatornán keresztül) exportálja a legenerált nyilvános kulcsot tanúsítvány készítés céljából.
10. Végül a hitelesítés-szolgáltató által elkészített tanúsítványt a felhasználó küldje át az intelligens kártyára.

9. Az aláíró csak megbízható (host oldali) aláírás-létrehozó alkalmazást használhat.

10. Jelen Tanúsítvány csak a jelenlegi verzióra érvényes:
/P8WE5032v0G chip, SPK 2.3 v 7.0 operációs rendszer, StarCert v 2.2 alkalmazás/

Új chip verzió esetén mind a chip-re, mind az operációs rendszerre és alkalmazásra új tanúsítás szükséges.
Amennyiben csak az operációs rendszer vagy az alkalmazás változik, elég egy olyan új, az operációs rendszerre és az alkalmazásra 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-0158-2001 Certification /for Philips Smart Card Controller P8WE5032V0G/

BSI-DSZ-ITSEC-0158-2001 Certification Report /for Philips Smart Card Controller P8WE5032V0G/

BSI-DSZ-ITSEC-0158 Security Target /Evaluation on Philips P8WE5032 Secure 8-bit Smart Card Controller Version P8WE5032V0G/

T-Systems 02078.TE.12.2001 Certification /Signature Creation Device "Integrated Circuit Card with processor P8WE5032V0G and STARCOS SPK 2.3 v 7.0 with Digital Signature Application StarCert v 2.2/

T-Systems-DSZ-ITSEC-04075-2001 Certification Report /STARCOS SPK 2.3 v 7.0 with Digital Signature Application StarCert v 2.2/

T-Systems-DSZ-ITSEC-04075-2001 Security Target /StarCert version 2.2 signature application on STARCOS SPK 2.3 version 7.0/

BSI-DSZ-ITSEC-0172-2003 IT-Sicherheitszertifikat /zu STARCOS SPK 2.4 mit Tachograph Card Applikation/

BSI-DSZ-ITSEC-0172-2003 Zertifizierungreport /zu STARCOS SPK 2.4 mit Tachograph Card Applikation/

BSI-DSZ-ITSEC-0172-2003 Sicherheitsvorgaben /zu STARCOS SPK 2.4 mit Tachograph Card Applikation/

A Giesecke & Devrient felelős vezetőinek írásos nyilatkozata arról, hogy a STARCOS SPK 2.3 v7.0 és a STARCOS 2.4 (Tachográf kártya alkalmazással) ugyanazt a megbízható csatornát valósítja meg a "biztonságos adatcsere" funkción keresztül".

9. Rövidítések

AC	Access Control
AE	Assumption about the Environment
BALE	Biztonságos aláírás-létrehozó eszköz
BSI	Bundesamt für Sicherheit in der Informationtechnik
CA	Certification Authority
CC	Common Criteria
CEN	European Comittee for Standardization
CH	Card Holder
CPU	Central Processing Unit
DES	Data Encryption Standard /FIPS PUB 46-3, FIPS PUB 74, FIPS PUB 81/
DPA	Differencial Power Analysis
DSA	Digital Signature Algorithm /FIPS PUB 186-2/
EAL	Evaluation Assurance Level
EEPROM	Electrically Erasable Programmable Read Only Memory
IEC	International Electrotechnical Comission
I/O	Input/output
ISO	International Organization for Standardization
ISSS	Information Society Standardization System
ITSEC	Information Technology Security Evaluation Criteria
ITSEM	Information Technology Security Evaluation Manual
PIN	Personal Identification Number
PKCS	Public Key Cryptographic Standards
PKCS #1	RSA Cryptography Standard
PP	Protection Profile
PUK	PIN Unblocking Key
RA	Registration Authority
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/
SK	Secret Key
SO	Security Objective
SSCD	Secure Signature Creation Device (lásd BALE)
SSL	Secure Sockets Layer
T	Threat
TA	Timing Attacks
Triple-DES	/FIPS PUB 46-3, ANSI X9.52/
UART	Universal Asynchronous Receiver/transmitter
XRAM	eXtended Random Access Memory