Tanúsítási jelentés

Hung-TJ-007-2003

a CSA8000 kriptográfiai adapter

biztonságos aláírás-létrehozó eszközről

/ Eracom Technologies Group, Eracom Technologies Australia, Pty. Ltd./

/hardver verzió: G revízió,
Cprov förmver verzió: 1.10/

Tartalom

1. A tanúsítási jelentés tárgya, feladata és hatóköre

Jelen tanúsítási jelentés tárgya a CSA8000 kriptográfiai adapter, melyet minősített aláírás létrehozásához kívánnak felhasználni, mint biztonságos aláírás-létrehozó eszközt (BALE).

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

1. *A biztonságos aláírás-létrehozó eszköznek megfelelő technikai és eljárási eszközökkel biztosítaniuk kell legalább a következőket:*

   a) *az aláírás készítéséhez használt aláírás-létrehozó adat aláírónként biztosan mindig különbözik, s titkossága kellően biztosított,*

   b) *az aktuálisan elérhető technológiával kellő bizonyossággal garantálható, hogy az aláírás készítéséhez használt aláírás-létrehozó adat nem rekonstruálható, megvalósítható annak a jogosulatlan felhasználókkal szembeni védelme, illetve az aláírás nem hamisítható.*

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

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

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.”

Az 1-es típus szigorúan véve nem is BALE, csak azok a hitelesítés-szolgáltatók használhatják, melyek felvállalják az aláíró előfizetők számára történő kulcsgenerálás („aláírás-létrehozó eszközön az aláírás-létrehozó adat elhelyezése") szolgáltatását.

A HUNG-T-001-2003. számú tanúsítás szerint:

„a CSA8000 Adapter
…
megfelel
…….
Aláírás-létrehozó eszközön az aláírás-létrehozó adat elhelyezése szolgáltatás keretén belül:
az előfizetői (aláírói) kulcspár generálására."

A fenti állítás azt jelenti, hogy **a CSA8000 használható 1-es típusú BALE-ként**.

Jelen tanúsítási jelentés ugyanakkor a CSA8000 Adapter 3-as típusú BALE-ként való felhasználhatóságával foglalkozik[3].

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 CSA8000 kriptográfiai adapter 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.

Jelen tanúsítási jelentés fő feladata annak megállapítása, hogy:

- a CSA8000 kriptográfiai adapterre vonatkozó értékelési és tanúsítási eredmények (FIPS 140-1 3-as szint) alapján ki lehet-e mutatni, hogy a kriptográfiai adapter megfelel az egyik „BALE specifikus" védelmi profil követelményeinek is, s ezáltal alkalmas-e minősített aláírás-létrehozáshoz való felhasználásra,
- a FIPS 140-1 követelményeknek való megfelelést igazoló tanúsítvány érvényessége, illetve a többi kielégítendő funkcionális és biztonsági

[3] Mert a tanúsítási jelentés megrendelője ilyen formában is fel kívánja használni az adaptert, attól függetlenül, hogy 1-es típusú BALE-ként már használja is (egészen eltérő feltétel rendszer mellett).

követelmény teljesülése milyen korlátozásokat, feltételeket támaszt a kriptográfiai adapter (3-as típusú BALE-ként való) felhasználására.

Jelen tanúsítási jelentés hatóköre ugyanakkor csak a biztonságos aláírás-létrehozó eszközként való felhasználhatóságra és ennek feltétel-rendszerének meghatározására szorítkozik.
Nem terjed ki a CSA8000 kriptográfiai adapter egyéb, köztük a FIP 140-1 tanúsítvánnyal igazolt tulajdonságaira, beleértve az alábbiakat:

- A FIPS 140-1-es tanúsítvány érvényességébe tartozó, FIPS által jóváhagyott titkosító algoritmusra /DES, Triple-DES/,
- a CSA8000 adapter által megvalósított azon kriptográfiai algoritmusokra, melyek nem FIPS által jóváhagyott algoritmusok, s így már a FIPS értékelés sem terjedt ki rájuk /HMAC-SHA-1, RSA (kódolás, dekódolás), CAST128, IDEA, AES[4] RC2, RC4, MD2, MD5, Diffie-Hellman (kulcsegyeztetés)/.

A tanúsítási jelentés további szerkezete a következő:

- A CSA8000 kriptográfiai adapter legfontosabb tulajdonságai (2. fejezet).
- A CSA8000 kriptográfiai adapterre vonatkozó FIPS 140-1-es tanúsítvány eredményei (3. fejezet).
- A FIPS 140-1 (3-as biztonsági szint) megfelelőségéből adódó, **kielégített funkcionális biztonsági követelmények** (4. fejezet).
- A FIPS 140-1 (3-as biztonsági szint) megfelelőségéből adódó, **kielégített garanciális biztonsági követelmények** /az értékeléshez megkövetelt fejlesztői bizonyítékok/ (5. fejezet).
- A Common Criteria SSCD védelmi profil bevezető, követelményeket megalapozó részeinek ismertetése /biztonsági környezet (kivédendő veszélyek és érvényre juttatandó biztonsági szabályok), biztonsági célok/ (6. fejezet).
- Az SSCD védelmi profil által **elvárt funkcionális biztonsági követelmények** (7. fejezet).
- Az SSCD védelmi profil által **elvárt garanciális biztonsági követelmények** (8. fejezet).
- Az SSCD védelmi profil által **elvárt követelményeknek való megfelelés levezetése a** FIPS 140-1 3-as szintű tanúsítás által igazolt **kielégített követelményekből**, valamint a CSA8000 kriptográfia adapter tulajdonságaiból (9. fejezet).
- A minősített aláírás-létrehozáshoz való alkalmasság megállapítása, valamint az alkalmazás feltételeinek és korlátainak a meghatározása (10. fejezet).
- A jelen tanúsítási jelentéshez figyelembe vett dokumentumok jegyzéke (11. fejezet).
- A felhasznált rövidítések jegyzéke (12. fejezet).

[4] az értékeléskor az AES még nem volt FIPS jóváhagyott algoritmus.

2. A CSA8000 legfontosabb tulajdonságainak összefoglalása

Az Eracom CSA8000 Adapter egy intelligens PCI adapter kártya, mely a kriptográfiai funkciók széles választékát biztosítja, speciális tervezésű DES, TripleDES és RSA hardver gyorsítók alkalmazásával.
A kriptográfiai modul támogatja kulcs tároló intelligens kártyák (smart card token) használatát.
A modul egy FIPS-engedélyezett förmvert, az ún. Cprov-t futtatja, mely a PKCS #11 kriptográfiai alkalmazói programozói interfészt (API) valósítja meg[5]. Bár bizonyos PKCS #11 tulajdonságokat nem támogat a modul, ugyanakkor biztosítja a PKCS #11 szabványnak való átfogó megfelelőséget, illetve bizonyos felhasználó-specifikus kiterjesztéseket[6] is támogat.
A CSA8000 Adapter kielégíti a FIPS 140-1 követelményeit, a 3. biztonsági szinten, a több chip-es, beágyazott modulok fizikai implementálása mellett.

2.1 A kriptográfiai modul

A CSA8000 segítségével nagy hatékonyságú PKI kriptográfiai funkciók integrálhatók minden olyan rendszerbe, mely tartalmaz szabványos, 33MHz-es, 32 bites slot-ot.
A modul kriptográfiai határa az adapter kártya nagy részét magába foglalja (kivéve a kártya azon végét, ahol az elemek csatlakoztathatók). A modul kriptográfiai határa magába foglalja az alábbi elemeket: kriptográfiai processzor (DCP), beágyazott processzor, SDRAM memória chip-ek, belső óra (RTC), hardver véletlenszám generátor, 32 bites RISC mikroprocesszor (a gyors kriptográfiai feldolgozáshoz és menedzsmenthez). Az adapter kriptográfiai határát egy polikarbonátból készült erős borítás képezi, mely beavatkozás elleni védelmet biztosít.
Az adaptert előzetesen feltöltik a FIPS-engedélyezett “Cprov” elnevezésű förmverrel. Egy új förmver verzió jövőbeli biztonságos feltöltése érdekében az Eracom cég digitálisan aláírja a hiteles új verziókat, az adapter pedig képes az aláírás ellenőrzésére.

2.2 Modul interfészek

A CSA8000 modulnak 4 fizikai interfésze van: egy szabványos PCI busz, két RS232 soros port, illetve egy áram interfész a kikapcsolt állapotban memóriatartalom őrzést biztosító tartalék elemek felé.
Valamennyi PCI buszon vagy soros porton érkező kérést az adapter processzora értelmez, ellenőrizve a kártya kriptográfiai szolgáltatásaihoz és kulcsaihoz való hozzáférést. Ez a processzor válaszol a PKCS #11 funkció parancsokra is, biztosítva, hogy a FIPS üzemmódban csak hitelesített operátorok kaphassanak kriptográfiai szolgáltatást (lásd a Tanúsítás 3. érvényességi feltételét az alkalmazandó biztonsági beállításokról).
Az alkalmazások kizárólag a PCI buszon keresztül érik el a kriptográfiai modult, ugyanakkor ezen interfészen belül logikailag elkülönülnek az adat input, adat output, vezérlési input, státusz output, valamint elektromos áram interfészek. Ugyancsak elkülönítve kezelődnek a különböző operátorok üzenetei.

[5] Ezen az API-n keresztül lehet a CSA8000 kriptográfiai modult egy informatikai rendszerbe integrálni.
[6] Ezen kiterjesztések a FIPS 140-1-nek megfelelő üzemmódban tiltottak.

2.3 Megbízható csatornák

A CSA8000 megbízható csatornát képes kiépíteni, melyen keresztül az operátorok biztonságosan kommunikálhatnak a PCI busz interfészen keresztül a modullal. A megbízható csatornák munkaszakasz kulcsokat (session key) használnak az üzenetek titkosítására/dekódolására, illetve digitális aláírására/a digitális aláírás ellenőrzésére. FIPS üzemmódban kötelező a megbízható csatornák kiépítése és használata (lásd a Tanúsítás 3. érvényességi feltételét az alkalmazandó biztonsági beállításokról).
A CSA8000 párhuzamosan (egyidejűleg) több megbízható csatorna kiépítésére képes, mindegyikben külön véletlenül generált munkaszakasz kulcsokkal. Az adapter háromszoros DES kulcsokat (ezek az ún. HIMK kulcsok) használ. Minden operátornak rendelkeznie kell ezen HIMK kulcsok egyikével, ahhoz, hogy megbízható csatornát építhessen ki a modullal. A HIMK kulcsok titkos értékeit (véletlenül generált adatok mellett) használják a megbízható csatornák munkaszakasz kulcsainak kialakításához (mind az adapter, mind az operátorok oldalán). A CSA8000 adapter a HIMK-kat az Admin tokenen (vagyis az adminisztrátor által birtokolt és őrzött intelligens kártyán) tárolja.
A kezdeti installálást követően az adapter egy HIMK-t tartalmaz, alap (default) értékkel. Az adminisztrátor új HIMK értékeket generáltathat, illetve törölhet régieket, köztük a default értéket is. FIPS üzemmódban kötelező új HIMK(-k) generálása és a default érték törlése (lásd a Tanúsítás 4. érvényességi feltételét).

2.4 Szolgáltatások és szerepkörök

A CSA8000 Adapter operátorainak azonosságán alapuló hitelesítését támogatja, egyben lehetővé teszi több operátor egyidejű kiszolgálását, az operátorok számára egyedileg (szerepkörük alapján) kijelölt, jogosult szolgáltatás körből. Az egyes operátorok egyidejűleg több munkaszakaszt is nyithatnak. Az operátorok hitelesítése PIN kódjuk megadását, illetve ellenőrzését jelenti.

A szerepkörök a PKCS #11 token koncepcióján alapulnak. Minden token kriptográfiai objektumok egy készlete. Minden tokennek két operátora van: egy kriptográfiai tisztviselő és egy felhasználó. A CSA8000 modul három fajta tokent támogat: egy adminisztrátori tokent, több Cprov tokent, illetve egy vagy több fizikai intelligens kártya tokent. Az adminisztrátori token kriptográfiai tisztviselője és felhasználója különleges jogosultságokkal rendelkezik, így a CSA8000 négy szerepkört támogat:

- Adminisztrátori kriptográfiai tisztviselő
  Elsődleges felelőssége az Adminisztrátor rendszerbe léptetése, annak kezdeti PIN kódjának megadásával. A szerepkör elérését egy gyári beállítású alap (default) azonosító és jelszó teszi lehetővé. Az Adminisztrátori kriptográfiai tisztviselő felelőssége ezen default érték lecserélése is, lásd a Tanúsítás 5. érvényességi feltételét.
- Adminisztrátor
  Ő a felelős a CSA8000 általános biztonságkezeléséért, valamint a slot[7]-ok és a Token kriptográfiai tisztviselők ellenőrzéséért.

[7] A PKCS #11 egy slot-ot olyan logikai olvasóként definiálja, mely potenciálisan egy tokent tartalmaz.

- Token kriptográfiai tisztviselő
  Ő a felelős egy token tulajdonjogának megadásáért, illetve visszavonásáért. Ha egy tokennek nincs felhasználói PIN-je, akkor neki kell inicializálnia azt, kezdeti felhasználói PIN értéket és címkét hozzárendelve. Ő vonhatja vissza a Token felhasználó jogosultságait, s esetleg egy másik operátorhoz rendelheti ezen jogosultságokat, de csak valamennyi létező kulcs törlése után.
- Token felhasználó
  Saját token-jein, saját magán és nyilvános kulcsait gondozhatja, illetve használhatja.

A CSA8000 Adapter szolgáltatásai és kulcsgondozása a PKCS #11 API-n alapulnak, a szolgáltatások elérése pedig a tokeneken és a token tároló objektumain alapul. Minden objektumra attribútumok határozzák meg, hogy a kriptográfiai tisztviselők és felhasználók hozzáférhetnek-e, illetve milyen parancsokat hajthatnak rajta végre. Az adapter háromféle tároló objektumot támogat:

- Rendszer objektum
  (Az adminisztrátori token objektumai, melyek csak az adapter Adminisztrátorai számára elérhetőek.)
- Magán objektum
  (Csak a Token felhasználó számára elérhetőek.)
- Nyilvános objektum
  (Az adapter valamennyi operátora számára elérhetőek, de a felhasználóknak hitelesíteniük kell magukat a token felé, mielőtt kriptográfiai műveleteket végezhetnének ezekkel az objektumokkal.)

A megbízható csatornákat az adapter hozzáférés ellenőrzésének részeként használják. Az operátoroknak megbízható csatornát kell létesíteniük, mielőtt PIN kódjuk megadásával hitelesítenék magukat a token számára. Sikeres hitelesítés után a megbízható csatorna alkalmazás oldalának minden kriptográfiai szolgáltatás kérésre vonatkozó üzenetet hitelesítenie kell[8]. Az adapter pedig ellenőrizni fog minden kriptográfiai szolgáltatás kérésre vonatkozó üzenetet, és sikertelen ellenőrzés esetén visszautasítja a kérést.

2.5 Fizikai biztonság

A CSA8000 adaptert egy polikarbonátból készült erős, átlátszatlan borítás fedi, megvédve a kriptográfiai összetevőket a megfigyeléstől. A borítás alatt nyomásérzékelő mikrokapcsolók és érzékelők vannak elhelyezve, melyek beavatkozás elleni védelmet biztosítanak. A borítás bármely részének megbontása a biztonságkritikus paramétereket (kriptográfiai kulcsok és PIN kódok) tartalmazó memória nullázását eredményezi. A modul áramellátási állapotától függően ez a nullázódás kétféleképpen következik be: bekapcsolt állapotban az eszköz minden biztonságkritikus paramétert felülír, kikapcsolt állapotban pedig a tartalék (elem) áramforrás leszakad a RAM-ról. A CSA8000 adapter lehetővé teszi a nullázás beállítását arra az esetre is, amikor a modult a gazdagép PCI slot-jából kiemelik, sőt egy olyan interfésze is van, melybe egy külső behatolás érzékelő köthető be.

[8] Egy 20 byte-os HMAC-SHA-1 érték generálásával, melyet az előzőleg küldött üzenet hitelesítő kódjából, illetve az aktuális üzenet tartalmából számolnak ki.

Az adapter megfelel az otthoni használatra tervezett személyi számítógépekre és perifériákra vonatkozó, elektromágneses interferencia és elektromágneses kompatibilitás (FCC) követelményeinek.

2.6 Biztonságos kriptográfia

A CSA8000 kriptográfia modul biztonságos módon adminisztrálja a kriptográfiai kulcsokat, valamint az egyéb biztonságkritikus paramétereket, mint pl. a PIN kódokat. Az adapter az alábbi kulcsokkal kapcsolatos funkciókat képes biztosítani:

- kulcsok generálása,
- kulcsok importálására és exportálására (kulcs titkosító kulcs védelme alatt),
- kulcsok tárolása,
- kulcsok törlése,
- kulcsok intelligens kártyára történő mentése.

Az adapter kulcstípusai az alábbiak:

HIMK /Host Interface Master Key/	Közös titkok az alkalmazások (operátorok) és az adapter közötti kezdeti kézfogás védelmére.
HIK /Host Interface Key/	Egyedi kulcs, melyet minden egyes munkaszakaszhoz egy kulcsegyeztetési eljárással alakítanak ki (session kulcsnak is nevezik).
Felhasználói magánkulcsok	A felhasználók szimmetrikus és aszimmetrikus kulcsokat hozhatnak létre, az adapter által megvalósított kriptográfiai mechanizmusok végrehajtásához.
Nyilvános kulcsok	A modul valamennyi felhasználója számára elérhető szimmetrikus és aszimmetrikus kulcsok[9].

Az adapter az alábbi kriptográfiai mechanizmusokat támogatja (bár nem mindegyik elérhető a FIPS 140-1-nek megfelelő üzemmódban, s ezen belül sem mindegyik tárgya jelen, kizárólag digitális aláírással kapcsolatos Tanúsítási jelentésnek):

Szimmetrikus titkosító algoritmusok	CAST128, DES TripleDES (kétszeres és háromszoros kulcshosszúság mellett egyaránt), IDEA, RC2, RC4, AES
Szimmetrikus titkosító üzemmódok	ECB, CBC, OFB
Üzenet hitelesítő kódok /MAC/ generálása	HMAC-MD5, HMAC-RMD128, HMAC-RMD160
Aszimmetrikus algoritmusok	RSA, RSA PKCS #1, DSA, Diffie-Hellman
Lenyomatoló függvény	SHA-1, MD2, MD5, RIPEMD-128, RIPEMD-160
Tanúsítvány gondozás	X509 v3 tanúsítvány generálása (RSA és DSA aláírással), aláírások ellenőrzése X509 v3 tanúsítvány alapján (RSA, DSA), PKCS#10 tanúsítvány kérelem generálása, dekódolása (RSA, DSA), PKCS#7 tanúsítvány/tanúsítvány visszavonási lista csomag

[9] FIPS üzemmódban a nem hitelesített Token felhasználók és Token kriptográfiai tisztviselők láthatják ugyan a nyilvános kulcsokat, de kriptográfiai műveleteket nem végezhetnek velük (lásd a Tanúsítás 3. érvényességi feltételét, ezen belül a “No Public Cryptography” flag-et).

	(RSA, DSA).

A CSA8000 egy hardver véletlenszám generátort alkalmaz, a gyors kulcsgenerálás érdekében egy FIPS által jóváhagyott véletlenszám generálási technikával (FIPS 186-2) kombinálva. Az adapteren belül generált RSA és DSA nyilvános kulcsokat egy (a gyártástól kezdve az adapteren belül tárolt) aláíró kulccsal digitálisan alá lehet írni, ezzel bizonyítva az adapter általi generálás eredetiségét.
Generálás és letárolás után egy kulcsot exportálni is lehet.
Egy kulcsot átmenetileg (ekkor a kommunikációs munkaszakasz végén törlődik), illetve folyamatosan (tartalék /elem/ áramforrással biztosított, beavatkozás ellen védett memóriában) lehet tárolni a kriptográfiai modulban.
Az adapter azt is támogatja, hogy belül letárolt kulcsból osztott kulcs összetevőket generáljon, s ezeket intelligens kártyára küldje, illetve intelligens kártyákon tárolt osztott kulcs összetevőkből helyreállítsa a modulon belüli az eredeti kulcsot.
Az adapter valamennyi kulcsát le lehet nullázni (törölni). A Token felhasználók és a Token kriptográfiai tisztviselők a felügyeletük alatt álló kulcsokat nullázhatják le, míg az Adminisztrátor a modul valamennyi kulcsát nullázhatja.

2.7 Ön-tesztek

A CSA8000 összetevői helyes működésének ellenőrzése céljából ön-tesztek sorát képes megvalósítani a modul áram alá helyezési szakaszában (bekapcsoláskor), illetve működés közben, időszakosan.
Az áram alá helyezési tesztek magukba foglalják a következőket:

- "ismert eredmény teszt"[10]ek a modul által támogatott valamennyi kriptográfiai algoritmusra,
- szoftver (förmver) integritás teszt (32 bites hiba detektáló kódot és SHA-1 lenyomatoló függvényt használva),
- statisztikus véletlenszám generátor tesztek,
- egyéb kritikus funkciók tesztjei (köztük minden funkcionális modulra ellenőrző összeg számítás, valamint a RAM-ra, biztonságos memóriára, belső órára és a soros kommunikációs eszközökre elvégzett hardver ellenőrzések),

A működés közbeni időszakos vagy feltételes tesztek között pedig az alábbi tesztek valósulnak meg:

- szoftver betöltési teszt (RSA aláírást használva),
- folyamatos véletlenszám generátor teszt,
- páronkénti konzisztencia teszt (RSA és DSA kulcspár generálásakor),
- hibák monitorozása (a kriptográfiai hardver használata esetén mindig).

[10] Ilyenkor az algoritmust olyan adatokon hajtják végre, melyekre a helyes output már előzetesen ismert. A teszt akkor sikeres, ha az aktuálisan kiszámított output megegyezik a korábban generált outputtal.

3. A FIPS-140-1 tanúsítvány eredményeinek összefoglalása

A CSA8000 Adaptert egy kriptográfiai modulok tesztelésére az Egyesült Államokban és Kanadában akkreditált laboratórium[11] megvizsgálta, értékelte és tesztelte az alábbi követelményrendszernek való megfelelőség szempontjából:

> *a FIPS 140-1-ből (Kriptográfiai modulokra vonatkozó biztonsági követelmények) származtatott teszt követelmények*
> */Derived Test Requirements for FIPS 140-1, Security Requirements for Cryptographic Modules/*

A (FIPS) értékelés eredményei az alábbiak voltak:

A kriptográfiai modul tervezése és dokumentálása:	3-as szint
Modul interfészek:	3-as szint
Szerepkörök és szolgáltatások:	3-as szint
Véges állapotú automata modell:	3-as szint
Fizikai biztonság /több chip-es, beágyazott/:	3-as szint
Szoftver biztonság:	3-as szint
Az operációs rendszer biztonsága:	nincs értékelve[12]
Kriptográfiai kulcsgondozás:	3-as szint
Elektromágneses interferencia és kompatibilitás:	3-as szint
Ön-tesztek:	3-as szint

Az értékelés az alábbi digitális aláíráshoz kapcsolódó, FIPS által jóváhagyott algoritmusok megvalósítását vizsgálta, tesztelte: **DSA, RSA (PKCS #1), SHA-1**

Az értékelés az alábbi titkosításhoz kapcsolódó[13], FIPS által jóváhagyott algoritmusok megvalósítását vizsgálta, tesztelte: **DES, Triple-DES**

Az elért általános biztonsági szint: 3-as

[11] a CygnaCom Solutions Laboratory /NVLAP LAB CODE 200002-0/
[12] Minthogy a nevezett IT terméknek nincs saját operációs rendszere
[13] jelen Tanúsítási jelentés hatókörén kívül álló,

4. A CSA8000 által kielégített funkcionális biztonsági követelmények

Az alábbiakban áttekintjük azokat a (FIPS 140-1 követelményrendszer 3-as szintjéből fakadó) biztonsági követelményeket, melyeknek való megfelelőséget a CSA8000 értékelését végző laboratórium vizsgálta és igazolta.
Az alábbi jelölést alkalmazzuk:

KÖV_x.y: a FIPS 140-1 x. fejezetének y. biztonsági követelménye.[14]

4.1. A kriptográfiai modul tervezése és dokumentálása

KÖV_01.01:
A dokumentációnak teljes mértékben meg kell határoznia a kriptográfiai modul minden hardver, szoftver és förmver komponensét.

KÖV_01.02:
A dokumentációnak teljes mértékben meg kell határoznia a modulnak a kriptográfiai határát, amely a komponenseket körülzárja.

KÖV_01.03:
Ha a kriptográfiai modul szoftvert vagy förmvert tartalmaz, a kriptográfiai határt úgy kell definiálni, hogy az tartalmazzon minden olyan processzort, amely végrehajtja a szóban forgó kódot.

KÖV_01.04:
A dokumentációnak teljes mértékben ismertetnie kell a modul fizikai konfigurációját.

KÖV_01.05:
A dokumentációnak tartalmaznia kell egy blokkdiagramot, amely leírja a modul minden fontos hardver komponensét és azok csatlakozásait.

KÖV_01.06:
A dokumentációnak meg kell említenie a modul minden olyan hardver, szoftver vagy förmver komponensét, amely nem tartozik a szabvány biztonsági követelményei alá, és bizonyítania kell, hogy ezek a részek nem befolyásolják a modul biztonságosságát.

KÖV_01.07:
A dokumentációnak teljes mértékben meg kell határoznia a kriptográfiai modul biztonsági politikáját, vagyis mindazokat a biztonsági szabályokat, amelyek alatt a modulnak üzemelnie kell. Különösen fontos az, hogy a biztonsági politikának tartalmaznia kell azokat a biztonsági szabályokat, amelyek ezen szabvány[15] biztonsági követelményeiből illetve a gyártó által előírt járulékos biztonsági követelményekből származnak.

[14] Csak azokat a követelményeket adjuk meg, mely a CSA8000 kriptográfiai modulra ténylegesen vonatkoznak, ezért a követelmények sorszámozása nem mindig folyamatos.
[15] FIPS 140-1

4.2 Modul interfészek

KÖV_02.01:
A modult úgy kell megszerkeszteni, hogy a modulhoz tartozó minden információ áramlás és minden fizikai hozzáférés olyan logikai interfészekre legyen korlátozva, amelyek valamennyi, a modulba való belépési- illetve a modulból való kilépési pontot meghatároznak. A modul interfészeknek egymástól logikailag el kell különülniük.

KÖV_02.02:
A modulnak legalább a következő négy logikai interfészt tartalmaznia kell:

- adat input interfész,
- adat output interfész,
- vezérlési input interfész,
- státusz output interfész.

KÖV_02.03:
A modul tartalmazhatja a következő logikai interfészeket is:

- elektromos áram interfész,
- karbantartói hozzáférési interfész[16].

KÖV_02.04:
Az adat output interfészen keresztül történő minden adat outputot le kell tiltani hiba állapot vagy az ön-tesztek végrehajtása során.

KÖV_02.09:
A dokumentációnak a modul minden logikai interfészét ismertető, teljes specifikációt kell tartalmaznia.

KÖV_02.10:
A dokumentációnak expliciten definiálnia és specifikálnia kell minden fizikai és logikai input és output adat útvonalat a modulon belül.

KÖV_02.11:
Két független, belső tevékenység szükséges az olyan adat output interfészen keresztül megvalósuló outputhoz, amely kiadhat nyíltan megjelenő kriptográfiai kulcsokat és egyéb kritikus biztonsági paramétereket.

KÖV_02.12:
Az output adat útvonalnak logikailag el kell különülnie azoktól az áramköri elemektől és eljárásoktól, amelyek kulcs generálást, kézi kulcs bevitelt vagy kulcs törlést (lenullázást) hajtanak végre.

KÖV_02.13:
A nyíltan megjelenő kriptográfiai adatokhoz, nyíltan megjelenő hitelesítési adatokhoz és más, nem védett kritikus biztonsági paraméterekhez alkalmazott adat input és output portoknak fizikailag el kell különülniük a modul összes többi portjától.

[16] A CSA8000 nem tartalmaz karbantartói hozzáférési interfészt, így az erre vonatkozó követelményeket (KÖV_02.05 - KÖV_02.08, KÖV_03.03. - KÖV_03.05.) nem tartalmazza ez a fejezet.

KÖV_02.14:
A nyíltan megjelenő kriptográfiai adatokhoz, nyíltan megjelenő hitelesítési adatokhoz és más nem védett kritikus biztonsági paraméterekhez alkalmazott adat input és output portoknak lehetőséget kell biztosítani ezen adatok közvetlen bevitelére.

4.3 Szerepkörök és szolgáltatások

4.3.1 Szerepkörök

KÖV_03.01:
A dokumentációnak teljes specifikációt kell nyújtania mindazokról a jogosult szerepkörökről, amelyeket a modul támogat.

KÖV_03.02:
A kriptográfiai modulnak minimálisan a következő jogosult szerepköröket kell támogatnia:

- Felhasználói szerepkör: a szerepkört egy olyan felhasználó tölti be, aki fel van jogosítva biztonsági szolgáltatások elérésére, kriptográfiai műveletek és egyéb jogosult funkciók végrehajtására,
- Kriptográfiai tisztviselő szerepkör: a szerepkört egy olyan kriptográfiai tisztviselő tölti be, aki fel van jogosítva az összes kriptográfiai inicializálás és menedzsment funkció végrehajtására (pl. kriptográfiai kulcsok és paraméterek beírása, kriptográfiai kulcsok katalogizálása, naplózási funkciók és alarm nullázások).

KÖV_03.06[17].
Ha a modul több egyidejű operátort támogat[18], akkor a modulnak belsőleg le kell kezelnie az egyes operátorok által végrehajtott jogosult szerepkörök és szolgáltatások szétválasztását.

4.3.2 Szolgáltatások

KÖV03.07.
A dokumentációnak teljes specifikációt kell nyújtania minden olyan jogosult szolgáltatásról, műveletről és funkcióról, amelyet a modul segítségével végre lehet hajtani. Minden szolgáltatás esetén specifikálni kell a szolgáltatás inputokat, a megfelelő szolgáltatás outputokat és azt a jogosult szerepkört illetve szerepköröket, amelyben a szóban forgó szolgáltatás végrehajtható.

[17] Mivel a CSA8000 nem tartalmaz karbantartói hozzáférési interfészt, így az erre vonatkozó követelményeket (KÖV_02.05 - KÖV_02.08, KÖV_03.03. - KÖV_03.05.) nem tartalmazza ez a fejezet.
[18] A CSA8000 támogat több egyidejű operátort.

KÖV_03.08.
A kriptográfiai modulnak minimálisan a következő szolgáltatásokat kell nyújtania:

- státusz kijelzés: a modul aktuális státuszának outputja,
- ön-teszt: az ön-teszt inicializálása és futtatása a 11. fejezetben (Ön-tesztek) specifikáltaknak megfelelően.

KÖV_03.09.
A kriptográfiai modul opcionálisan a következő szolgáltatást is nyújthatja:

- Megkerülés: egy olyan megkerülési lehetőség aktiválása vagy lebénítása, amely kriptográfiai feldolgozás nélküli szolgáltatást (pl. nyílt szöveg továbbítást a modul segítségével) is lehetővé tesz[19].

KÖV_03.11.
Minden szolgáltatás inputnak egy szolgáltatás outputot kell eredményeznie.

4.3.3 Operátori hitelesítés

KÖV_03.12:
A hozzáférés ellenőrző mechanizmusok megvalósításához szükséges hozzáférés ellenőrző információk inicializálására használt szolgáltatások esetében a modulhoz való hozzáférés szabályozására különböző módszerek használhatók, mint pl. ügyrendi ellenőrzés, vagy gyári alap (default) beállítású hitelesítési és jogosultsági információk.

KÖV_03.13:
Ha egy modult áram alá helyeznek miután előzőleg az áramellátás megszűnt (pl. villamos hálózati hiba következtében) vagy karbantartás, illetve javítás után, a megelőző hitelesítés eredményeit nem szabad megőrizni, azaz a modulnak újra hitelesítenie kell az operátor jogosultságát ahhoz, hogy a megkívánt szerepkört betölthesse.

KÖV_03.16:
Azonosságon alapuló hitelesítés[20] esetén a kriptográfiai modulnak hitelesítenie kell az operátor azonosságát, és ellenőriznie kell, hogy az azonosított operátor jogosult-e egy vagy több meghatározott szerepkör betöltésére. A modulnak a következő tevékenységeket kell végrehajtania:

- meg kell követelnie, hogy az operátor egyedileg azonosított legyen,
- hitelesítenie kell az operátor megadott azonosságát,
- meg kell követelnie, hogy az operátor közvetett vagy közvetlen módon kiválasszon egy vagy több szerepkört,
- A hitelesített azonosság alapján ellenőriznie kell, hogy az operátor jogosult betölteni a kiválasztott szerepkört, valamint jogosult végrehajtani az annak megfelelő szolgáltatásokat.

[19] A CSA8000 nem biztosítja a megkerülés lehetőségét, így az erre vonatkozó követelményt (KÖV_03.10.) sem tartalmazza ez a fejezet.
[20] Ellentétben a szerepkörön alapuló hitelesítéssel, mely az 1-es és 2-es biztonsági szinten még elegendő (s, melyre az itt nem részletezett KÖV_03.14, KÖV_03.15 követelmények vonatkoznak).

KÖV_03.17:
Az azonosságon alapuló hitelesítés esetén a modul engedélyezheti, hogy egy operátor szerepkört váltson anélkül, hogy szükséges lenne az operátor azonosságának újbóli hitelesítése, de a modulnak ellenőriznie kell, hogy a hitelesített operátor jogosult-e az új szerepkör végrehajtására.

KÖV_03.20[21]:
A kriptográfiai modulnak azonosságon alapuló hitelesítési mechanizmusokat (pl. az operátor azonosításán alapuló mechanizmust) kell alkalmazni abból a célból, hogy az operátor jogosultságát ellenőrizze arra vonatkozóan, hogy a kívánt szerepköröket betölthesse és az annak megfelelő szolgáltatásokat igényelhesse. Ezeken túlmenően, nyílt formában megjelenő hitelesítési adatokat (pl. jelszavakat és PIN kódokat), nyílt formában megjelenő kriptográfiai kulcs komponenseket és más, nem védett kritikus biztonsági paramétereket olyan porton vagy portokon keresztül kell beadni, amelyek fizikailag el vannak különítve a többi porttól, és amelyek lehetővé teszik a direkt megadást /ahogyan azt a 2. fejezet (Modul interfészek) előírja/. Ide vonatkozó követelmények találhatók az KÖV_02.13 és KÖV_02.14-ben is.

[21] Ez a követelmény csak a 3-as és a 4-es biztonsági szintre vonatkozik. Ez a fejezet nem tartalmazza a csak az 1-es szintre vonatkozó KÖV_03.18-t, illetve a csak a 2-es szintre vonatkozó KÖV_03.19-t,

4.4. Véges állapotú automata modell

KÖV_04.01:
Minden kriptográfiai modult egy olyan véges állapotú automata modell felhasználásával kell megtervezni, amely világosan meghatározza a modul minden üzemelés közbeni és hiba állapotát.

KÖV_04.02:
A dokumentációnak meg kell adnia és ismertetnie kell a modul minden állapotát, valamint le kell írnia a megfelelő állapot átmenetek mindegyikét.

KÖV_04.03:
Az állapot átmenetek leírásának tartalmaznia kell azokat a belső modul feltételeket, adat inputokat és vezérlő inputokat, amelyek egy állapotból egy másikba való átmenetet okoznak, és tartalmaznia kell azokat a belső modul feltételeket, adat outputokat és státusz outputokat, amelyeket egy állapotból egy másikba való átmenet eredményez.

KÖV_04.04:
A dokumentációnak megfelelő részletességű véges állapot diagrammokat is kell tartalmaznia annak biztosítására, hogy ellenőrizni lehessen ezen követelményrendszernek való megfelelést.

KÖV_04.05:
Egy kriptográfiai modult a következő állapot típusok alkalmazásával kell tervezni:

- Áram bekapcsolási-kikapcsolási állapot: primer, szekunder és tartalék áramellátási állapotok. Ezek az állapotoknak különbséget tehetnek a modul különböző részeinek ellátására szolgáló áramellátások között,
- Kriptográfiai tisztviselő állapotok: olyan állapotok, amelyekben a kriptográfiai tisztviselő funkciók kerülnek végrehajtásra (pl. kriptográfiai inicializálás és kulcs menedzsment funkciók),
- Kulcs beírási állapotok: olyan állapotok, amelyek kriptográfiai kulcsoknak és más kritikus biztonsági paramétereknek a modulba való beírási, és azok érvényességének ellenőrzésére szolgálnak,
- Felhasználói szolgáltatói állapotok: olyan állapotok, amelyekben az arra feljogosított felhasználók biztonsági szolgáltatásokhoz juthatnak, kriptográfiai funkciókat vagy más jogosult felhasználói funkciót hajthatnak végre,
- Ön-tesz állapotok: olyan állapotok, amelyek a modul ön-tesztjének végrehajtására szolgálnak /lásd 11. fejezet (Ön-teszt)/,
- Hiba állapotok: olyan állapotok, amelyekbe a modul hiba fellépésekor kerül (pl. sikertelen ön-teszt, titkosítás megkísérlése olyan esetben, amikor működéshez szükséges kulcsok vagy más kritikus biztonsági paraméterek hiányoznak, vagy kriptográfiai hibák lépnek fel). A hiba állapotok felölelhetnek működést kizáró (hard) hibákat, amelyek egy készülék hibáját jelzik és a modul karbantartását vagy javítását igénylik, és felölelhetnek helyreállítható (soft) hibákat, amelyek a modul inicializálását vagy “reset”-elését igényelhetik.

KÖV_04.06:
Egy kriptográfiai modul egyéb állapot típusokat is tartalmazhat, beleértve a következőket:

- Nem-inicializált állapotok: olyan állapotok, amelyekben nincsenek a modulba betöltve a működéshez szükséges biztonsági paraméterek,
- Üresjárati állapotok: olyan állapotok, amelyekben a modul elvileg működőképes, de éppen nem nyújt biztonsági szolgáltatásokat, illetve nem hajt végre kriptográfiai funkciókat. A kriptográfiai kulcsok és biztonsági paraméterek be vannak töltve, és a modul adatra vagy vezérlő inputra vár.
- Biztonsági zár állapotok: olyan állapotok, amelyekben a modul az adott pillanatban nem működőképes, bár a kriptográfiai kulcsok és paraméterek be vannak töltve. Ezen állapotok arra szolgálnak, hogy védelmet nyújtsanak a modul számára a jogosulatlan felhasználással szemben az operátor ideiglenes távolléte esetén.
- Megkerülési állapotok: olyan állapotok, amelyek kriptográfiai műveletek nélküli szolgáltatásokat tesznek lehetővé (pl. nyílt szövegek továbbítását a modulon keresztül),
- Karbantartási állapotok: olyan állapotok, amelyek a modul karbantartására és szervizelésre szolgálnak, beleértve a karbantartási tesztek végrehajtását.[22]

KÖV_04.07:
Bármilyen hiba állapot esetén az adat output interfészen keresztül történő minden adat outputot le kell tiltani[23].

KÖV_04.08:
Minden hiba állapotnak olyannak kell lenni, hogy azt vissza lehessen állítani (reset) egy elfogadható működési állapotba vagy kezdeti állapotba, kivéve azokat a nem helyrehozható (hard) hibákat, amelyek a modul karbantartását, szervizelését vagy javítását igénylik.

KÖV_04.11:
A kriptográfiai modul minden állapotát megfelelő részletezettséggel, világosan meg kell határozni, annak biztosítására, hogy ellenőrizni lehessen a modulnak ezen követelményrendszernek való megfelelését.

[22] A CSA8000 kriptográfiai modulnak nincs se biztonsági zár, se karbantartási állapota, így ez a fejezet nem tartalmazza az ezekre vonatkozó KÖV_04.09 és KÖV_04.10 követelményeket.
[23] Ez a követelmény hasonló a 2. fejezet (Modul interfészek) KÖV_02.04 követelményéhez.

4.5. Fizikai biztonság

4.5.1 Közös követelmények[24]

KÖV_05.01:
A dokumentációnak tartalmaznia kell a fizikai megvalósítás teljes specifikációját, valamint azoknak az alkalmazható biztonsági mechanizmusoknak a teljes leírását, amelyeket a modul alkalmazhat.

4.5.2 Több chip-es, beágyazott kriptográfiai modulra vonatkozó követelmények

KÖV_05.07[25]:
Több chip-es, beágyazott kriptográfiai modul esetén a modulban lévő chip-eknek olyan termék minőségűeknek kell lenniük, amelyek magukban foglalnak standard passziválási technikát is.

KÖV_05.08:
Több chip-es, beágyazott kriptográfiai modul esetén a modult termék szintű több chip-es formában kell megvalósítani.

KÖV_05.09:
Több chip-es, beágyazott kriptográfiai modul esetében a modult egy nem átlátszó, beavatkozást kimutató anyaggal kell beburkolni.

KÖV_05.10:
Több chip-es, beágyazott kriptográfiai modul esetében a következő három követelmény egyikét kell alkalmazni a modulra:

- egy kemény, nem átlátszó kiöntő anyagot kell alkalmazni,
- a modult egy erős, nem eltávolítható burkoló anyagnak kell tartalmaznia,
- a modult egy erős, eltávolítható burkolatba kell bezárni, és tartalmaznia kell beavatkozásra reagáló és nullázó áramköri egységet.

KÖV_05.11[26]:
Több chip-es, beágyazott kriptográfiai modul esetében, ha a modul valamilyen szellőzőnyílást tartalmaz, azt olyan módon kell megtervezni, hogy az meggátoljon minden észrevétlen szondázást.

[24] Vagyis a kriptográfiai modul mindhárom lehetséges fizikai konfigurációjára (egy chip-ből álló, több chip-es , beágyazott, illetve több chip-es , önmagában álló) vonatkozik.
[25] Ez a fejezet nem tartalmazza a csak az egy chip-ből álló kriptográfiai modulokra vonatkozó KÖV_05.02 - KÖV_05.06 követelményeket.
[26] Ez a fejezet nem tartalmazza a csak a 4-es biztonsági szintre vonatkozó KÖV_05.12 - KÖV_05.14 követelményeket, valamint a csak a több chip-es , önmagában álló kriptográfiai modulokra vonatkozó KÖV_05.15 - KÖV_05.24 követelményeket.

4.6. Szoftver biztonság

KÖV_06.01:
A dokumentációnak meg kell határoznia minden olyan szoftvert és förmvert, amely nem áll jelen szoftver biztonsági követelmények hatálya alatt, s ezt a kizárást elfogadható módon meg kell magyarázni.

KÖV_06.02:
A dokumentációnak tartalmaznia kell a modulon belüli szoftver szerkezetének részletes leírását /pl. véges állapotú automaták specifikációját, amelyet a 4. fejezet (Véges állapotú automata modell) követel meg/.

KÖV_06.03:
A dokumentációnak részletes magyarázatot kell tartalmaznia a szoftver szerkezete és a kriptográfiai modul biztonsági politikája közötti megfelelésre vonatkozóan.

KÖV_06.04:
A dokumentációnak tartalmaznia kell a modul által tartalmazott minden szoftver teljes forrás-kód listáját.

KÖV_06.05:
Minden szoftver modul, szoftver funkció és szoftver eljárás esetén a forrás kód listákat magyarázatokkal kell ellátni, amelyek világosan leírják ezen szoftver egységeknek a szoftver szerkezetével való kapcsolatát.

KÖV_06.06:
A kriptográfiai modulon belüli minden szoftvert egy magas szintű programnyelv alkalmazásával kell megvalósítani, kivéve azt az esetet, amikor egy alacsony szintű nyelv (pl. assembly nyelvek) korlátozott alkalmazása alapvetően fontos a modul hatékonyságához, vagy ha magas szintű nyelv nem áll rendelkezésre[27].

4.7 Az operációs rendszer biztonsága

Nincsenek követelmények[28].

[27] Ez a fejezet nem tartalmazza a csak a 4-es biztonsági szintre vonatkozó KÖV_06.07 - KÖV_06.10 követelményeket.
[28] Mivel a CSA8000 kriptográfiai modulnak nincs saját operációs rendszere.

4.8 Kriptográfiai kulcsgondozás

4.8.1 Általános követelmények

KÖV_08.01:
Dokumentációnak kell specifikálnia a kriptográfiai modulra vonatkozó kulcsgondozás minden vonatkozását.

KÖV_08.02:
A titkos és magán kulcsokat védeni kell a jogosulatlan felfedéssel, módosítással és helyettesítéssel szemben.

KÖV_08.03:
A nyilvános kulcsokat védeni kell a jogosulatlan módosítással és kicseréléssel szemben.

4.8.2 Kulcs generálásra vonatkozó követelmények

KÖV_08.04:
Egy kriptográfiai modul opcionálisan ki lehet egészítve egy belső kulcs generálási funkcióval[29]. A modulnak egy FIPS által jóváhagyott kulcs generálási algoritmust kell implementálni. A dokumentációnak specifikálnia kell a FIPS által jóváhagyott kulcs generálási algoritmust, amelyet a modul végrehajt.

KÖV_08.05:
Ha a kulcs generálási folyamatban egy véletlenszám generátor is alkalmazva van[30], minden értéket olyan módon kell véletlenszerűen vagy pszeudo-véletlenszerűen generálni, hogy a bitek minden lehetséges kombinációja és minden lehetséges érték egyenlő valószínűséggel generálódjon.

KÖV_08.06:
Ha egy kezdeti *(seed)* kulcs alkalmazva van[31], akkor azt ugyanolyan módon kell bevinni, mint a kriptográfiai kulcsokat.

KÖV_08.07:
Közbenső kulcs generálási állapotoknak és értékeknek nem szabad hozzáférhetőnek lenniük a modulon kívül nyílt vagy más nem védett formában.

4.8.3 Kulcs szétosztásra vonatkozó követelmények

KÖV_08.08:
Kulcs szétosztás végrehajtható kézi módszerekkel, automatizált módszerekkel vagy kézi és automatizált módszerek kombinációjával. Egy kriptográfiai modulnak FIPS által jóváhagyott kulcs szétosztási technikát kell implementálnia. Amíg nincs FIPS által jóváhagyott kulcs szétosztási technika bevezetve, kereskedelmi forgalomban beszerezhető nyilvános kulcs módszerek is alkalmazhatók. A dokumentációnak specifikálnia kell a modul által alkalmazott kulcs szétosztási technikát.

[29] A CSA8000 megvalósít belső kulcs generálási funkciót.
[30] A CSA8000 alkalmaz véletlenszám generátort.
[31] A CSA8000 véletlenszám generátora alkalmaz kezdeti *(seed)* kulcsot.

4.8.4 Kulcs bevitelére és kivitelére vonatkozó követelmények

KÖV_08.09:
Kézi úton szétosztott kriptográfiai kulcsok bevihetők a kriptográfiai modulba, illetve outputként kinyerhetők abból, tisztán kézi módszerekkel vagy elektronikus módszerekkel.

KÖV_08.10:
Az elektronikus úton szétosztott titkos és magán kulcsokat kódolt formában kell bevinni és kinyerni.

KÖV_08.11:
A kézi úton szétosztott kriptográfiai kulcsokat a kriptográfiai modulba való bevitel során ellenőrizni kell a helyesség szempontjából a 11 fejezetben (Ön-tesztek) meghatározott kézi kulcs beviteli teszt felhasználásával.

KÖV_08.12:
A kulcs bevitele során a kulcsokat és kulcs komponenseket átmenetileg ki lehet jelezni a vizuális ellenőrizhetőség és a pontosság javítása érdekében. Ha kódolt kulcsok vagy kulcs komponensek kerülnek beírásra, az ebből származó nyílt formájú titkos vagy magán kulcsok nem jeleníthetők meg.

KÖV_08.13:
Eszközt kell szolgáltatni annak biztosítására, hogy a modulba bevitt vagy abból outputként kinyert kulcs azzal a megfelelő jogi személlyel legyen összekapcsolva (pl. személy, csoport vagy eljárás), akihez a kulcs hozzá van rendelve.

KÖV_08.15[32]:
A kézi úton szétosztott titkos vagy magán kulcsokat nem szabad bevinni vagy outputként kinyerni a kriptográfiai modulból nyílt formában. Ha kézi úton szétosztott titkos vagy magán kulcsokat kell bevinni a kriptográfiai modulba vagy outputként kinyerni onnan, akkor ezeket a következő módszerek valamelyikével kell elvégezni:

- kódolt formában,
- osztott tudáson alapuló (azaz két vagy több nyílt formájú kulcs komponenst felhasználó) eljárás alkalmazásával.

KÖV_08.16:
Ha kézi úton szétosztott titkos vagy magán kulcsot osztott tudáson alapuló eljárás segítségével visznek be vagy nyernek ki, a modulnak lehetőséget kell nyújtania arra, hogy az operátort külön-külön hitelesítse minden egyes kulcs komponens esetében. Ezen túlmenően, a kulcs komponenseket közvetlenül a kriptográfiai modulba kell bevinni, illetve közvetlenül a kriptográfiai modulból kell kinyerni (pl. megbízható útvonalon vagy közvetlenül csatlakoztatott kábelen keresztül) anélkül, hogy az áthaladna valamilyen borításon vagy olyan közbenső rendszeren, ahol a komponensek tárolhatók, összekapcsolhatók vagy más módon feldolgozhatók. Idevonatkozó követelmény található a KÖV_02.14-ben is.

[32] Ez a követelmény csak a 3-as és a 4-es biztonsági szintre vonatkozik. Ez a fejezet nem tartalmazza ugyanakkor a csak az 1-es és 2-es szintre vonatkozó KÖV_08.14-t.

4.8.5 Kulcs tárolásra vonatkozó követelmények

KÖV_08.17:
Ha a titkos vagy magán kulcsokat a kriptográfiai modul tartalmazza, akkor azok tárolhatók nyílt formában. Ezek a nyílt formájú kulcsok a modulon kívülről nem lehetnek hozzáférhetők. Ez a követelmény kapcsolódik az KÖV_08.02-höz.

KÖV_08.18:
Eszközt kell szolgáltatni annak biztosítására, hogy minden kulcs azzal a megfelelő jogi személlyel lett összekapcsolva (pl. személy, csoport vagy eljárás), akihez a kulcs hozzá van rendelve.

4.8.6 Kulcs megsemmisítésre vonatkozó követelmények

KÖV_08.19:
Egy kriptográfiai modulnak lehetőséget kell arra nyújtani, hogy minden nyíltan tárolt kriptográfiai kulcsot és egyéb nem védett kritikus biztonsági paramétert a modulon belül nullázni lehessen. A kriptográfiai kulcsok és egyéb kritikus biztonsági paraméterek nullázása nem követelmény abban az esetben, ha a kulcsok és paraméterek kódolt formában vannak tárolva, vagy valamilyen más fizikai vagy logikai módon védve vannak (pl. egy járulékosan beépített, jelen követelményrendszernek megfelelő kriptográfiai modulon belül vannak elhelyezve).

4.8.7 Kulcs archiválásra vonatkozó követelmények

KÖV_08.20:
Egy kriptográfiai modul opcionálisan kiadhat kulcsokat archiválási célokból. Az archiválásra kiadott kulcsoknak kódoltnak kell lenniük.

4.9. Kriptográfiai algoritmusok

KÖV_09.01:
A kriptográfiai moduloknak FIPS által jóváhagyott algoritmusokat kell alkalmazniuk.

4.10 Elektromágneses interferencia, elektromágneses kompatibilitás

KÖV_10.01:
A kriptográfiai modulok jeladó részének (rádiónak) minden alkalmazható FCC követelménynek eleget kell tenniük.

KÖV_10.03[33]:
Egy kriptográfiai modulnak alkalmazkodnia kell az EMI/EMC követelményekhez, amelyek az FCC 15. részében, a J alfejezetben és a B osztályban (azaz a házi alkalmazásra vonatkozó részben) vannak megadva.

[33] Ez a követelmény csak a 3-as és a 4-es biztonsági szintre vonatkozik. Ez a fejezet nem tartalmazza ugyanakkor a csak az 1-es és 2-es szintre vonatkozó KÖV_10.02-t.

4.11 Ön-tesztek

4.11.1 Általános követelmények

KÖV_11.01:
Egy kriptográfiai modulnak képesnek kell lennie arra, hogy ön-teszteket hajtson végre a modul megfelelő működésének ellenőrzésére. Bizonyos ön-teszteket akkor kell végrehajtani, amikor a modul áram alá kerül (áram alá helyezéskor végrehajtandó tesztek), egyéb ön-teszteket pedig különböző feltételek esetén kell végrehajtani, általában akkor, ha egy meghatározott funkció vagy művelet kerül végrehajtásra (feltételhez kötött tesztek). A modul opcionálisan végrehajthat más ön-teszteket is, a jelen szabványban[34] meghatározottakon túlmenően.

KÖV_11.02:
Amennyiben a kriptográfiai modul valamelyik ön-tesztje sikertelen, a modulnak hiba állapotba kell kerülnie, és hiba jelet kell kiadnia a státusz interfészen keresztül.

KÖV_11.03:
A modul semmilyen kriptográfiai funkciót nem végezhet addig, amíg hiba állapotban van, és semmilyen adatot nem adhat ki outputként az adat output interfészen keresztül, amíg a hiba feltétel fennáll. Ide vonatkozó követelmények találhatók az KÖV_02.04-ben és KÖV_04.07-ben.

KÖV_11.04:
Minden lehetséges hiba feltételnek dokumentáltnak kell lenni mindazokkal a tevékenységekkel együtt, amelyek szükségesek a hiba törlésére és a normál működéshez való visszatéréshez (ez tartalmazhatja a modul karbantartását, szervizelését és javítását is).

4.11.2 Áram alá helyezési tesztek

4.11.2.1 Általános tesztek

KÖV_11.05:
Miután egy kriptográfiai modult áram alá helyeztek, a modulnak ön-teszt állapotba kell kerülnie, és legalább a következő (áram alá helyezési) teszteket végre kell hajtania:

- kriptográfiai algoritmus teszt,
- szoftver/förmver teszt,
- a kritikus műveletek tesztje és
- a statisztikus véletlenszám generátor tesztek.

A modul opcionálisan további teszteket is végrehajthat.

KÖV_11.06:
Az áram alá helyezés utáni ön-tesztek nem igényelhetnek operátori közreműködést a futtatáshoz.

[34] FIPS 140-1

KÖV_11.07:
Amennyiben minden áram alá helyezés utáni teszt sikeres, akkor egy jelzést kell kiadni a "státusz output" interfészen keresztül.

KÖV_11.08:
Minden adat outputot le kell tiltani, amíg ezek a tesztek végrehajtás alatt állnak. Ide vonatkozó követelmény még a KÖV_02.04.

KÖV_11.09:
A modulnak eszközöket kell biztosítania arra, hogy az áram alá helyezési teszteket igény esetén a modul periodikus tesztelésére is kezdeményezni lehessen.

4.11.2.2 Kriptográfiai algoritmus tesztek

KÖV_11.10:
A kriptográfiai algoritmusokat tesztelni kell oly módon, hogy az algoritmust olyan adatokon kell végrehajtani, amelyekre vonatkozóan a helyes output már ismert ("ismert eredmény teszt"). A teszt akkor sikeres, ha a kiszámított output megegyezik a korábban generált outputtal.

KÖV_11.11:
Az ismert eredmény tesztet minden egyes kriptográfiai funkcióra vonatkozóan (pl. kódolás, dekódolás, hitelesítés) végre kell hajtani[35].

4.11.2.3 Szoftver/förmver teszt

KÖV_11.14:
A modulban (például az EEPROM-ban vagy RAM-ban) található minden beágyazott szoftver és förmver esetén számításba kell venni és tárolni kell egy hiba detektáló kódot (EDC) vagy FIPS által jóváhagyott hitelesítési technikát (pl. egy adat hitelesítési kód kiszámítását és ellenőrzését vagy egy FIPS által elfogadott digitális aláírási algoritmust). Ezt a hiba detektáló kódot, adat hitelesítési kódot ill. digitális aláírást ellenőrizni kell akkor, amikor az áram alá helyezési ön-tesztek futnak.

4.11.2.4 Kritikus funkciók tesztjei

KÖV_11.15:
Minden más, a modul biztonságos működése szempontjából kritikus funkció tesztelhető azon ön-tesztek részeiként, amelyeket az áram alá helyezéskor kell végrehajtani. A dokumentációnak teljes specifikációt kell szolgáltatnia a kritikus funkciókról és azon áram alá helyezési ön-tesztek természetéről, amelyek ezen funkciók számára ki vannak jelölve. A meghatározott feltételek esetén végrehajtandó egyéb kritikus funkciókat a feltételhez kötött tesztek részeként kell végrehajtani.

[35] Mivel a CSA8000 nem implementál se tömörítő algoritmust, se kettős, párhuzamos algoritmus végrehajtást, ezért az ezekre vonatkozó KÖV_11.12 - KÖV_11.13-t nem tartalmazza ez a fejezet.

4.11.2.5 Statisztikus véletlenszám generátor tesztek

KÖV_11.16:
Azon kriptográfiai moduloknak, amelyek egy véletlenszám vagy pszeudó véletlenszám generátort implementálnak, tartalmazniuk kell a véletlenség vizsgálatára szolgáló statisztikai tesztek végrehajtásának lehetőségét. Jelen követelményrendszer az alábbi négy javasolt tesztet határozza meg:

- Monobit teszt
  1. *Számoljuk le az 1-es értékű biteket egy 20 000 hosszú bit sorozatban. Jelöljük az 1-es bitek számát X-szel.*
  2. *A teszt akkor sikeres, ha 9725 < X < 10 275 (0 .0001 I-es típusú hiba mellett).*
- Póker teszt
  1. *Osszunk fel egy 20 000 hosszú bit sorozatot 5 000 egymást követő bit 4-es részekre. Számoljuk meg és tároljuk le a bit 4-esek 16 lehetséges kombinációjába tartozó szegmenseket. Jelölje f(i) minden i értékre (i = 0,1,2, … 15) a megfelelő gyakoriságértéket.*
  2. *Számoljuk ki a következő értéket:*

$$X = (16 / 5000) * \left(\sum_{i=0}^{15} [f(i)]^2 \right) - 5000$$

  3. *A teszt akkor sikeres, ha 2.16 < X < 46.17 (0 .0001 I-es típusú hiba mellett).*
- Futam teszt
  1. *Egy futam a maximális hosszúságú, csupa 0 vagy csupa 1-es értékű, egymást követő bit részsorozat egy 20 000 hosszúságú bit mintasorozatban. Számoljuk össze és tároljuk a mintasorozat futam-hosszúságainak gyakoriságát minden futamhosszra (1,2,3,…) mind a 0-kból, mind az 1-esekből álló futamok esetén.*
  2. *A teszt akkor sikeres, ha mind a 12 alábbi érték (6 darab 1-esekből, 6 darab 0-okból álló futamokra számított érték) az alábbi táblázatban meghatározott intervallumon belül van. Ez a teszt a 6-nál hosszabb futamokat összevontan kezeli.*

Futam hossz	*Elvárt intervallum (0 .0001 I-es típusú hiba mellett)*
1	*2 315 – 2 685*
2	*1114 – 1386*
3	*527 – 723*
4	*240 – 384*
5	*103 – 209*
6+ (6 vagy hosszabb)	*103 – 209*

- Hosszú távú futam teszt
  1. ***Hosszú futamnak a 26 vagy nagyobb hosszúságú (akár 1-esekből, akár 0-kból álló) futamot nevezzük.***
  2. *Egy 20 000 hosszú bitsorozatra a teszt akkor sikeres, ha nincs hosszú futama. (0 .0001 I-es típusú hiba mellett).*

A fenti tesztek helyettesíthetők olyan alternatív tesztekkel, amelyek ezekkel megegyező vagy jobb ellenőrzést nyújtanak a véletlenségre. Ha a tesztek valamelyike sikertelen, a modulnak hiba állapotba kell kerülnie. Idevonatkozó követelmény a KÖV_11.02 is.

KÖV_11.17[36]:
A statisztikai teszteknek igény esetén meghívhatóknak kell lenniük. Idevonatkozó követelmény a KÖV_11.09 is.

[36] Ez csak a 3-as biztonsági szinten elvárt követelmény. A fejezet ugyanakkor nem tartalmazza a csak a 4-es biztonsági szinten elvárt KÖV_11.18-at.

4.11.3 Feltételhez kötött tesztek

4.11.3.1 Páronkénti konzisztencia teszt

KÖV_11.19:
Azon kriptográfiai modulok, amelyek nyilvános és magán kulcsokat generálnak, tesztelniük kell a kulcsokat a páronkénti konzisztencia szempontjából. Ha a kulcsokat csak digitális aláírás létrehozására és ellenőrzésére használják, akkor a kulcsok konzisztenciája tesztelhető egy aláírás létrehozásával és ellenőrzésével is.

4.11.3.2 Szoftver/förmver betöltési tesztek

KÖV_11.20:
Minden olyan érvényesített szoftver és förmver esetében, amelyet kívülről lehet betölteni a kriptográfiai modulba, alkalmazni kell egy olyan kriptográfiai mechanizmust, amely FIPS által jóváhagyott hitelesítési technikát (pl. adat hitelesítési kód vagy FIPS által elfogadott digitális aláírási algoritmus) használ. Ezen tesztnek kell ellenőrizni az adat hitelesítési kódot, illetve digitális aláírást minden olyan esetben, amikor szoftver vagy förmver kerül kívülről betöltésre a modulba[37].

4.11.3.3 Kézi kulcs bevitel tesztje

KÖV_11.21:
Amennyiben egy kriptográfiai modulba kézi úton visznek be kriptográfiai kulcsokat vagy kulcs elemeket, a kulcsoknak rendelkezniük kell egy hiba detektáló kóddal (pl. paritás ellenőrzési érték), vagy pedig kétszeres beírást kell alkalmazni a beírt kulcsok helyességének ellenőrzésére. A kriptográfiai modulnak ellenőriznie kell a hiba detektáló kódot vagy duplikált beírást, és jelzést kell adnia a beírási eljárás sikerességéről vagy sikertelenségéről[38].

4.11.3.4 Folyamatos véletlenszám generátor teszt

KÖV_11.22:
Azon kriptográfiai moduloknak, amelyek egy véletlenszám vagy pszeudó véletlenszám generátort implementálnak, tesztelniük kell a generátort a sikertelenség szempontjából egy konstans értékig. Ha a generátor n bitből álló blokkokat generál, ahol n>15, a bekapcsolás után generált első blokkot nem szabad felhasználni, de tárolni kell abból a célból, hogy összehasonlításra kerüljön a következő generálandó blokkal. Az egymást követő generálások során az újonnan generált blokk összehasonlításra kerül az előző generált blokkal. A teszt sikertelen, ha a két összehasonlított blokk azonos. Ha a generátornak minden hívása 16 bitnél kevesebbet szolgáltat, akkor a bekapcsolás utáni első n bitet, valamilyen n>15-re, nem szabad felhasználni, de tárolni kell a következő n generált bittel való összehasonlításra. Minden egymást követő n-bit generálás összehasonlításra kerül a megelőzően generált n-bittel. A teszt sikertelen, ha két összehasonlított n-bites sorozat megegyezik.

[37] A CSA8000 adapterbe lehetséges kívülről szoftvert betölteni (upgrade céljából). Ilyenkor csak az Eracom gyártó cég (RSA algoritmussal) digitálisan aláírt szoftverét fogadja el a modul.
[38] A CSA8000 egy speciális kulcs ellenőrző kódot (Key Verification Code) alkalmaz hiba detektálásra.

5. A CSA8000 által kielégített garanciális biztonsági követelmények

Az alábbiakban áttekintjük azokat a fejlesztői bizonyítékokat (dokumentálást, egyéb információ szolgáltatást), melyeket a fejlesztő cég biztosított a CSA8000 értékelését végző laboratórium számára, s melyek megalapozzák az értékelés garanciális szintjét.

Az alábbi jelölést alkalmazzuk:

FB_x.y.z: a FIPS 140-1 x. fejezetének y. biztonsági követelményére vonatkozó z. fejlesztői bizonyítékot meghatározó elvárása.

5.1. A kriptográfiai modul tervezése és dokumentálása

FB_01.01.01:
A fejlesztői dokumentációban meg kell határozni minden olyan komponenst, amely kriptográfiai logikai áramkört vagy eljárást alkalmaz. A felsorolandó komponenseknek tartalmazniuk kell értelemszerűen a következőket:

- integrált áramköröket, beleértve a processzorokat, memóriákat és fogyasztói rendelésre készített *(custom)* integrált áramköröket,
- egyéb aktív elektronikai áramköri elemeket,
- villamos áram bemeneteket és kimeneteket, belső áramellátásokat vagy konvertereket,
- fizikai struktúrákat, beleértve az áramköri kártyákat vagy más szerelési alapfelületeket, foglalatokat és csatlakozókat,
- a szoftver és förmver modulokat,
- a modulban alkalmazott egyéb komponenseket.

FB_01.01.02:
A fenti komponens listának konzisztensnek kell lennie azokkal az információkkal, amelyek az 1. fejezet (A kriptográfiai modul tervezése és dokumentálása) egyéb követelményeinek kielégítésére szolgálnak.

FB_01.02.01:
A fejlesztői dokumentációnak meg kell határoznia a modul kriptográfiai határát. A kriptográfiai határnak egy olyan világosan meghatározott, összefüggő védelmi peremkerületnek kell lennie, amely a kriptográfiai modul fizikai határát alakítja ki. A védelmi peremkerület definíciónak meg kell határoznia a modul komponenseket és csatlakozókat (portokat), valamint a modul információ áramlási folyamatait, feldolgozó és input/output jeleit**.**

FB_01.02.02:
A kriptográfiai határnak tartalmaznia kell minden olyan hardvert vagy szoftvert, amely inputként fogad, feldolgoz, vagy outputként kiad olyan fontos biztonsági paramétereket, amelyek ha nincsenek kellően ellenőrizve, akkor ez érzékeny információk veszélyeztetéséhez vezethet.

FB_01.03.01:
A modulban lévő valamennyi processzorra a fejlesztőnek meg kell határoznia azt a szoftvert és förmvert, amelyet az adott processzor hajt végre, és azokat a memória egységeket, amelyek a végrehajtható kódot és adatokat tartalmazzák, és meg kell jelölni a szoftverek és förmverek fő funkcióját is.

FB_01.03.02:
Minden processzor esetén a fejlesztőnek meg kell határoznia minden olyan hardvert, amelyhez a szóban forgó processzor kapcsolódik.

FB_01.04.01:
A fejlesztőnek meg kell határoznia, hogy a modul fizikai konfigurációja a három lehetséges eset közül melyik: egyetlen chip-ből álló modul, több chip-es, beágyazott modul vagy több chip-es önmagában álló modul.

FB_01.04.02:
A fejlesztői dokumentációnak vázolnia kell a modul belső elrendezését és összeszerelési módszereit (pl. rögzítők és szerelvények), beleértve a tervrajzokat is, amelyeknek méret-arányosaknak kell lenniük. Az integrált áramkörök belsejét nem kell ábrázolni.

FB_01.04.03:
A fejlesztői dokumentációnak ismertetnie kell a modul elsődleges fizikai paramétereit, beleértve a foglalatoknak, a hozzáférési pontoknak, az áramköri kártyáknak, az áramellátás elhelyezkedésének, az összekötő huzalok menetének, a hűtőberendezések elhelyezkedésének és más fontos paramétereknek a leírását.

FB_01.05.01:
A fejlesztői dokumentációnak tartalmaznia kell egy olyan funkcionális blokkdiagramot, amely bemutatja a hardver komponenseket és azok csatlakozásait. A blokkdiagramnak tartalmaznia kell értelemszerűen a következő komponenseket:

- mikroprocesszorok,
- input/output bufferek,
- nyíltan tárolt szöveg / kódoltan tárolt szöveg bufferek,
- ellenőrző bufferek,
- kulcs tárolás,
- munka memória,
- program memória,
- minden más, fontos felhasznált komponens.

FB_01.05.02:
A blokkdiagramnak ezeken felül tartalmaznia kell minden más fogyasztói rendelésre készített integrált áramköröket, mint pl. előre megtervezett kriptográfiai áramköröket, kapu áramköröket vagy egyéb programozható logikai áramköröket. Az ilyen komponenseken belüli független funkciókat elkülönítetten kell meghatározni a blokkdiagramban.

FB_01.05.03:
A blokkdiagramnak tartalmaznia kell a fő modul komponensek vagy részegységek funkcióit.

FB_01.05.04:
A blokkdiagramnak be kell mutatnia a modul fő komponensei közötti, valamint a modul és a külső berendezés közötti kapcsolatokat.

FB_01.05.05:
A blokkdiagramnak be kell mutatnia a modul kriptográfiai határát.

FB_01.06.01:
Minden olyan komponenst, amely nem tartozik a biztonsági követelmények alá, tételesen fel kell sorolni a fejlesztői dokumentációban.

FB_01.06.02:
A FB_01.06.01 követelmény kielégítésére készített lista valamennyi elemére vonatkozóan a kizárás okát elfogadható módon meg kell magyarázni a fejlesztői dokumentációban. A fejlesztőnek bizonyítania kell, hogy ezen komponensek egyike sem okozhat veszélyeztetést elfogadható körülmények között, még hibás működés vagy rosszindulatú használat esetén sem.

FB_01.07.01:
A fejlesztőnek gondoskodnia kell egy különálló dokumentumról vagy dokumentum fejezetről, amely meghatározza azt a biztonsági politikát (vagyis azokat a biztonsági szabályokat, amelyek mellett egy modulnak működnie kell), amelyet a kriptográfiai modul léptet hatályba.

5.2 Modul interfészek

FB_02.01.01:
A fejlesztői dokumentációnak részleteznie kell a modul információ folyamait és hozzáférési pontjait azáltal, hogy az 1. fejezetben (A kriptográfiai modul tervezése és dokumentálása) megkövetelt blokkdiagram másolatait kiemelésekkel és jegyzetekkel látja el. Ezeken felül további dokumentációt is kell szolgáltatni, amely szükséges a logikai interfészek világos specifikálásához. A modulhoz csatlakozó minden input és output esetében a dokumentációnak meg kell határoznia azt a logikai interfészt, amelyhez az adott input vagy output tartozik, és meg kell határoznia a megfelelő fizikai belépési/kilépési pontokat. Az ezen követelmény kielégítésére szolgáltatott információknak konzisztenseknek kell lenniük azokkal a komponens információkkal, amelyek az 1. fejezet (A kriptográfiai modul tervezése és dokumentálása) KÖV_01.01, KÖV_01.02 és KÖV_01.05 követelményei kielégítésére készültek.

FB_02.01.02:
A fejlesztői tervnek a modul interfészeket logikailag elkülönített kategóriákra kell szétválasztani minimálisan azon kategóriák alkalmazásával, amelyek a KÖV_02.02 és a KÖV_02.03 követelményekben definiálva vannak. Amennyiben két vagy több interfész ugyanazon a fizikai porton osztozik, a fejlesztőnek meg kell határoznia, hogy a különböző interfész kategóriákból származó információk hogyan különíthetők el logikailag.

FB_02.02.01:
A modulnak rendelkeznie kell egy adat input interfésszel, amely definiálva van a fejlesztői dokumentációban, beleértve az alábbiakat:

- nyíltan tárolt adatok,
- kódolt szövegként tárolt adatok,
- kriptográfiai kulcsok,
- egyéb kulcsgondozási adatok,
- hitelesítési adatok,
- státusz információk,
- minden más input adat.

FB_02.02.02:
A modulnak rendelkeznie kell egy adat output interfésszel, amely definiálva van a fejlesztői dokumentációban, beleértve az alábbiakat:

- nyíltan tárolt adatok,
- kódolt szövegként tárolt adatok,
- kriptográfiai kulcsok,
- egyéb kulcsgondozási adatok,
- hitelesítési adatok,
- vezérlési információk,
- minden más output adat.

FB_02.02.03:
A modulnak rendelkeznie kell egy vezérlési input interfészel, amely definiálva van a fejlesztői dokumentációban, és amelyet a modul működésének vezérlésére alkalmaznak, beleértve az input parancsokat, jelzéseket, adatokat és kézi inputokat.

FB_02.02.04:
A modulnak rendelkeznie kell egy státusz output interfésszel, amely definiálva van a fejlesztői dokumentációban, és amelyet a modul státuszának megjelenítésére vagy kijelzésére alkalmaznak, beleértve az output adatokat, jelzéseket, kijelzőket és fizikai kijelzőket.

FB_02.03.01:
Ha a modul felvesz vagy szolgáltat külső áramot[39], rendelkeznie kell egy elektromos áram interfésszel, amely a fejlesztői dokumentációban megfelelő módon definiálva van, és amely tartalmazza az elektromos áram valamennyi belépési vagy kilépési pontját.

FB_02.04.01:
A fejlesztői tervezetnek biztosítania kell, hogy az adat output interfészen keresztül történő minden adat output letiltásra kerüljön, amikor a modul hiba állapotba kerül, ahogyan azt a 4. fejezet (Véges állapotú automata modell) dokumentálja, és a fejlesztői dokumentációnak tartalmaznia kell, hogy ez hogyan valósul meg.

FB_02.04.02:
A fejlesztői tervezetnek biztosítania kell, hogy az adat output interfészen keresztül történő minden adat output letiltásra kerüljön, amikor a modul ön-teszt állapotba kerül, ahogyan azt a 11. fejezet (Ön-tesztek) dokumentálja, és a fejlesztői dokumentációnak tartalmaznia kell, hogy ez hogyan valósul meg.

FB_02.09.01:
A dokumentációnak tartalmaznia kell egy teljes specifikációt, amely a modul minden logikai interfészét ismerteti, beleértve minden egyes:

- fizikai és logikai portot és azok pin kiosztását,
- fizikai borítót, nyílászárót vagy nyílást,
- kézi vagy logikai vezérlést,
- fizikai vagy logikai státusz kijelzőt,
- fizikai, logikai vagy elektronikus karakterisztikát, ha ezek értelmezhetők a fenti interfészek esetében.

FB_02.10.01:
A fejlesztői dokumentációnak minden fizikai és logikai input és output adat útvonalat megfelelő részletességgel ismertetnie kell abból a célból, hogy a modul input-, feldolgozott- és output információinak minden fő kategóriája specifikálva legyen. Minden input adat, amely az adat input interfészen keresztül lép a modulba, csak az input adat útvonalat használhatja a belépéshez, és minden output adat, amely az adat output interfészen keresztül lép ki modulból, csak az output adat útvonalon keresztül juthat ki.

[39] A CSA8000 adapter felvesz áramot.

FB_02.11.01:
Ha bármilyen lehetősége fennáll annak, hogy a modul szerkezete valamelyik porton lehetővé teszi nyílt formában megjelenő kriptográfiai kulcsok vagy más kritikus biztonsági pataméterek outputját, a szerkezetnek két független belső tevékenységet kell megkövetelnie, mielőtt az output bekövetkezik egy ilyen porton. Ebben az esetben a fejlesztői dokumentációnak definiálnia kell, hogy mik ezek a tevékenységek és hogyan nyújtanak védelmet a kritikus biztonsági paraméterek gondatlan közzétételével szemben. A dokumentációnak tartalmaznia kell a modul azon funkcionális részeinek a specifikációját (akár hardverben akár szoftverben van megvalósítva), amelyekben a két független tevékenység végrehajtásra kerül.

FB_02.12.01:
A fejlesztői dokumentációnak bizonyítania kell, hogy a modul szerkezete biztosítja az output adat útvonalaknak a logikai elkülönítését azoktól az eljárásoktól, amelyek kriptográfiai kulcsok generálását, kézi bevitelét és kinullázását hajtanak végre.

FB_02.13.01:
Amennyiben a modul szerkezete nem védett kritikus biztonsági paramétereket tesz szükségessé, beleértve nyíltan megjelenő kriptográfiai kulcsokat vagy nyíltan megjelenő hitelesítési adatokat, az ezen adatok inputjára vagy outputjára szolgáló adat portoknak fizikailag el kell különülniük a modul összes többi portjától. A fejlesztői dokumentációnak be kell mutatnia, hogy ez hogyan valósul meg.

FB_02.14.01:
Amennyiben a modul szerkezete nem védett kritikus biztonsági paramétereket tesz szükségessé, beleértve nyíltan megjelenő kriptográfiai kulcsokat, nyíltan megjelenő hitelesítési adatokat, az ezen paraméterek inputjára vagy outputjára szolgáló adat portokat közvetlenül a kriptográfiai határhoz kell csatolni, anélkül, hogy azok áthaladnának bármilyen, a kriptográfiai határon kívül eső processzoron, komplex logikai blokkon vagy a kulcs kezeléssel kapcsolatban nem álló funkciókat végrehajtó modul részen. A fejlesztői dokumentációnak be kell mutatnia a megvalósítás módját.

5.3 Szerepkörök és szolgáltatások

5.3.1 Szerepkörök

FB_03.01.01:
A fejlesztői dokumentációnak meg kell határoznia minden megkülönböztethető jogosult szerepkört, beleértve annak megnevezését, célját és azokat a szolgáltatásokat, amelyek az adott szerepkörben végrehajthatók.

FB_03.02.01:
A fenti FB_03.01.01 kielégítésére megkövetelt dokumentációba a fejlesztőnek legalább egy felhasználói és egy kriptográfiai tisztviselő szerepkört bele kell vennie.

FB_03.06.01:
A fejlesztői dokumentációnak meg kell határoznia, hogy egyidejűleg több operátor engedélyezett-e. Amennyiben engedélyezett, a fejlesztőnek ismertetnie kell azt a módszert, amellyel az egyes operátorok által végrehajtott jogosult szerepkörök és szolgáltatások szétválasztása megvalósul. A fejlesztői dokumentációnak tartalmaznia kell az egyidejű operátorokra vonatkozó minden korlátozást (pl. nem engedélyezett egyidejűleg egy operátor karbantartói szerepkörben és egy másik operátor felhasználói szerepkörben).

5.3.2 Szolgáltatások

FB3.07.01:
A fejlesztői dokumentációnak teljesen ismertetnie kell minden szolgáltatást, beleértve annak célját és funkcióját. A lehetséges szolgáltatások tartalmazhatják a következőket, bár nem kell ezekre korlátozódniuk:

- kriptográfiai műveletek, mint pl.:
  - kódolás,
  - dekódolás,
  - üzenet sértetlenség,
  - digitális aláírás létrehozás,
  - digitális aláírás ellenőrzés,
  - egyéb olyan műveletek, amelyek kriptográfia alkalmazását igénylik,
- kulcsgondozási műveletek, mint pl.:
  - kulcs és paraméter bevitel (input),
  - kulcs generálás,
  - kulcs kivitel (output),
  - kulcs archiválás,
  - kulcs nullázás,
  - egyéb kulcsgondozási funkciók,
- kriptográfiai menedzsment funkciók:
  - naplózási paraméterek bevitele és beállítása,
  - riasztás kezelés és “reset”-elés,
  - egyéb kriptográfiai menedzsment funkciók,

- operátor által választható ön-tesztek végrehajtása, mint pl.:
  - kriptográfiai algoritmus tesztek,
  - szoftver/förmver tesztek,
  - a kritikus funkciók tesztjei,
  - statisztikus véletlenszám generátor tesztek,
  - egyéb tesztek, amelyeket egy operátor kezdeményezhet,
- "státusz kijelzés", amely a következőket jelezheti ki:
  - aktív szerepkör(ök),
  - a modul kriptográfiai státusza (nullázott, beavatkozás következményeként fellépő, betöltött, inicializált, stb.),
  - hiba kód, ha a modul hiba állapotban van,
  - a megkerülés lehetőségének engedélyezettsége vagy tiltottsága, ha a megkerülés lehetséges,
  - A karbantartói tesztek végrehajtása[40],
  - A kriptográfia megkerülése[41].

FB_03.07.02:
A fejlesztői dokumentációnak meg kell határoznia minden egyes szolgáltatás esetében a szolgáltatás inputjait, a megfelelő szolgáltatás outputokat és a jogosult szerepkört, illetve szerepköröket, amelyekben a szóban forgó szolgáltatás végrehajtható. A szolgáltatás inputoknak tartalmaznia kell minden, a modulhoz irányuló adat vagy vezérlő inputot, amelyek kezdeményeznek vagy kieszközölnek meghatározott szolgáltatásokat, műveleteket vagy funkciókat. A szolgáltatás outputoknak minden olyan adat és státusz outputot tartalmazniuk kell, amelyeket a szolgáltatás inputok által kezdeményezett vagy kieszközölt szolgáltatások, műveletek vagy funkciók eredményeztek. A fejlesztő szolgáltathat egy mátrixot is, amely feltünteti mindazokat a szolgáltatásokat, amelyek végrehajthatók az egyes szerepkörökben.

FB_03.08.01:
A fejlesztői dokumentációnak ismertetnie kell a modul aktuális státuszának outputját és a felhasználó által hívható ön-tesztek inicializálását és futtatását, az egyéb olyan szolgáltatásokkal együtt, amelyek megfelelnek a FB_03.07.01-ben specifikáltaknak.

FB_03.11.01:
A fejlesztői dokumentációnak minden egyes szolgáltatás input esetében meg kell jelölnie a megfelelő szolgáltatás outputot.

[40] A CSA8000 modulban nincsenek karbantartói tesztek.
[41] A CSA8000 modulban a kriptográfia megkerülése nem lehetséges.

5.3.3 Operátori hitelesítés

FB_03.13.01:
A fejlesztői dokumentációnak ismertetnie kell, hogy egy áramellátás megszűnését követően a megelőző hitelesítések eredményei hogyan lesznek törölve.

FB_03.16.01:
A fejlesztőnek dokumentálnia kell azokat a mechanizmusokat, amelyeket az operátor azonosításának végrehajtására, az operátor azonosságának hitelesítésére, a szerepkör vagy szerepkörök közvetett vagy közvetlen kiválasztására és annak ellenőrzésére alkalmaznak, hogy az operátor jogosult-e a szerepkör(ök) felvételére. Meg kell jegyezni, hogy az azonosságon alapuló hitelesítés figyelembe veszi az operátornak az azonosságát, aki egy meghatározott szerepkört felvesz. Ez a hitelesítési módszer nemcsak a szerepkörök között tesz különbséget, de ugyanazon szerepkörön belül is; két operátor, aki ugyanazt a szerepkört kívánja betölteni, a modul számára különböző információt fog felmutatni, mivel azonosítójuk különböző. Például ha egy operátornak egy PIN kódot kell megadnia akkor, ha megkísérel egy szerepkört betölteni, minden egyes operátornak különböző PIN kóddal kell rendelkeznie, mivel a PIN kód a modul számára az operátort azonosítja.

FB_03.17.01:
A fejlesztőnek dokumentálnia kell, hogy a modul lehetővé teszi-e egy operátor számára, hogy szerepkört váltson anélkül, hogy azonosságát újra hitelesíteni kellene. Ha ez a lehetőség fennáll, a fejlesztői dokumentációnak ismertetnie kell, hogy az operátor számára fennáll az a lehetőség, hogy szerepkört váltson, és világosan ki kell jelentenie, hogy ellenőrizni kell az operátor jogosultságát az új szerepkörre.

FB_03.20.01:
A fejlesztői dokumentációnak világosan ki kell jelentenie, hogy a modul számára azonosságon alapuló hitelesítés kerül végrehajtásra. A fejlesztői dokumentációnak ismertetnie kell az alkalmazott hitelesítési mechanizmusokat az FB_03.16.01-ben specifikáltaknak megfelelően.

FB_03.20.02:
A fejlesztői dokumentációra vonatkozó azon követelmények, amelyek a nyílt formában megjelenő hitelesítési adatoknak a megadására vonatkoznak, erre kijelölt, közvetlenül kapcsolódó portokon keresztül, az FB_02.13.01-ben és az FB_02.14.01-ben vannak leírva.

5.4 Véges állapotú automata modell

FB_04.02.01:
A fejlesztőnek leírást kell adnia a véges állapotú automata modellről. Ezen leírásnak tartalmaznia kell a modul minden állapotának megadását és leírását, és le kell írnia a megfelelő állapot átmenetek mindegyikét. Az állapot átmeneteknek tartalmazniuk kell azokat a belső modul feltételeket, adat inputokat és vezérlő inputokat, amelyek egy állapotból egy másikba való átmenetet okoznak, és azokat a belső modul feltételeket, adat outputokat és státusz outputokat, amelyeket egy állapotból egy másikba való átmenet eredményez.

FB_04.04.01:
A fejlesztőnek megfelelő részletességű véges állapot diagrammo(ka)t is kell szolgáltatnia annak biztosítására, hogy ellenőrizni lehessen ezen követelmény-rendszernek való megfelelést.

5.5 Fizikai biztonság

5.5.1 Közös követelmények

FB_05.01.01:
A fejlesztői dokumentációnak specifikálnia kell, hogy a modulra vonatkozóan az alábbi három fizikai megvalósítás melyike áll fenn: egyetlen chip-ből álló modul, több chip-es, beágyazott modul vagy önmagában álló kriptográfiai modul[42]. A specifikált fizikai megvalósításnak konzisztensnek kell lennie az aktuális modul fizikai tervével.

FB_05.01.02:
A fejlesztői dokumentációnak teljesen le kell írnia azokat az alkalmazható fizikai biztonsági mechanizmusokat, amelyeket a modul felhasznál. A modul összes összetevőjét, beleértve minden hardvert, szoftvert, förmvert és adatot (beleértve a nyíltan tárolt kriptográfiai kulcsokat és nem védett kritikus védelmi paramétereket) védeni kell.

5.5.2 Több chip-es, beágyazott kriptográfiai modulra vonatkozó követelmények

FB_05.07.01:
A több chip-es, beágyazott modul chip-jeinek szabványos termék minőségű IC-knek kell lenniük, amelyeket úgy terveztek, hogy legalább a tipikus kereskedelmi minőségi specifikációknak feleljenek meg az áramellátás, hőmérséklet, megbízhatóság, ütés/rázkódás stb. tekintetében. Különösen fontos, hogy a modul standard passziválási technikát alkalmazzon minden egyes chip-re vonatkozóan. A fejlesztői dokumentációnak ismertetnie kell az IC-k minőségét. Ha valamelyik alkalmazott IC nem szabványos, annak passziválási szerkezetét szintén ismertetni kell.

FB_05.08.01:
A modult tipikus termék szintű, több chip-es eszközként kell megvalósítani, mint amilyen pl. egy IC-s nyomtatott áramköri kártya vagy kerámia hordozón lévő IC-k. A fejlesztői dokumentációnak ismertetnie kell a modulnak a termékbe való beépítését.

FB_05.09.01:
A modult egy nem átlátszó, beavatkozást kimutató burkolattal kell befedni, mint pl. egy, az alakot követő burkolat, vagy folyékony festék. Az anyagnak átlátszatlannak kell lennie a látható tartományon belül. A fejlesztői dokumentációnak meg kell adnia a beavatkozást kimutató, nem átlátszó burkolat fajtáját és annak karakterisztikáját.

FB_05.10.01:
A fejlesztői dokumentációnak rögzítenie kell, hogy a KÖV_05.10-ben specifikált három lehetőség közül melyiket alkalmazzák a követelmény kielégítésére, és alátámasztó részletes szerkezeti információt kell szolgáltatnia. A választástól függően a megfelelő fejlesztői követelményt (a következők egyikét, a választásnak megfelelően) ki kell elégíteni:

[42] A CSA8000 esetében ez: több chip-es, beágyazott modul.

- A modul több chip-es áramköri egységét teljesen be kell burkolni egy kemény, átlátszatlan kiöntő anyaggal. A kiöntő anyag lehet egy kemény, átlátszatlan epoxy vagy valamilyen más, azonos szintű biztonságot nyújtó anyag. Az anyagnak átlátszatlannak kell lennie a látható tartományon belül.
- A modult teljes egészében egy erős, nem eltávolítható burkolatba kell foglalni. A burkolatot olyan módon kell megtervezni, hogy a burkolat eltávolítására vagy az azon való áthatolásra irányuló kísérlet nagy valószínűséggel a modul súlyos károsodásához vezessen (vagyis a modul ne működjön).
- A modult teljes egészében egy erős, eltávolítható burkolatba kell foglalni, és tartalmaznia kell egy beavatkozásra reagáló és nullázó áramköri egységet. Az áramköri egységnek folyamatosan figyelnie kell a burkolatot, és annak eltávolításakor azonnal hatékonyan nulláznia kell minden nyíltan tárolt kriptográfiai kulcsot és minden más nem védett kritikus biztonsági paramétert. Az áramköri egységnek működőképesnek kell lennie, amikor nyíltan tárolt kriptográfiai kulcsok vagy más nem védett kritikus biztonsági paraméterek vannak tárolva a modulon belül[43].

FB_05.11.01:
Ha a modul egy tokba vagy burkolatba van foglalva, és ha a tok vagy burkolat valamilyen szellőző nyílást vagy rést tartalmaz, akkor azoknak kicsiknek kell lenniük, és olyan módon kell azokat megalkotni, ami meggátolja a foglalaton belüli észrevétlen szondázást. A fejlesztői dokumentációnak ismertetnie kell a szellőzés fizikai szerkezetének megoldási módját.

[43] A CSA8000 esetében a 3. megoldást alkalmazzák: az adapter egy polikarbonátból készült erős borítást kapott, mely alatt nyomásérzékelő mikrokapcsolók és érzékelők vannak elhelyezve. A borítás bármely részének megbontása a biztonságkritikus paramétereket (kulcsok és PIN kódok) tartalmazó memória nullázását eredményezi. A modul áramellátási állapotától függően ez a nullázódás kétfélképpen következik be: bekapcsolt állapotban az eszköz minden biztonságkritikus paramétert felülír, kikapcsolt állapotban pedig a tartalék (elem) áramforrás leszakad a RAM-ról. Ezen kívül a CSA8000 adapter lehetővé teszi a nullázás beállítását arra az esetre is, amikor a modult a gazdagép PCI slotjából kiemelik, illetve egy olyan interfésze is van, melybe egy külső behatolás érzékelő köthető be.

5.6. Szoftver biztonság

FB_06.01.01:
A KÖV_06.01 követelmény kielégítésére a fejlesztői dokumentációra vonatkozó előírások megegyeznek az FB_01.06.01, illetve az FB_01.06.02 követelményeivel.

FB_06.02.01:
A fejlesztőnek részletes szoftver terv dokumentációt kell nyújtania. Ezen dokumentációnak tartalmaznia kell a véges állapotú automata modell diagrammokat és leírásokat, de semmiképpen sem korlátozódhat ezekre. Amennyiben a véges állapotú automata specifikáció és a forrás kód közötti kapcsolat nem világos, a fejlesztőnek további dokumentációt kell szolgáltatnia, amely ismertetni a véges állapotú automata specifikáció és a forrás kód közötti kapcsolatot.

FB_06.03.01:
A fejlesztői dokumentációnak egy külön részt vagy fejezetet kell tartalmaznia, amely világosan ismerteti, hogy a szoftver/förmver szerkezet hogyan felel meg a kriptográfiai modul biztonsági politikájának (működési szabályainak).

FB_06.04.01:
A fejlesztőnek szolgáltatnia kell egy listát, amely tartalmazza a kriptográfiai modul által tartalmazott minden szoftver és förmver modul, funkció és eljárás megnevezését. Ez a lista állhat a végrehajtható program aktuális példányát előállító program szerkesztési eljáráshoz *(link)* használt tételekből.

FB_06.04.02:
A fejlesztőnek egy megjegyzésekkel ellátott forrás listát kell szolgáltatnia a kriptográfiai modul által tartalmazott minden szoftver és förmver modulról, funkcióról és eljárásról, a fejlesztő által megadott szoftver/förmver listán feltüntetetteknek megfelelően.

FB_06.05.01:
A KÖV_06.04 követelmény kielégítésére vonatkozóan a fejlesztői dokumentációval szembeni elvárások ugyanazok, mint az FB_06.04.02-ben leírtak a KÖV_06.04 követelményeire vonatkozóan.

FB_06.06.01:
A fejlesztőnek rá kell mutatnia minden olyan szoftver modulra, amely nem magas szintű program nyelven íródott, és elfogadható magyarázatot, illetve indoklást kell adnia arra, hogy a modul miért készült alacsony szintű programnyelven. A magyarázatnak hivatkoznia kell arra, hogy vagy nem állt rendelkezésre magas szintű programnyelv, vagy pedig a szoftver fokozott hatékonysága volt szükséges. Hatékonysági okokra való hivatkozás esetében az indoklásnak technikai magyarázatot kell adnia arra, hogy a magas szintű programnyelv miért nem nyújt kellő hatékonyságot.

5.7. Az operációs rendszer biztonsága

Nincsenek követelmények[44].

[44] Mivel a CSA8000 kriptográfiai modulnak nincs saját operációs rendszere.

5.8. Kriptográfiai kulcsgondozás

5.8.1 Általános követelmények

FB_08.01.01:
A fejlesztői dokumentációnak ismertetnie kell a kriptográfiai modul kulcsgondozását. Minimális követelményként a dokumentációnak meg kell adnia a következő információkat:

1. Alapvető kulcs információk, úgy mint:
   a. a modul által alkalmazott valamennyi kulcstípus listája, mind a külsőleg mind a belsőleg generált kulcsokra vonatkozóan,
   b. minden egyes kulcs funkciójának magyarázata,
   c. minden bevitt és outputként kinyerhető kulcs formátuma,
   d. annak kifejtése, hogy hogyan vannak védve a kulcsok,
2. Kulcs generálás, úgy mint:
   a. a kulcs generálási eljárás leírása,
   b. annak meghatározása, hogy a kulcs generálási algoritmus FIPS által jóváhagyott-e,
   c. annak meghatározása, hogy mely kulcstípusok vannak generálva,
3. Kulcs szétosztás, úgy mint:
   a. a szétosztási technika ismertetése,
   b. annak jelzése, hogy ez a technika FIPS által jóváhagyott-e,
   c. annak jelzése, hogy mely kulcstípusokat kell szétosztani,
4. Kulcs bevitel és output, úgy mint:
   a. a kulcs beviteli eljárások ismertetése,
   b. a kulcs output eljárások ismertetése,
   c. annak közlése, hogy kézi vagy elektronikus kulcs bevitelt alkalmaznak-e,
   d. annak közlése, hogy kézi vagy elektronikus kulcs outputot alkalmaznak-e,
   e. annak közlése, hogy mely típusú kulcsok esetén történik kézi bevitel, illetve output,
   f. annak közlése, hogy mely típusú kulcsok esetén történik elektronikus bevitel, illetve output,
   g. annak a formának a közlése, amelyben a kulcsok bevitele, illetve outputja történik (nyílt formában, kódolt formában vagy osztott tudás alapján működő eljárások segítségével),
   h. annak közlése, hogy alkalmazásra kerül-e manuális kulcs beviteli teszt a bejegyzett kulcsok ellenőrzésére,
5. Kulcs tárolás, úgy mint:
   a. annak közlése, hogy milyen típusú kulcsok kerülnek tárolásra
   b. annak közlése, hogy ezek hol kerülnek tárolásra
   c. annak a formának a közlése, amelyben a kulcsok tárolásra kerülnek (nyílt formában, kódolt formában, osztott tudás alapján működő eljárások segítségével)

6. Kulcs megsemmisítés, úgy mint:
   a. a kulcs megsemmisítő technikák és mechanizmusok ismertetése,
   b. a megszorítások közlése, amelyek mellett a modul nullázható,
   c. annak közlése, hogy milyen típusú kulcsok kerülnek nullázásra és miért,
   d. annak közlése, hogy mely biztonsági paraméterek kerülnek nullázásra és miért,
   e. annak közlése, hogy mely kulcstípusok és biztonsági paraméterek nem kerülnek nullázásra és miért,
7. Kulcs archiválás, úgy mint:
   a. kulcs archiválás alkalmazásra kerül-e,
   b. a kulcs archiválási technikának az ismertetése,
   c. annak közlése, hogy mely típusú kulcsok archiválhatók,
   d. annak közlése, hogy a kulcsok kódolva vannak-e az archiváláshoz.

FB_08.02.01:
A fejlesztői dokumentációnak ismertetnie kell minden, a modul számára belső titkos és/vagy magán kulcs védelmét az FB_08.01.01 alatti 1-es tétel követelményeinek megfelelően. A védelemnek tartalmaznia kell olyan mechanizmusok implementálását, amelyek védelmet nyújtanak a jogosulatlan felfedéssel, módosítással és helyettesítéssel szemben.

FB_08.03.01:
Ha a modul támogat nyilvános kulcsokat, a fejlesztői dokumentációnak ismertetnie kell minden nyilvános kulcs védelmét az FB_08.01.01 alatti 1-es tétel követelményeinek megfelelően. A védelemnek tartalmaznia kell olyan mechanizmusok implementálását, amelyek védelmet nyújtanak a jogosulatlan módosítással és helyettesítéssel szemben.

5.8.2 Kulcs generálásra vonatkozó követelmények

FB_08.04.01:
Lásd az FB_08.01.01 alatti 2a és 2b tételeket a fejlesztői dokumentációra vonatkozó követelmények tekintetében. Ezek tartalmazzák a kulcs generálási algoritmus leírását és a FIPS által jóváhagyott kulcs generálási algoritmus specifikációját. A fejlesztőnek bizonyítékot is kell nyújtania arra vonatkozóan, hogy a kulcs generálási algoritmus FIPS által jóváhagyott. Ennek a bizonyítéknak tartalmaznia kell egy FIPS értékelésre meghatalmazott (akkreditált) laboratóriumtól származó tanúsítványt, mely bizonyítja, hogy a modulban végrehajtott algoritmus FIPS által jóváhagyott algoritmus. Ha nem áll rendelkezésre egy FIPS által meghatalmazott laboratórium, amely érvényesíthetné az algoritmust, akkor a fejlesztő szervezetnek kell gondoskodnia egy írásos nyilatkozatról, amely bizonyítja, hogy a modulban végrehajtott algoritmus FIPS által jóváhagyott algoritmus.

FB_08.05.01:
Ha a modul véletlenszám generátort alkalmaz[45], a kulcs generálási eljárásra vonatkozó fejlesztői dokumentációnak, amely az FB_08.02.01 alatti 2-es tételben van specifikálva, ismertetnie kell azt is, hogy a véletlenszám generátor hogyan működik.

[45] A CSA8000 egy hardver véletlenszám generátort alkalmaz, kombinálva egy FIPS által jóváhagyott véletlenszám generálási technikával (FIPS 186-2).

FB_08.06.01:
A kulcsgondozás dokumentációjának meg kell határoznia, hogy a kulcs generáláshoz kezdeti kulcs alkalmazva van-e. Ha igen, akkor a kulcsgondozás dokumentációjának intézkednie kell a kezdeti kulcs beviteléről hasonló módon, mint minden más kulcs esetében.

FB_08.07.01:
A kulcs generálást a felhasználói szolgáltatói állapotok egyikének kell tekinteni (lásd KÖV_04.05). A közbenső kulcs generálási állapotok azok az állapotok, amelyeken keresztül a modul átmegy a kulcs generálási eljárás inicializálása és befejezése között. A közbenső kulcs generálási értékek olyan, matematikai számításból származó belső eredmények, amelyek végül is egy kriptográfiai kulcsot eredményeznek. A véges állapotú automata modell /lásd a 4. fejezet (Véges állapotú automata modell) követelményeit/ nem tartalmazhat ilyen állapotokat és nem tehet lehetővé semmilyen közbenső kulcs generálási állapotnak vagy közbenső kulcs generálási értéknek a kiadását. A kulcs generálási eljárások nem tehetnek lehetővé semmilyen outputot a kulcs generálási folyamat során, kivéve azokat az értékeket, amelyek kódolva vannak.

5.8.3 Kulcs szétosztásra vonatkozó követelmények

FB_08.08.01:
Lásd az FB_08.01.01 alatti 3a és 3b tételeket a fejlesztői dokumentációra vonatkozó követelményeket illetően. Ezek tartalmazzák a kulcs szétosztási technika leírását és annak jelzését, hogy ez a technika FIPS által jóváhagyott-e. Ha a kulcs szétosztási technika FIPS által jóváhagyott, a fejlesztőnek bizonyítékot kell nyújtania egy olyan tanúsítvány formájában, amelyet egy FIPS értékelésre meghatalmazott (akkreditált) laboratórium bocsát ki a kulcs szétosztási technikára vonatkozóan. Ha nem áll rendelkezésre ilyen bizonyítvány, akkor a fejlesztő szervezetnek kell gondoskodnia egy írásos nyilatkozatról, amely bizonyítja, hogy a kulcs szétosztási technika FIPS által jóváhagyott. Amennyiben a kulcs szétosztási technika nem FIPS által jóváhagyott, akkor a fejlesztői dokumentációnak világosan ki kell ezt jelentenie.

5.8.4 Kulcs bevitelére és kivitelére vonatkozó követelmények

FB_08.09.01:
Lásd az FB_08.01.01 alatti 4a – 4f tételeket a fejlesztői dokumentációra vonatkozó követelményeket illetően.

FB_08.09.02:
A kulcs beviteli és output eljárások és mechanizmusok implementálása során a fejlesztőnek a következő irányvonalakat kell követnie:

- Ha tisztán kézi módszereket alkalmaznak a kulcs bevitelre vagy kulcs kivitelre, azok történhetnek a következők valamelyikével, bár nem kizárólag azokkal:

  - Billentyűzet[46],
  - forgó kapcsolók,
  - kézzel forgatható kerekek,
  - LCD display-k,
- Ha elektronikus eszközöket alkalmaznak a kulcs bevitelre vagy kulcs kivitelre, azok történhetnek a következők valamelyikével, bár nem kizárólag azokkal:
  - memória kártya/token (pl. mágnes csíkos kártyák, IC chip készülékek),
  - intelligens kártyák/tokenek[47],
  - elektronikus kulcs betöltők.

FB_08.10.01:
A fejlesztői dokumentációnak meg kell határoznia, hogy mely kulcstípusok vannak elektronikus úton szétosztva, és meg kell adni azt a formát, amelyben az elektronikusan szétosztott kulcsok a modulba bevitelre vagy abból kinyerésre kerülnek.

FB_08.11.01:
Lásd az FB_08.01.01 alatti 4h tételt a fejlesztői dokumentációra vonatkozó követelményeket illetően.

FB_08.12.01:
A dokumentált kulcs beviteli eljárásnak lehetővé kell tennie a kódolt kulcsok és kulcs komponensek kijelzését a kulcs beírás folyamán, ha ez szükséges, de lehetetlenné kell tenni azoknak a nyílt formájú titkos és magán kulcsok kijelzését, amelyek a kódolt kulcsok és kulcs komponensek beviteléből származnak.

FB_08.12.01:
A dokumentált kulcs beviteli / kiviteli eljárásoknak ismertetniük kell azokat a mechanizmusokat vagy eljárásokat, amelyeket annak biztosítására alkalmaznak, hogy minden kulcs a megfelelő jogi személlyel legyen összekapcsolva.

FB_08.15.01:
Lásd az FB_08.01.01. alatti 4g tételt a fejlesztői dokumentációra vonatkozó követelményeket illetően.

FB_08.16.01:
Ha kézi úton szétosztott titkos vagy magán kulcsokat osztott tudáson alapuló eljárás segítségével visznek be vagy nyernek outputként ki[48], a fejlesztői dokumentációnak a kulcs beviteli eljárás leírásában meg kell határoznia, hogy az operátor minden egyes kulcs komponens esetén külön-külön lesz hitelesítve.

FB_08.16.02:
A kulcs komponensek közvetlen bevitelére vonatkozó fejlesztői követelmények az FB_02.14.01-ben vannak leírva.

[46] Azon ritka esetben, amikor a CSA8000 kézi kulcsbevitelt alkalmaz /a 48 hexadecimális HIMK kulcs bevitelére, illetve a magán kulcsok mentésére alkalmazott kulcs-csomagoló kulcsok (KWRAP) bevitelére), a billentyűzetet lehet használni.
[47] A CSA8000 magán kulcsainak mentésére és visszatöltésére intelligens kártyák használhatók.
[48] Ez a helyzet a CSA8000 esetében, ahol a HIMK titkos kulcsokat, illetve a különböző magán kulcsokat tetszőleges számú komponensre lehet (kódolt formában) kimenteni, illetve a komponensekből visszaállítani.

5.8.5 Kulcs tárolásra vonatkozó követelmények

FB_08.17.01:
Lásd az FB_08.01.01. alatti 5a és 5c tételeket a fejlesztői dokumentációra vonatkozó követelményeket illetően.

FB_08.17.02:
A fejlesztői dokumentációnak ismertetnie kell minden, a modul számára belső titkos és magán kulcs védelmét az FB_08.02.01-ben meghatározottaknak megfelelően. A védelemnek tartalmaznia kell olyan mechanizmusok implementációját is, amelyek a jogosulatlan felfedéssel, módosítással és helyettesítéssel szemben nyújtanak védelmet.

FB_08.18.01:
A kulcs tárolásról szóló fejlesztői dokumentációnak ismertetnie kell azokat a mechanizmusokat vagy eljárásokat, amelyeket annak biztosítására alkalmaznak, hogy minden kulcs a megfelelő jogi személlyel legyen összekapcsolva.

5.8.6 Kulcs megsemmisítésre vonatkozó követelmények

FB_08.19.01:
Lásd az FB_08.01.01. alatti 6 tételt a fejlesztői dokumentációra vonatkozó követelményeket illetően.

5.8.7 Kulcs archiválásra vonatkozó követelmények

FB_08.20.01:
Ha a modul támogatja a kulcs archiválást[49], lásd az FB_08.01.01. alatti 7a-tól 7d-ig terjedő tételeket a fejlesztői dokumentációra vonatkozó követelményeket illetően.

[49] A CSA8000 támogatja a HIMK titkos kulcsok és a különböző magán kulcsok archiválását (komponensekre bontva, kódolt formában, intelligens kártyákon tárolva).

5.9 Kriptográfiai algoritmusok

FB_09.01.01:
A fejlesztőnek egy tanúsítványt kell szolgáltatnia, amely bizonyítja, hogy a kriptográfiai modul FIPS által jóváhagyott algoritmusokat használ, és hogy ezen FIPS által jóváhagyott algoritmusok tesztelve lettek és megfeleltek a FIPS által jóváhagyott eljárásoknak és teszteknek egy FIPS ellenőrzésre meghatalmazott (akkreditált) szervezetnél[50].
Megjegyzés: A fejlesztő beépíthet a kriptográfiai modulba más (azaz nem FIPS által jóváhagyott) kriptográfiai algoritmusokat is[51].

5.10 Elektromágneses interferencia, elektromágneses kompatibilitás

FB_10.01.01:
A fejlesztőnek egy FCC bizonyítványt kell szolgáltatnia arra vonatkozóan, hogy a kriptográfiai modul rádió kielégít minden FCC követelményt.

FB_10.03.01:
A fejlesztőnek egy FCC bizonyítványt kell szolgáltatnia arra vonatkozóan, hogy a kriptográfiai modul alkalmazkodik azokhoz az EMI/EMC követelményekhez, amelyek az FCC 15 részében, a J alrészben és B osztályban vannak megadva.

5.11 Ön-tesztek

5.11.1 Általános követelmények

FB_11.01.01:
A fejlesztőnek listát kell szolgáltatni valamennyi, kötelező és opcionális ön-tesztről, amelyeket a modul végre tud hajtani. Ennek a listának egyaránt tartalmaznia kell az áram bekapcsolási teszteket és a feltételes teszteket.

FB_11.02.01:
A fejlesztőnek dokumentálnia kell minden egyes ön-teszthez kapcsolódó minden hiba állapotot, és minden egyes hiba állapot esetén közölnie kell a várt hiba jelzést.

FB_11.03.01:
Lásd az FB_02.04.01-t a fejlesztői dokumentációra vonatkozó követelményeket illetően. A fejlesztői tervezetnek azt is biztosítania kell, hogy kriptográfiai műveletek nem hajthatók végre, amíg a modul hiba állapotban van.

[50] A CSA8000 rendelkezik ilyen tanúsítvánnyal a DES, Triple-DES, DSA, SHA-1 és RSA kriptográfiai algoritmusokra.
[51] A CSA8000 megvalósít több FIPS által nem jóváhagyott kriptográfiai algoritmust is, köztük az alábbiakat: HMAC-SHA-1, RSA (kódolás,dekódolás), CAST128, IDEA, AES (az értékeléskor az AES még nem volt jóváhagyva), RC2, RC4, MD2, MD5, Diffie-Hellman (kulcsegyeztetés).

FB_11.04.01:
A fejlesztői dokumentációnak minden egyes hiba feltételre vonatkozóan meg kell adnia annak megnevezését, azokat az eseményeket, amelyek kiváltják, azokat a tevékenységeket, amelyek szükségesek a hiba törlésére és a normál működéshez való visszatéréshez. Meg kell jegyezni, hogy a szükséges tevékenységek magukban foglalhatják azt is, hogy a modult a gyártóhoz kell elküldeni javításra.

5.11.2 Az áram alá helyezési tesztek

5.11.2.1 Általános tesztek

FB_11.05.01:
Lásd az FB_11.01.01-t a fejlesztői dokumentációra vonatkozó követelményeket illetően. Meg kell jegyezni, hogy az áram alá helyezés után a statisztikus véletlenszám generátor tesztek végrehajtása a 4-es szint esetén kötelező, az egyéb szintek esetén opcionális[52]. Ezen felül a fejlesztőnek dokumentálnia kell minden opcionális, az áram alá helyezés utáni ön-tesztet.

FB_11.06.01:
A fejlesztői dokumentációnak meg kell követelnie, hogy az áram alá helyezés utáni ön-tesztek nem vonhatnak maguk után semmilyen operátori inputot vagy operátori tevékenységet.

FB_11.07.01:
A fejlesztőnek dokumentálnia kell azt a jelzést, amelyet a modul kiad az áram alá helyezés után végrehajtandó tesztek sikeres végrehajtása esetén.

FB_11.08.01:
Lásd az FB_02.04.02-t a fejlesztői dokumentációra vonatkozó követelményeket illetően.

FB_11.09.01:
A fejlesztőnek ismertetnie kell azokat az eljárásokat, amelyek segítségével egy operátor elindíthatja az áram alá helyezéskor elvégzendő ön-teszteket.

5.11.2.2 Kriptográfiai algoritmus tesztek

FB_11.10.01:
A fejlesztőnek dokumentálnia kell az "ismert eredmény" tesztet, amelyet a kriptográfiai algoritmus tesztelésére végre kell hajtani.

FB_11.11.01:
Az ismert eredmény tesztre vonatkozó fejlesztői dokumentációban a fejlesztőnek közölnie kell, hogy minden egyes kriptográfiai funkció le van tesztelve az ismert eredmény teszttel, és fel is kell sorolni ezeket a funkciókat.

[52] A CSA8000 végrehajtja a 3-as szinten opcionális statisztikus véletlenszám generátor teszteket.

5.11.2.3 Szoftver/förmver teszt

FB_11.14.01:
A fejlesztői dokumentációnak meg kell határoznia, hogy a beágyazott szoftver és förmver sértetlenségének biztosítására hiba detektálási kódot (EDC) vagy pedig egy FIPS által jóváhagyott hitelesítési technikát (pl. FIPS által jóváhagyott adat hitelesítési kódot (DAC) vagy FIPS által elfogadott digitális aláírást) alkalmaznak-e[53]. Ha a modul egy FIPS által jóváhagyott hitelesítési technikát implementál, a fejlesztőnek egy olyan bizonyítékot kell szolgáltatnia, amely tartalmaz egy FIPS értékelésre meghatalmazott (akkreditált) laboratóriumtól származó tanúsítványt, amely kijelenti, hogy a modulban implementált hitelesítési technika FIPS által jóváhagyott[54]. Egy ilyen bizonylat hiányában a fejlesztő cégnek írásos nyilatkozatot kell szolgáltatnia, amely kijelenti, hogy a modulban implementált hitelesítési technika FIPS által jóváhagyott. A dokumentációnak ismertetnie kell az implementált sértetlenséget vizsgáló mechanizmust.

5.11.2.4 Kritikus funkciók tesztjei

FB_11.15.01:
A kritikus funkciók olyan funkciókként definiálhatók, amelyek nyílt formában tárolt információk felfedéséhez vezethetnek (beleértve az adatat és kriptográfiai kulcsokat), ha a funkció végrehajtása sikertelen. A kritikus funkciók közé tartoznak pl. a véletlen / pszeudó véletlenszám előállítások, a kriptográfiai algoritmusok működése és a kriptográfia megkerülése.

FB_11.15.02:
A fejlesztőnek minden kritikus funkcióról egy mátrixot kell szolgáltatnia. Minden egyes kritikus funkció esetén a fejlesztőnek fel kell tüntetnie:

- annak célját (pl. azt, hogy a szóban forgó funkció miért "kritikus"),
- melyek azok a kritikus funkciók, amelyeket az áram alá helyezési ön-tesztek tesztelnek,
- melyek azok a kritikus funkciók, amelyeket feltételhez kötött tesztek tesztelnek.

5.11.2.5 Statisztikus véletlenszám generátor tesztek

FB_11.16.01:
Ha a modul egy hardver vagy pszeudó véletlenszám generátort implementál, a fejlesztői dokumentációnak specifikálnia kell a véletlenszerűségre vonatkozó statisztikai teszteket. A modul által megvalósított véletlenszerűségi tesztek tartalmazhatják az összes következőkben felsorolt tesztet, bár nem kell ezekre korlátozódniuk:

- monobit teszt,
- poker teszt,
- runs teszt,
- long run teszt.

[53] A CSA8000 a gyártó cég (Eracom) digitális aláírását alkalmazza a beágyazott szoftver hitelességének ellenőrzésére, ugyanakkor egy 32 bites hiba detektálási kódot, valamint az SHA-1 üzenet lenyomatoló kódot használja a beágyazott szoftver integritásának gyors ellenőrzésére.
[54] A CSA8000 rendelkezik ilyen tanúsítvánnyal (DSA, SHA-1, RSA).

FB_11.17.01:
Lásd az FB_11.09.01-t a fejlesztői dokumentációra vonatkozó követelményeket illetően azon tesztek esetén, amelyeket egy operátor kezdeményezhet.

5.11.3 Feltételhez kötött tesztek

5.11.3.1 Páronkénti konzisztencia teszt

FB_11.19.01:
Ha a modul nyilvános és magán kulcsokat generál, a fejlesztői dokumentációnak ismertetnie kell, hogy ezen kulcsokat hogyan használja a modul. Ha a kulcsokat kódolásra/dekódolásra használja, a dokumentációnak ismertetnie kell egy páronkénti konzisztencia tesztet, amely kódoláson/dekódoláson alapul. Ha a kulcsokat a modul digitális aláírások számítására és ellenőrzésére használja, akkor vagy a kódolásra/dekódolásra használatos eljáráshoz hozzáadva, vagy azt helyettesítve, a fejlesztői dokumentációnak ismertetnie kell egy páronkénti konzisztencia tesztet, amely egy digitális aláírás létrehozásán és ellenőrzésén alapul.

5.11.3.2 Szoftver/förmver betöltési tesztek

FB_11.20.01:
A fejlesztői dokumentációnak ismertetnie kell a FIPS által jóváhagyott hitelesítési technikát, amelyet a kívülről betöltött szoftver és förmver sértetlenségének védelmére alkalmaznak[55]. A fejlesztőnek bizonyítékot kell szolgáltatnia arra vonatkozóan, hogy a technika FIPS által jóváhagyott. Ezen bizonyítéknak egy FIPS értékelésre meghatalmazott (akkreditált) laboratóriumtól származó érvényesítési bizonyítványból kell állnia, amely kijelenti, hogy a modulban implementált hitelesítési technika FIPS által jóváhagyott. Egy ilyen érvényesítési bizonylat hiányában a fejlesztő cégnek írásos nyilatkozatot kell szolgáltatnia, amely kijelenti, hogy a modulban implementált hitelesítési technika FIPS által jóváhagyott.

5.11.3.3 Kézi kulcs bevitel tesztje

FB_11.21.01:
A fejlesztőnek dokumentálnia kell a kézi kulcs bevitel tesztjét. Attól függően, hogy hiba detektáló kódot vagy duplikált kulcs bevitelt alkalmaznak, a kézi kulcs bevitel tesztje tartalmazhatja a következőket:

- hiba detektáló kódok (EDC)[56]:
  - a hiba detektáló kód számítási algoritmusának ismertetése,
  - az ellenőrzési eljárás ismertetése,
  - várható outputok sikeres vagy sikertelen teszt esetén,
- duplikált kulcs bevitel:
  - az ellenőrzési eljárás ismertetése
  - várható outputok sikeres vagy sikertelen teszt esetén

[55] A CSA8000 által alkalmazott technika az új szoftver digitális aláírása (RSA algoritmussal) a fejlesztő cég által, illetve az upgrade betöltésekor az aláírás ellenőrzése az adminisztrátor által.
[56] A CSA8000 ezt a technikát alkalmazza.

FB_11.21.02:
Ha a hiba detektáló kódot alkalmazzák[57], a fejlesztői dokumentáció azon részének, amely a kriptográfiai kulcsok formátumát ismerteti (lásd KÖV_08.01), tartalmaznia kell a hiba detektáló kódra vonatkozó részt is.

5.11.3.4 Folyamatos véletlenszám generátor teszt

FB_11.22.01:
Ha a modul hardver vagy pszeudó véletlenszám generátort implementál[58], a fejlesztőnek dokumentálnia kell a folyamatos véletlenszám generátor tesztet.

[57] Mint a CSA8000 esetében.
[58] Mint ahogy a CSA8000, mely egy hardver véletlenszám generátort alkalmaz, kombinálva egy FIPS által jóváhagyott (pszeudó) véletlenszám generálási technikával (FIPS 186-2).

6. Egy 3-as típusú BALE követelményeinek megalapozása az SSCD védelmi profil szerint

Az alábbiakban áttekintjük annak az SSCD védelmi profilnak a bevezető részeit (a környezetre vonatkozó állításokat, valamint a biztonsági célokat), melyek megalapozzák a védelmi profil funkcionális és garanciális biztonsági követelményeit (melyeknek való megfelelőséget kívánjuk a CSA8000 adapterre kimutatni a későbbiekben).

6.1 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.

6.1.1 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 nyújtott 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.

6.1.2 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[59] meghatározott elemeket, köztük az aláíró nevét és az aláíró kizárólagos ellenőrzése alatt álló BALE-n implementált aláírás-létrehozó adatnak megfelelő aláírás-ellenőrző adatot[60]. A hitelesítés-szolgáltató a tanúsítvány vagy más nyilvánosan rendelkezésre álló információn keresztül biztosítja, hogy a BALE-nak az aláírással kapcsolatos használata nyilvánvaló legyen.

[59] lásd a 2001. évi XXXV. elektronikus aláírási törvény 2. számú mellékletét
[60] 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.

6.2 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 módosítva az aláírás-létrehozó alkalmazás és a BALE közötti átvitel során. Az intelligens kártyának biztosítania kell azt is, hogy önmaga sem módosítja az aláírandó adat-reprezentánst.

Az aláírás előállítási funkció csak a törvényes aláírónak áll rendelkezésre

A 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.

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.

7. Egy 3-as típusú BALE funkcionális biztonsági követelményei

Az alábbiakban felsorolt funkcionális biztonsági követelmények kielégítése esetén a BALE:

- kivédi a biztonságra irányuló veszélyeket (6.1.1),
- érvényre juttatja a biztonsági szabályokat (6.1.2), egyúttal
- megvalósítja a biztonsági célokat (6.2).

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

8. 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) szintű értékelés garanciaosztályait és garanciaösszetevőit.

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

9. A CSA8000 megfelelése az SSCD védelmi profil követelményeinek

9.1 A CSA8000 megfelelése az SSCD védelmi profil funkcionális biztonsági követelményeinek

Kriptográfiai kulcs generálás (FCS_CKM.1)	
Követelmény (CC SSCD-PP)	A BALE legyen képes kriptográfiai kulcsokat generálnia a következőknek megfelelően: ***[behelyettesítés: kriptográfiai kulcs generálási algoritmus]*** és ***[behelyettesítés: kriptográfiai kulcs méret],*** mely eleget tesz a következőknek: ***[behelyettesítés: szabványok listája.]***
CSA8000 tulajdonság	A CSA8000 képes (többek között): • az **RSA** és **DSA** digitális aláírás algoritmusokhoz kulcsokat generálni, • **triple-DES** kulcsokat generálni a host oldali aláíró alkalmazással (operátorral) kialakított megbízható csatorna kiépítéséhez (HIMK kulcsok, majd munkaszakasz kulcsok). A CSA8000 a fenti kulcsok generálásához egy belső kulcs generálási funkcióval van kiegészítve. A kulcs generálási funkció egy hardver fizikai véletlenszám generátorra épül, mely a gyors kulcsgenerálás érdekében egy FIPS által jóváhagyott (pszeudó) véletlenszám generálási technikával (FIPS 186-2) van kombinálva.
Teljesített követelmények (FIPS 140-1 3-as szint)	4.8.2 Kulcs generálásra vonatkozó követelmények KÖV_08.04: /FIPS által jóváhagyott kulcs generálási algoritmus implementálása/ KÖV_08.05: /korrekt véletlenszám generálás/ KÖV_08.06: /a kezdeti *(seed)* kulcs védett bevitele/ KÖV_08.07: /a közbenső kulcs generálási állapotok és értékek védelme/

Értékelés	Az RSA (legalább 1020 bitméret mellett) minősített aláíráshoz elfogadott algoritmus. A CSA8000 képes a megfelelő méretű RSA kulcsok szabványos generálására. A DSA (legalább 1024 bites p prímhosszúság és legalább 160 bites q prímhosszúság mellett) minősített aláíráshoz elfogadott algoritmus. A CSA8000 képes a megfelelő méretű DSA kulcsok szabványos generálására. Következésképp a CSA8000 képes minősített aláírásokhoz elfogadott digitális aláíró algoritmusok kulcsainak generálására. A triple-DES szabvány kriptográfiai algoritmus, alkalmas a megbízható csatorna bizalmasságának biztosítására (112 és 168 bitméret mellett egyaránt). A CSA8000 képes mindkét megfelelő méretben triple-DES kulcsok szabványos generálására. Következésképpen a CSA8000 képes a (host oldali) aláíró alkalmazással kialakítandó megbízható csatorna bizalmasságát biztosító, megfelelő kriptográfiai algoritmus kulcsainak szabványos generálására.
Következtetés	A CSA8000 (a feltételek betartása esetén) **megfelel** az SSCD-PP „Kriptográfiai kulcs generálás” követelményének.
Feltételek:	2., 3., 4., 8., 9.

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.]***
CSA8000 tulajdonság	A CSA8000: • automatikusan törli a munkaszakasz kulcsokat a kommunikációs munkaszakasz végén, • valamennyi egyéb kulcsát le lehet nullázni (törölni) (a Token felhasználók és a Token kriptográfiai tisztviselők a felügyeletük alatt álló kulcsokat nullázhatják le, míg az Adminisztrátor a modul valamennyi kulcsát nullázhatja)
Teljesített követelmények (FIPS140-1 3.)	KÖV_08.19: /a nyíltan tárolt kriptográfiai kulcsok (szabványos, FIPS által jóváhagyott) törlési lehetősége/
Értékelés	A kulcsok egy része (munkaszakasz kulcsok) automatikusan törlődik, a többi kulcsra pedig biztosított a törlés lehetősége. A FIPS értékelés azt is igazolja, hogy a törlés a tárolt kulcsértékeinek fizikailag visszafordíthatatlan megsemmisítésével jár. Következésképpen a BALE képes tárolt kulcsértékeinek fizikailag visszafordíthatatlan, szabványos megsemmisítésére.
Következtetés	A CSA8000 (a feltételek betartása esetén) **megfelel** az SSCD-PP „Kriptográfiai kulcs megsemmisítés” követelményének.
Feltétel:	13.

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].***
CSA8000 tulajdonság	A CSA8000: • megvalósítja a páronkénti konzisztencia tesztet az RSA és a DSA kulcspárok generálásakor, • támogatja az **RSA** digitális aláírás algoritmust, (***1024 bites kulcsmérettel, a PKCS#1-es szabvánnyal***), • támogatja a **DSA** digitális aláírás algoritmust (***1024 bites p prímhosszúság és 160 bites q prímhosszúság kulcsmérettel, a FIPS PUB 186-2-es szabvánnyal***).
Teljesített követelmények, értékelési eredmények (FIPS 140-1 3-as szint)	KÖV_09.01: /FIPS által jóváhagyott kriptográfiai algoritmusok alkalmazása/ KÖV_11.19: /a generált nyilvános és magán kulcsok tesztelése a páronkénti konzisztencia szempontjából/ A FIPS értékelés az alábbi digitális aláíráshoz kapcsolódó, FIPS által jóváhagyott algoritmusok megvalósítását vizsgálta, tesztelte: **DSA, RSA (PKCS #1), SHA-1**
Értékelés	A BALE képes (az RSA és DSA, minősített aláíráshoz elfogadott) szabványos kriptográfiai algoritmusok végrehajtásával az alábbi feladatokat ellátni: • a magánkulcs/nyilvános kulcs megfelelésének bizonyítása, • Az aláírandó adatok digitális aláírása.
Következtetés	A CSA8000 (a feltételek betartása esetén) **megfelel** az SSCD-PP „Kriptográfiai eljárás” követelményének.
Feltételek:	2., 8., 9., 10.

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 aláíró generálhatja (inicializáláskor), 2. az aláírás-ellenőrző adatot (nyilvános kulcsot) csak az aláíró exportálhatja (tanúsítvány generálása céljából, a minősített hitelesítés-szolgáltatóhoz), 3. a hitelesítő adatot (PIN kód) csak az adminisztrátor hozhatja létre (a megszemélyesítés fázisában). 4. az aláíró alkalmazás által küldött lenyomat értéket csak az aláíró írhatja alá.
CSA8000 tulajdonság	A CSA8000 nem két, hanem négy szerepkört támogat (a hagyományos adminisztrátori szerepkör háromfelé osztásával): • Adminisztrátori kriptográfiai tisztviselő /aki az Adminisztrátort kezdeti PIN kódja megadásával a rendszerbe lépteti/ • Adminisztrátor /aki felel a CSA8000 általános biztonságkezeléséért, valamint a slot-ok és a Token kriptográfiai tisztviselők ellenőrzéséért/ • Token kriptográfiai tisztviselő /aki felelős egy token tulajdonjogának megadásáért, illetve visszavonásáért, aki inicializálja a Token felhasználó PIN-jét. • Token felhasználó /aki saját token-jein, magán- és nyilvános kulcsait gondozhatja, illetve használhatja/ Egy BALE-ként használt CSA8000 esetén az „aláíró” a Token felhasználó, az „adminisztrátor” pedig a Token kriptográfiai tisztviselő. Ilyen szerepkör megfeleltetés, valamint a 14. Feltétel betartása esetén: • csak az „aláíró” generálhatja saját magánkulcsát, • csak az „aláíró” exportálhatja saját nyilvános kulcsát, • az aláíró PIN kódját csak az „adminisztrátor” hozhatja létre, • csak az „aláíró” írhat alá magánkulcsa aktivizálásával.
Teljesített követelmények (FIPS140-1 3.)	KÖV_03.02: /A kriptográfiai modulnak minimálisan a következő jogosult szerepköröket kell támogatnia: • Felhasználói szerepkör • Kriptográfiai tisztviselő szerepkör (a CSA8000 ez utóbbi szerepkört háromfelé bontja) /

Részleges hozzáférés ellenőrzés (FDP_ACC.1) /folytatás/	
Értékelés	Az SSCD-PP „Részleges hozzáférés ellenőrzés” követelményét a CSA8000 támogatja, a FIPS értékelés pedig igazolja (a 14. feltétel betartása esetén): • csak a Token kriptográfiai tisztviselő hozhatja létre a Token felhasználó (aláíró) kezdeti PIN kódját, • csak a Token felhasználó (aláíró) generálhatja saját magánkulcsát, • csak a Token felhasználó (aláíró) exportálhatja nyilvános kulcsát, • csak a Token felhasználó (aláíró) írhat alá saját magánkulcsával.
Következtetés	A CSA8000 (a feltételek betartása esetén) **megfelel** az SSCD-PP „Részleges hozzáférés ellenőrzés” követelményének.
Feltétel:	14.

Biztonsági jellemzőkön alapuló hozzáférés ellenőrzés (FDP_ACF.1)	
Követelmény (CC SSCD-PP)	1. A BALE az általános és inicializáló biztonsági jellemzőkre 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 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/	
CSA8000 tulajdonság	A CSA8000 az alábbi szerepköröket támogatja (a hagyományos adminisztrátori szerepkör háromfelé osztásával): • Adminisztrátori kriptográfiai tisztviselő • Adminisztrátor • Token kriptográfiai tisztviselő • Token felhasználó
Teljesített Követelmények (FIPS140-1 3.)	A FIPS 140-1 általános követelmény-rendszere nem tartalmazza a fenti speciális követelményt.
Értékelés	Egy BALE-ként használt CSA8000 esetén az „aláíró” a Token felhasználó, az „adminisztrátor” pedig a Token kriptográfiai tisztviselő. Ilyen szerepkör megfeleltetés esetén, valamint a 14. feltétel rezsim utasításainak betartása esetén: • csak az erre felhatalmazott „aláíró” vagy „adminisztrátor” generálhatja az „aláíró” magánkulcsát, • csak az „aláíró” vagy az „adminisztrátor”exportálhatja a nyilvános kulcsot, • csak az „adminisztrátor” hozhatja létre az „aláíró” PIN kódját, • csak az „aláíró” hozhat létre elektronikus aláírást.
Következtetés	A CSA8000 (a feltételek betartása esetén) **megfelel** az SSCD-PP „Biztonsági jellemzőkön alapuló hozzáférés ellenőrzés” követelményének.
Feltétel:	14.

Részleges maradvány információ védelem (FDP_RIP.1)	
Követelmény (CC SSCD-PP)	A BALE-nak biztosítania kell, hogy erőforrás visszavétel (deallokáció) után semmilyen korábbi információ tartalom ne legyen hozzáférhető az alábbi objektumokra nézve: • aláírás-létrehozó adat (magánkulcs), • hitelesítő adat (megadott PIN kód), • hitelesítést ellenőrző adat (a PIN kód tokenen tárolt képe).
CSA8000 tulajdonság	A CSA8000 szolgáltatásainak az elérése a tokeneken és a token tároló objektumain alapul. Minden objektumra attribútumok határozzák meg, hogy a kriptográfiai tisztviselők és felhasználók hozzáférhetnek-e, illetve milyen parancsokat hajthatnak rajta végre. Az adapter háromféle tároló objektumot támogat: • Rendszer objektum (az adminisztrátori token objektumai, melyek csak az adapter Adminisztrátorai számára elérhetőek) • Magán objektum (csak a Token felhasználó számára elérhető) • Nyilvános objektum (az adapter valamennyi operátora számára elérhető, de a felhasználóknak hitelesíteniük kell magukat a token felé, mielőtt kriptográfiai műveleteket végezhetnének ezekkel az objektumokkal.) Az aláíró magánkulcsa és a hitelesítést ellenőrző adat (PIN kód tokenen tárolt képe) magán objektum, így csak a Token felhasználó (aláíró) számára elérhető. A hitelesítő adat (megadott PIN kód) megbízható útvonalon, titkosítva jut a CSA8000 adapterbe. Itt dekódolásra kerül, s a sikeres hitelesítés után automatikusan törlődik, így a későbbiekben senki sem férhet hozzá.
Teljesített követelmények (FIPS140-1 3.)	Modul interfészek / KÖV_02.01 - KÖV_02.14/ • a kriptográfiai modul interfészein belül logikailag elkülönülnek az adat input, adat output, vezérlési input, státusz output, valamint elektromos áram interfészek. • a kriptográfiai modul egyáltalán nem enged hozzáférést belső memóriáihoz, az adat és vezérlési input interfészeken keresztül kapott adatok és parancsok feldolgozása után az adat és státusz output interfészeken keresztül küldi vissza a parancsokra adandó helyes választ vagy hibajelzést.
Értékelés	A FIPS 140-1 (teljes) maradvány információ védelmet biztosít, a modul interfészek elkülönítésével, illetve a modullal való kommunikáció (parancs – válasz) szerkezetével. A CSA8000 megfelel a FIPS 140-1 modul interfészekre vonatkozó követelményeinek.
Következtetés	A CSA8000 **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 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).
CSA8000 tulajdonság	A CSA8000 a folyamatosan tárolt kritikus adatokra (köztük a Token felhasználó (aláíró) magán és nyilvános kulcsára, a PIN kód tárolt képére): • védett memóriában tárolja ezen adatokat, • minden bekapcsoláskor, illetve minden kriptográfiai hardver használat esetén ellenőrzi a védett memóriatartalom sértetlenségét, • integritás hiba esetén egy biztonságos hibaállapotba kerül, melyről értesíti a felhasználókat is. A CSA8000 a parancsokban kívülről kapott, átmenetileg tárolt adatokra (köztük az aláírandó adat reprezentánsra is): • ellenőrzi a kapott adatok sértetlenségét, • azonnal feldolgozza azokat.
Teljesített követelmények (FIPS140-1 3.)	A FIPS értékelés igazolja a fenti tulajdonságokat.
Értékelés	A CSA8000 valamennyi tárolt adatára biztosítja a sértetlenség figyelését (beavatkozás mellett). A 3. feltétel betartása esetén (FIPS által előírt kötelező beállítás) valamennyi kívülről kapott adatra is ellenőrzi a sértetlenséget (s beavatkozik, hiba esetén).
Következtetés	A CSA8000 (a feltételek betartása esetén) **megfelel** az SSCD-PP „A tárolt adatok sértetlenségének figyelése és beavatkozás” követelményének.
Feltétel:	3. /“Session Protection” flag kötelező értéke: TRUE/

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.
CSA8000 tulajdonság	A CSA8000 megbízható csatornát képes kiépíteni, melyen keresztül az operátorok (köztük az aláíró) biztonságosan kommunikálhatnak a PCI busz interfészen keresztül a modullal. A megbízható csatornák munkaszakasz kulcsokat használnak az üzenetek (HMAC DES algoritmussal történő) digitális aláírására / a digitális aláírás ellenőrzésére.
Teljesített követelmények (FIPS140-1 3.)	A FIPS 140-1 nem tartalmazza a fenti követelményt. Azt viszont elvárja, hogy ha a hitelesítési adatokat nyílt formában adják meg, akkor arra fizikailag elkülönített portot használjanak /KÖV_03.20/
Értékelés	A CSA8000 FIPS üzemmódjában kötelező a megbízható csatornák kiépítése és használata. A megbízható csatornán minden adat (tehát az SSCD-PP által megkövetelt nyilvános kulcs és aláírandó adat reprezentáns is) védve van a módosításból, törlésből és beszúrásból eredő hibákkal szemben.
Következtetés	A CSA8000 (a feltételek betartása esetén) **megfelel** az SSCD-PP „Az adat-csere sértetlensége” követelményének.
Feltétel:	3.

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.
CSA8000 tulajdonság	A CSA8000 a sikertelen hitelesítési kísérletek megakadályozása érdekében az alábbi ellenintézkedéseket valósítja meg: A CSA8000 képes detektálni, ha három sikertelen, egymást követő hitelesítési kísérlet történt. A meghatározott számú (három) vagy ennél több sikertelen hitelesítési kísérlet bekövetkezése esetén a CSA8000 a következő ellenintézkedéseket valósítja meg: A három sikertelen hitelesítési kísérletet követő minden további sikertelen kísérlet öt másodperccel késlelteti a következő hitelesítés megkezdését (azaz: egy 5 másodperces késleltetést iktat be a 3. és a 4. hitelesítési kísérlet közé, egy 10 másodperces késleltetést iktat be a 4. és az 5. hitelesítési kísérlet közé, egy 15 másodperces késleltetést iktat be az 5. és a 6. hitelesítési kísérlet közé, stb.)
Teljesített követelmények (FIPS140-1 3.)	A FIPS 140-1 nem tartalmazza a fenti követelményt. Csak az azonosságon alapuló (egyedi) hitelesítést követeli meg. Erre a PIN kód egy lehetséges példa.
Értékelés	A Common Criteria a FIA_AFL.1 funkcionális biztonsági követelményt általánosan az alábbi módon fogalmazza meg: A BALE legyen képes detektálni, ha ***[behelyettesítés: egy meghatározott szám]*** sikertelen hitelesítési kísérlet történt az alábbiakra vonatkozóan: ***[behelyettesítés: hitelesítési események listája].*** A meghatározott számú vagy ennél több sikertelen hitelesítési kísérlet bekövetkezése esetén a BALE hajtsa végre az alábbiakat: ***[behelyettesítés: ellenintézkedések listája].*** Az SSCD védelmi profil a fenti általános követelményben szereplő 3 nyitott műveletet lezárt, konkrétan megkövetelve az egymást követő sikertelen kísérletek közös kezelését, illetve az ellenintézkedéseket a PIN kód blokkolására pontosítva. A CSA8000 teljesíti a CC általános FIA_AFL.1 követelményét. Pontosan megfelel az SSCD védelmi profil nyitott művelet lezárásának is az első esetben. Kicsit eltér a második művelet lezárással: nem blokkolja a PIN kódot 3 hitelesítési kísérlet után, hanem (5-5 másodperccel növelt, akkumulált késéssel) lassítja a sikertelen kísérletek végrehajtási lehetőségét. A fenti késleltetés megfelelő nagy PIN kód választék esetén gyakorlatilag blokkolja a sikertelen kísérletek végrehajtását: az 1000. sikertelen hitelesítési kísérlet után közel 29 napos, az 1000000. sikertelen kísérlet után közel 80000 év késleltetést okozva.
Következtetés	A CSA8000 (a feltételek betartása esetén) **megfelel** az SSCD-PP „A hitelesítési hiba kezelése” követelményének.
Feltétel:	3., 6., 7.

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.
CSA8000 tulajdonság	A CSA8000 képes kezelni a PIN kódot, valamennyi szerepkörhöz tartozóan (így a Token felhasználóra, vagyis az aláíróra is).
Teljesített követelmények (FIPS140-1 3.)	A FIPS 140-1 nem tartalmazza a fenti követelményt. Csak az azonosságon alapuló (egyedi) hitelesítést követeli meg. Erre a PIN kód kezelése csak egy lehetséges példa.
Értékelés	A CSA8000 PIN kód kezelését a FIPS értékelés is igazolja.
Következtetés	A CSA8000 (a feltételek betartása esetén) **megfelel** az SSCD-PP „A felhasználói jellemzők meghatározása” követelményének.
Feltétel:	3., 6., 7.

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[61].
CSA8000 tulajdonság	A CSA8000 megbízható csatornát képes kiépíteni, melyen keresztül az operátorok (köztük az aláíró) biztonságosan kommunikálhatnak a PCI busz interfészen keresztül a modullal. A megbízható csatornák munkaszakasz kulcsokat használnak az üzenetek (HMAC DES algoritmussal történő) digitális aláírására / a digitális aláírás ellenőrzésére.
Teljesített követelmények (FIPS140-1 3.)	A FIPS 140-1 direkt formában nem tartalmazza a fenti követelményt. Azt viszont elvárja, hogy a kriptográfiai modul azonosságon alapuló hitelesítési mechanizmusokat (pl. az operátor azonosításán alapuló mechanizmust) alkalmazzon abból a célból, hogy az operátor jogosultságát ellenőrizze arra vonatkozóan, hogy a kívánt szerepköröket betölthesse és az annak megfelelő szolgáltatásokat igényelhesse. /KÖV_03.20/ Ebben indirekten benne van, hogy szerepkör betöltése és az ennek megfelelő szolgáltatások igénylése csak a sikeres azonosítás után legyen lehetséges. Egy megbízható útvonal vagy csatorna előzetes létesítése egyrészt szükséges a biztonságos azonosításhoz, másrészt még nem jár szerepkör betöltéssel, szolgáltatás igénylésével, így nem mond ellent KÖV_03.20-nek.
Értékelés	A CSA8000 FIPS üzemmódjában kötelező a megbízható csatornák kiépítése és használata. A kiépített megbízható csatornán jut át az aláíró PIN kódja, mely nemcsak hitelesíti, hanem egyben azonosítja is tulajdonosát. A CSA8000 bármilyen további, általa közvetített tevékenységet csak akkor engedélyez, ha az aláíró már sikeresen azonosította magát.
Következtetés	A CSA8000 (a feltételek betartása esetén) **megfelel** az SSCD-PP „Az azonosítás időzítése” követelményének.
Feltétel:	3.

[61] 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[62].
CSA8000 tulajdonság	A CSA8000 megbízható csatornát képes kiépíteni, melyen keresztül az operátorok (köztük az aláíró) biztonságosan kommunikálhatnak a PCI busz interfészen keresztül a modullal. A megbízható csatornák munkaszakasz kulcsokat használnak az üzenetek (HMAC DES algoritmussal történő) digitális aláírására / a digitális aláírás ellenőrzésére.
Teljesített követelmények (FIPS140-1 3.)	A FIPS 140-1 direkt formában nem tartalmazza a fenti követelményt. Azt viszont elvárja, hogy a kriptográfiai modul azonosságon alapuló hitelesítési mechanizmusokat (pl. az operátor azonosításán alapuló mechanizmust) alkalmazzon abból a célból, hogy az operátor jogosultságát ellenőrizze arra vonatkozóan, hogy a kívánt szerepköröket betölthesse és az annak megfelelő szolgáltatásokat igényelhesse. /KÖV_03.20/ Ebben indirekten benne van, hogy szerepkör betöltése és az ennek megfelelő szolgáltatások igénylése csak a sikeres azonosítás és hitelesítés után legyen lehetséges. Egy megbízható útvonal vagy csatorna előzetes létesítése egyrészt szükséges a biztonságos azonosításhoz és hitelesítéshez, másrészt még nem jár szerepkör betöltéssel, szolgáltatás igénylésével, így nem mond ellent KÖV_03.20-nek.
Értékelés	A CSA8000 FIPS üzemmódjában kötelező a megbízható csatornák kiépítése és használata. A kiépített megbízható csatornán jut át az aláíró PIN kódja, mely hitelesíti tulajdonosát. A CSA8000 bármilyen további, általa közvetített tevékenységet csak akkor engedélyez, ha az aláíró már sikeresen hitelesített magát.
Következtetés	A CSA8000 (a feltételek betartása esetén) **megfelel** az SSCD-PP „Az azonosítás időzítése” követelményének.
Feltétel:	3.

[62] 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.
CSA8000 tulajdonság	A CSA8000 minden felhasználói tokenen csak a Token felhasználó számára teszi elérhetővé az adott Token felhasználó saját magánkulcsainak aktivizálását. Következésképpen csak az aláíró képes aktivizálni saját aláíró magánkulcsát.
Teljesített követelmények (FIPS140-1 3.)	A FIPS 140-1 általános követelmény-rendszere nem tartalmazza a fenti speciális követelményt.
Értékelés	A CSA8000 általánosan kielégíti a követelményt.
Következtetés	A CSA8000 (a feltételek betartása esetén) **megfelel** az SSCD-PP „A biztonsági funkciók viselkedésének kezelése” követelményének.
Feltétel:	14.

A biztonsági jellemzők kezelése (FMT_MSA.1)	
Követelmény (CC SSCD-PP)	A BALE legyen képes: • az „inicializálás” funkció „magán-nyilvános kulcspár kezelés” biztonsági jellemzőjének módosítási lehetőségét az adminisztrátorra korlátozni, • az „aláírás-létrehozás” funkció „magánkulcs működtetése (aláírás)” biztonsági jellemzőjének módosítási lehetőségét az aláíróra korlátozni.
CSA8000 tulajdonság	A 14. Feltétel betartása esetén csak az „adminisztrátor” adhatja meg (az „aláíró” PIN kódjának átadásával) a jogot az „aláíró”-nak a kulcspár generálásra. Az adminisztrátor ezt a jogot vissza is veheti, amennyiben újra inicializálja a tokent (s ezzel minden magán objektumot el is töröl a tokenen) /„Reset (re-imitialise) Normal Token”/. A 14. feltétel betartása esetén csak az „aláíró képes magánkulcsa legenerálásával az aláírás lehetőségét saját maga számára biztosítani. Saját magánkulcsának megsemmisítésével „Destroy Private Objects on a Normal Token” ezt a jogát vissza is veheti (bár ez a visszavétel már megfordíthatatlan, mert véglegesen törli a magánkulcsot).
Teljesített követelmények (FIPS140-1 3.)	A FIPS 140-1 általános követelmény-rendszere nem tartalmazza a fenti speciális követelményt.
Értékelés	A CSA8000 közvetlenül nem támogatja a BALE-ra elvárt, a biztonsági jellemzők módosítási lehetőségére vonatkozó fenti követelményt. Ugyanakkor a CSA8000 által biztosított általános szerepkörök jogosultság elkülönítésével, valamint a 14. feltétel rezsim utasításaival az elvárás teljesíthető.
Következtetés	A CSA8000 (a feltételek betartása esetén) **megfelel** az SSCD-PP „A biztonsági jellemzők kezelése” követelményének.
Feltétel:	14.

Biztonságos biztonsági jellemzők (FMT_MSA.2)	
Követelmény (CC SSCD-PP)	A BALE biztosítsa, hogy biztonsági jellemzőknek csak biztonságos értékek lesznek elfogadva.
CSA8000 tulajdonság	A CSA8000 FIPS üzemmódban meghatározott, biztonságos értékeket fogad csak el biztonsági jellemzőknek.
Teljesített követelmények (FIPS140-1 3.)	A FIPS 140-1 általános követelmény-rendszere nem tartalmazza a fenti speciális követelményt.
Értékelés	A FIPS értékelés tartalmazta ezt az elvárást, s meg is határozza a kötelezőn beállítandó biztonsági jellemzők körét, s a beállítandó biztonságos értékeket. A kötelezően elvárt FIPS üzemmód arról is gondoskodik, hogy a későbbiekben ez az értékbeállítás ne legyen módosítható, elrontható.
Következtetés	A CSA8000 (a feltételek betartása esetén) **megfelel** az SSCD-PP „Biztonságos biztonsági jellemzők” követelményének.
Feltétel:	3. /különböző flag értékek beállításának meghatározásával, köztük a ”Lock Security Mode” flag kötelező: TRUE érték beállításával/

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 („igen”-re állítsa a megszemélyesítés folyamán).
CSA8000 tulajdonság	A CSA8000 ezt a konkrét követelményt nem támogatja.
Teljesített követelmények (FIPS140-1 3.)	A FIPS 140-1 általános követelmény-rendszere nem tartalmazza a fenti speciális követelményt.
Értékelés	A CSA8000 közvetlenül nem támogatja a BALE-ra elvárt fenti követelményt. Ugyanakkor a CSA8000 által biztosított általános szerepkörök jogosultság elkülönítésével, valamint a 14. feltétel rezsim utasításaival az elvárás teljesíthető.
Következtetés	A CSA8000 (a feltételek betartása esetén) **megfelel** az SSCD-PP „Statikus jellemző inicializálás” követelményének.
Feltétel:	14.

A biztonsági funkciók adatainak kezelése (FMT_MTD.1)	
Követelmény (CC SSCD-PP)	A BALE a hitelesítő adatok (PIN kód) módosításának lehetőségét az aláíróra korlátozza.
CSA8000 tulajdonság	A CSA8000 a Token felhasználóra korlátozza a Token felhasználó saját PIN kódjának módosítási lehetőségét. A 14. feltétel betartása esetén az „aláíró” a Token felhasználó lesz.
Teljesített követelmények (FIPS140-1 3.)	A FIPS 140-1 általános követelmény-rendszere nem tartalmazza a fenti speciális követelményt.
Értékelés	A CSA8000 teljesíti az elvárást, a FIPS értékelés igazolja ezt.
Következtetés	A CSA8000 (a feltételek betartása esetén) **megfelel** az SSCD-PP „A biztonsági funkciók adatainak kezelése” követelményének.
Feltétel:	14.

Biztonsági szerepkörök (FMT_SMR.1)	
Követelmény (CC SSCD-PP)	A BALE legyen képes az alábbi szerepek kezelésére: adminisztrátor, aláíró. A BALE legyen képes összekapcsolni a felhasználókat az egyes szerepekkel.
CSA8000 tulajdonság	A CSA8000 az alábbi szerepköröket támogatja (a hagyományos adminisztrátori szerepkör háromfelé osztásával): • Adminisztrátori kriptográfiai tisztviselő • Adminisztrátor • Token kriptográfiai tisztviselő • Token felhasználó
Teljesített követelmények (FIPS140-1 3.)	KÖV_03.02: /A kriptográfiai modulnak minimálisan a következő jogosult szerepköröket kell támogatnia: • Felhasználói szerepkör, • Kriptográfiai tisztviselő szerepkör./
Értékelés	Egy BALE-ként használt CSA8000 esetén az „aláíró” a Token felhasználó, az „adminisztrátor” pedig a Token kriptográfiai tisztviselő. A felhasználók összekapcsolását az egyes szerepekkel a CSA8000 támogatja, a FIPS értékelés pedig igazolja.
Következtetés	A CSA8000 (a feltételek betartása esetén) **megfelel** az SSCD-PP „A biztonsági szerepkörök” követelményének.
Feltétel:	14.

Az absztrakt gép tesztelése (FPT_AMT.1)	
Követelmény (CC SSCD-PP)	A BALE ***[választás: a kezdeti rendszer indítás során; a normál működés során periodikusan; egy jogosult felhasználó kérelme esetén; más feltételek fellépésekor]*** hajtson végre egy olyan teszt-sorozatot, mely kimutatja, hogy helyesen működik a BALE alapját képező absztrakt gép.
CSA8000 tulajdonság	A CSA8000 összetevői helyes működésének ellenőrzése céljából ön-tesztek sorát képes megvalósítani a modul áram alá helyezési szakaszában (bekapcsoláskor, a kezdeti rendszer indítás során). Az áram alá helyezési tesztek magukba foglalják a következőket: • "ismert eredmény teszt"-ek a modul által támogatott valamennyi kriptográfiai algoritmusra, • szoftver (förmver) integritás teszt (32 bites hiba detektáló kódot és SHA-1 lenyomatoló függvényt használva), • statisztikus véletlenszám generátor tesztek, • egyéb kritikus funkciók tesztjei (köztük minden funkcionális modulra ellenőrző összeg számítás, valamint a RAM-ra, biztonságos memóriára, belső órára és a soros kommunikációs eszközökre elvégzett hardver ellenőrzések).
Teljesített követelmények (FIPS140-1 3.)	KÖV_11.05: Miután egy kriptográfiai modult áram alá helyeztek, a modulnak ön-teszt állapotba kell kerülnie, és legalább a következő (áram alá helyezési) teszteket végre kell hajtania: • kriptográfiai algoritmus teszt, • szoftver/förmver teszt, • a kritikus műveletek tesztje és • a statisztikus véletlenszám generátor tesztek.
Értékelés	A CSA8000 támogatja, a FIPS értékelés pedig igazolja a BALE alapját képező absztrakt gép kezdeti tesztelését.
Következtetés	A CSA8000 **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.
CSA8000 tulajdonság	Nem találtunk bizonyítékokat arra nézve, hogy a CSA8000 teljesíti a fenti követelményt.
Teljesített követelmények (FIPS140-1 3.)	A FIPS 140-1 nem tartalmazza a fenti követelményt. Azt viszont elvárja, hogy a kriptográfiai modul általános kisugárzása kellően alacsony legyen /KÖV_10.03/.
Értékelés	A CSA8000 FIPS értékelési eredményei, illetve dokumentációi nem térnek ki arra, hogy a kriptográfiai modul megakadályozza biztonságkritikus adatainak (köztük az aláíró magánkulcsa, PIN kódja) megismerését lehetővé tévő kisugárzást. Ezért ezen tulajdonságokat nem tételezhetjük fel a CSA8000 kriptográfiai adapterről. A 15. feltétel betartása esetén ugyanakkor az ilyen típusú támadásokat gyakorlatilag nem lehet kivitelezni, ezért ilyen körülmények között a CSA8000 alkalmazható BALE-ként. Megjegyezzük, hogy a 15. feltétel intelligens kártyákra (a tipikus BALE megvalósítási formára) nem tételezhető fel, de a CSA8000 adapterre betartható.
Következtetés	A CSA8000 (a 15. feltétel betartása esetén) **megfelel** az SSCD-PP „A BALE kisugárzása” követelményének.
Feltétel:	15.

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]***
CSA8000 tulajdonság	A CSA8000 megőriz egy biztonságos állapotot, ha a következő típusú hibák lépnek fel: • integritás hiba. (lásd „A tárolt adatok sértetlenségének figyelése és beavatkozás (FDP_SDI.2)” követelményt), • az órafrekvencia kilépése egy alulról és felülről is korlátozott tartományból (mivel saját belső órafrekvenciát használ).
Teljesített követelmények (FIPS140-1 3.)	A FIPS 140-1 nem tartalmazza a fenti követelményt. Ugyanakkor elvárja az alábbiakat: KÖV_04.07: Bármilyen hiba állapot esetén az adat output interfészen keresztül történő minden adat outputot le kell tiltani. KÖV_04.08: Minden hiba állapotnak olyannak kell lenni, hogy azt vissza lehessen állítani (reset) egy elfogadható működési állapotba vagy kezdeti állapotba, kivéve azokat a nem helyrehozható (hard) hibákat, amelyek a modul karbantartását, szervizelését vagy javítását igénylik.
Értékelés	A CSA8000 FIPS értékelési eredményei alapján a kriptográfiai modul megőriz egy biztonságos állapotot integritás hiba esetén, illetve alacsony és magas órafrekvenciával való manipulálás ellen. A 15. feltétel betartása esetén más tipikus támadási formákat (szokatlanul alacsony vagy magas áramerősséggel, áramfeszültséggel való manipulálás) sem lehet a gyakorlatban megvalósítani. Ezért ilyen körülmények között a CSA8000 alkalmazható BALE-ként. Megjegyezzük, hogy a 15. feltétel intelligens kártyákra (a tipikus BALE megvalósítási formára) nem tételezhető fel, de a CSA8000 adapterre betartható.
Következtetés	A CSA8000 (a feltételek betartása esetén) **megfelel** az SSCD-PP „A biztonságos állapot megőrzése hiba esetén” követelményének.
Feltétel:	15.

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.
CSA8000 tulajdonság	A CSA8000 kriptográfiai adaptert egy polikarbonátból készült erős borítás védi, mely alatt nyomásérzékelő mikrokapcsolók és érzékelők vannak elhelyezve. A borítás bármely részének megbontása a biztonságkritikus paramétereket (kulcsok és PIN kódok) tartalmazó memória nullázását eredményezi. A modul áramellátási állapotától függően ez a nullázódás kétfélképpen következik be: • bekapcsolt állapotban az eszköz minden biztonságkritikus paramétert felülír, • kikapcsolt állapotban pedig a tartalék (elem) áramforrás leszakad a RAM-ról.
Teljesített követelmények (FIPS140-1 3.)	A FIPS 140-1 is elvárja a fenti követelményt. KÖV_05.09 Több chip-es, beágyazott kriptográfiai modul esetében a modult egy nem átlátszó, beavatkozást kimutató anyaggal kell beburkolni. KÖV_05.11 Több chip-es, beágyazott kriptográfiai modul esetében, ha a modul valamilyen szellőzőnyílást tartalmaz, azt olyan módon kell megtervezni, hogy az meggátoljon minden észrevétlen szondázást.
Értékelés	A CSA8000 védő borítása alkalmas az ellene irányuló fizikai támadások észlelésére, sőt a kritikus biztonsági paraméterek megismerését meg is akadályozza ilyen esetekben.
Következtetés	A CSA8000 **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.
CSA8000 tulajdonság	A CSA8000 az alábbi két támadási forgatókönyv esetén biztosít ellenálló képességet: • keresztülhatolás a védelmi rétegen (A CSA8000 esetében a FIPS 140-1 KÖV_05.10-ben szereplő alternatívák közül a 3. megoldást alkalmazzák: az adapter egy polikarbonátból készült erős borítást kapott, mely alatt nyomásérzékelő mikrokapcsolók és érzékelők vannak elhelyezve. A borítás bármely részének megbontása a biztonságkritikus paramétereket (kulcsok és PIN kódok) tartalmazó memória nullázását eredményezi. • Külső órafrekvencia manipulálás (a CSA8000 saját belső órafrekvencia forrással rendelkezik, ennek alapján működik).
Teljesített követelmények (FIPS140-1 3.)	A FIPS 140-1 is elvár fizikai támadásokkal szembeni ellenálló képességet, döntően a védelmi rétegen való keresztülhatolás ellen: KÖV_05.10 Több chip-es, beágyazott kriptográfiai modul esetében a következő három követelmény egyikét kell alkalmazni a modulra: 1. egy kemény, nem átlátszó kiöntő anyagot kell alkalmazni, 2. a modult egy erős, nem eltávolítható burkoló anyagnak kell tartalmaznia, 3. a modult egy erős, eltávolítható burkolatba kell bezárni, és tartalmaznia kell beavatkozásra reagáló és nullázó áramköri egységet.
Értékelés	A CSA8000 védő borítása ellenáll a „keresztülhatolás a védelmi rétegen” típusú fizikai támadásoknak. A CSA8000 ezen kívül ellenáll a „külső órafrekvencia manipulálás”-nak. A 15. feltétel betartása esetén más tipikus támadási formákat (szokatlanul alacsony vagy magas áramerősséggel, áramfeszültséggel való manipulálás) sem lehet a gyakorlatban megvalósítani. Ezért ilyen körülmények között a CSA8000 alkalmazható BALE-ként. Megjegyezzük, hogy a 15. feltétel intelligens kártyákra (a tipikus BALE megvalósítási formára) nem tételezhető fel, de a CSA8000 adapterre betartható.
Következtetés	A CSA8000 (a feltételek betartása esetén) **megfelel** az SSCD-PP „A fizikai támadásokkal szembeni ellenálló képesség” követelményének.
Feltétel:	15.

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.
CSA8000 tulajdonság	A CSA8000 összetevői helyes működésének ellenőrzése céljából ön-tesztek sorát képes megvalósítani a modul áram alá helyezési szakaszában (bekapcsoláskor, a kezdeti rendszer indítás során). Az áram alá helyezési tesztek magukba foglalják a következőket: • "ismert eredmény teszt"[63]ek a modul által támogatott valamennyi kriptográfiai algoritmusra, • szoftver (förmver) integritás teszt (32 bites hiba detektáló kódot és SHA-1 lenyomatoló függvényt használva), • statisztikus véletlenszám generátor tesztek, • egyéb kritikus funkciók tesztjei (köztük minden funkcionális modulra ellenőrző összeg számítás, valamint a RAM-ra, biztonságos memóriára, belső órára és a soros kommunikációs eszközökre elvégzett hardver ellenőrzések). A fentieken kívül a CSA8000 a folyamatosan tárolt kritikus adatokra (köztük a biztonsági funkció adatokra): • védett memóriában tárolja ezen adatokat, • minden bekapcsoláskor, illetve minden kriptográfiai hardver használat esetén ellenőrzi a védett memóriatartalom sértetlenségét, • integritás hiba esetén egy biztonságos hibaállapotba kerül, melyről értesíti a felhasználókat is.

[63] Ilyenkor az algoritmust olyan adatokon hajtják végre, melyekre a helyes output már előzetesen ismert. A teszt akkor sikeres, ha az aktuálisan kiszámított output megegyezik a korábban generált outputtal.

A biztonsági funkciók tesztelése (FPT_TST.1) /folytatás/	
Teljesített követelmények (FIPS140-1 3.)	Az első elvárás egyben FIPS 140-1 követelmény is: KÖV_11.05 Miután egy kriptográfiai modult áram alá helyeztek, a modulnak önteszt állapotba kell kerülnie, és legalább a következő (áram alá helyezési) teszteket végre kell hajtania: • kriptográfiai algoritmus teszt, • szoftver/förmver teszt, • a kritikus műveletek tesztje és • a statisztikus véletlenszám generátor tesztek. Az SSCD-PP másik két elvárása nem szerepel a FIPS 140-1 tételes követelményei között. Ugyanakkor (mivel a feljogosított felhasználóknak megkívánt ellenőrzési lehetőségek részét képezik a bekapcsoláskor automatikusan megvalósuló tesztelésnek) egy kikapcsolással és újra indítással a másik két elvárás is teljesíthető.
Értékelés	A kezdeti rendszer indítás során elvárt tesztelési követelmények teljesülnek. A biztonsági funkció adatok sértetlenségének ellenőrzésére is sor kerül minden kriptográfiai hardver használat esetén. A felhasználók a CSA8000 kikapcsolásával és újra indításával elvileg kiválthatják a végrehajtható kódok sértetlenségének ellenőrzését is.
Következtetés	A CSA8000 **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 IT termék ***(a tanúsítvány generáló 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 ***[választás: a BALE, a távoli IT termék]*** kezdeményezze. A BALE ***vagy a távoli IT 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 IT 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 IT termék (az aláírás-létrehozó alkalmazás)*** kezdeményezze. A BALE ***vagy a távoli IT termék (az aláírás-létrehozó alkalmazás)*** ezen a biztonságos csatornán kezdeményezzen kommunikációt az alábbi esetekhez: • aláírandó adat reprezentáns fogadása (az aláírás-létrehozó alkalmazástól).
CSA8000 tulajdonság	A CSA8000 megbízható csatornát képes kiépíteni, melyen keresztül a CSA8000 szolgáltatásait felhívó programok (köztük a tanúsítvány-létrehozó alkalmazás és az aláírás-létrehozó alkalmazás) biztonságosan kommunikálhatnak a PCI busz interfészen keresztül a modullal. A megbízható csatornák munkaszakasz kulcsokat használnak az üzenetek titkosítására/dekódolására, illetve digitális aláírására/a digitális aláírás ellenőrzésére. FIPS üzemmódban kötelező a megbízható csatornák kiépítése és használata

Megbízható csatorna (FTP_ITC.1) /folytatás/ /A tanúsítvány-létrehozó alkalmazás, illetve az aláírás-létrehozó alkalmazás felé./	
Teljesített követelmények (FIPS140-1 3.)	A FIPS 140-1 indirekt módon tartalmazza a fenti követelményt. KÖV_02.13: A nyíltan megjelenő kriptográfiai adatokhoz, nyíltan megjelenő hitelesítési adatokhoz és más, nem védett kritikus biztonsági paraméterekhez alkalmazott adat input és output portoknak fizikailag el kell különülniük a modul összes többi portjától. Minthogy a CSA8000 nem biztosít fizikailag elkülönített input és output portokat a hitelesítési adatok és más kritikus biztonsági paraméterek számára (csak a PCI busz interfészen keresztül lehetővé téve a kommunikációt) adódik az indirekt követelmény: nem szabad nyíltan kiadni és fogadni a hitelesítési adatokat és más kritikus biztonsági paramétereket.
Értékelés	A CSA8000 FIPS üzemmódjában kötelező a megbízható csatornák kiépítése és használata. A megbízható csatornán minden adat (tehát az SSCD-PP által megkövetelt nyilvános kulcs kiadás és aláírandó adat reprezentáns fogadás is) védve van a módosításból, törlésből és beszúrásból eredő hibákkal szemben.
Következtetés	A CSA8000 (a feltételek betartása esetén) **megfelel** az SSCD-PP „Megbízható csatorna” követelményének.
Feltétel:	3. /“No Clear PINs” flag kötelező értéke: TRUE, “Session Protection” flag kötelező értéke: TRUE/

Megbízható útvonal (FTP_TRP.1) /A helyi felhasználók 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]]***.
CSA8000 tulajdonság	A CSA8000 megbízható csatornát képes kiépíteni, melyen keresztül a CSA8000 szolgáltatásait felhívó programok (köztük a hitelesítő adatokat az „aláíró”-tól bekérő aláírás-létrehozó alkalmazás) biztonságosan kommunikálhatnak a PCI busz interfészen keresztül a modullal. FIPS üzemmódban a CSA8000 ezt a megbízható csatornát használja a hitelesítési adatok védett továbbítására, mint megbízható útvonal. A megbízható útvonal munkaszakasz kulcsokat használ az üzenetek titkosítására/dekódolására, illetve digitális aláírására/a digitális aláírás ellenőrzésére. FIPS üzemmódban kötelező a megbízható útvonal kiépítése és használata.
Teljesített követelmények (FIPS140-1 3.)	A FIPS 140-1 indirekt módon tartalmazza a fenti követelményt. KÖV_02.13: A nyíltan megjelenő kriptográfiai adatokhoz, nyíltan megjelenő hitelesítési adatokhoz és más, nem védett kritikus biztonsági paraméterekhez alkalmazott adat input és output portoknak fizikailag el kell különülniük a modul összes többi portjától. Minthogy a CSA8000 nem biztosít fizikailag elkülönített input és output portokat a hitelesítési adatok és más kritikus biztonsági paraméterek számára (csak a PCI busz interfészen keresztül lehetővé téve a kommunikációt) adódik az indirekt követelmény: nem szabad nyíltan kiadni és fogadni a hitelesítési adatokat és más kritikus biztonsági paramétereket.
Értékelés	A CSA8000 FIPS üzemmódjában kötelező a megbízható útvonal kiépítése és használata. A megbízható útvonalon minden adat (tehát az SSCD-PP által megkövetelt első PIN kód, PIN kód és csere PIN kód is) védve van a módosításból, törlésből és beszúrásból eredő hibákkal szemben.
Következtetés	A CSA8000 (a feltételek betartása esetén) **megfelel** az SSCD-PP „Megbízható útvonal” követelményének.
Feltétel:	3. /“No Public Cryptography” flag kötelező értéke: TRUE/**,** 14. (helyi felhasználó)

9.2 A CSA8000 megfelelése az SSCD védelmi profil garanciális biztonsági követelményeinek

A FIPS 140-1 3-as biztonsági szintje /Level 3/ közvetlenül nem feleltethető meg a Közös szempontrendszer 4-es értékelési garancia szintjének. /Common Criteria EAL4/.

A FIPS 140-1 továbbfejlesztése (a FIPS 140-2) már közvetlenül összehasonlítható a Common Criteria garanciális elvárásaival, minthogy a követelményei közé felvett egy új követelmény osztályt (Tervezési garanciák) az alábbi elvárásokkal:

- A konfiguráció menedzselése, mely megfelel a Common Criteria ACM /A konfiguráció menedzselése/ garancia családjának,
- Kiszállítás és üzemeltetés, mely megfelel a Common Criteria ADO /Kiszállítás és üzemeltetés/ garancia családjának,
- Fejlesztés, mely megfelel a Common Criteria ADV /Fejlesztés/ garancia családjának,
- Útmutató dokumentumok, mely megfelel a Common Criteria AGD /Útmutató dokumentumok/ garancia családjának,
- A működés tesztelése és ennek kiterjedtsége, mely megfelel a Common Criteria ATE /Tesztelés/ garancia családjának.

Ugyanakkor számos meghatározó dokumentum, köztük az alábbiak is:

- ETSI TS 101 456: Policy Requirements for Certification Authorities Issuing Qualified Certificates
- CEN 14167-1 munkacsoport egyezmény: Security Requirements for Trustworthy Systems Managing Certificates for Electronic Signatures
- 2/2002. (IV. 26.) MeHVM irányelv a minősített elektronikus aláírással kapcsolatos szolgáltatásokra és ezek szolgáltatóira vonatkozó biztonsági követelményekről

az alábbi megfeleltetéseket teszi a FIPS 140-1 és a Common Criteria (ISO/IEC 15408) garancia szintjei között:

FIPS 140-1	ISO/IEC 15408
Level 1	EAL 2
Level 2	EAL 3
Level 3	**EAL 4**

A fenti táblázat utolsó sorát elfogadva, adódik a CSA8000 megfelelése az SSCD védelmi profil garanciális biztonsági követelményeinek.

A 9.1 alfejezetben kimutattuk, hogy a CSA8000 megfelel a két „BALE specifikus” védelmi profil funkcionális biztonsági követelményének. A garanciális biztonsági követelményekre vonatkozó FIPS Level 3 --- ISO/IEC 15408 EAL4 megfeleltetést is figyelembe véve, adódik tanúsítási jelentésünk első döntő következtetése:

A CSA8000 kriptográfiai adapter megfelel a 3-as típusú BALE-re vonatkozó (a garanciális biztonság szempontjából kevésbé szigorú) **védelmi profilnak:**
Protection Profile – Secure Signature-Creation Device Type 3, version: 1.05, EAL4.

10. A Tanúsítási jelentés eredménye, érvényességi feltételei

10.1 A Tanúsítási jelentés eredménye

A CSA8000 kriptográfiai adapter
/Eracom Technologies Group, Eracom Technologies Australia, Pty. Ltd./

tanúsítás tárgyát képező verziója
/hardver verzió: G revízió,
Cprov förmver verzió: 1.10/

a tanúsítás érvényességi feltételeinek[64] együttes teljesülése esetén

ALKALMAS

minősített aláírások létrehozására,

mint

a kriptográfiai adapterhez közvetlenül hozzáférő
több felhasználó (aláíró)
közös
3-as típusú biztonságos aláírás-létrehozó eszköze.

[64] Lásd a 10.2 "Az eredmények érvényességi feltételei" alfejezet 1.-20 feltételeit.

10.2 Az eredmények érvényességi feltételei

A CSA8000 adapter 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.

A FIPS 140-1-nek megfelelő módú működtetés (mely a biztonságra helyezi a hangsúlyt, sokszor a hatékonyság és a felhasználói kényelem rovására) számos konfigurációs beállítást megkövetel, s ezek betartása feltétele a tanúsítás érvényességének.

Amennyiben a CSA8000 adaptert minősített aláírások létrehozására kívánják felhasználni, további követelményeknek kell megfelelni, melyek a felhasználhatóságot tovább korlátozzák, kiegészítő feltételek betartását követelve meg.

Tovább bonyolítja a helyzetet, hogy a CSA8000 adapter tervezett felhasználási módja (**több felhasználó közös aláíró eszköze)** igen szokatlan. Ennek engedélyezése további szigorításokat, extra feltételeket kíván meg.

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

10.2.1 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 CSA8000 kriptográfiai modul szolgáltatásait igénybe vevő különböző munkaköröket (Admin, Admin Security Officer, Token Security Officer, Token User) betöltő személyek:
    - kompetensek, jól képzettek és megbízhatóak, valamint
    - betartják a különböző útmutatók (CSA8000 Adapter Installation Guide, Cprov Installation Guide, Cprov Administration Manual, Cprov Key Management Utility User Manual) által leírt, kötelező tevékenységeket.

10.2.2 A FIPS 140-1 megfelelőségből fakadó érvényességi feltételek

Az alábbi feltételek ahhoz elengedhetetlenek, hogy a CSA8000 adaptert megfeleljen a FIPS 140-1 3-as biztonsági szintjének.

2. A digitális aláírással kapcsolatos kriptográfiai funkcionalitást az alábbi algoritmusokra kell korlátozni: **DSA, RSA (PKCS #1), SHA-1**.

3. A következő biztonsági beállításokat kell alkalmazni (konfigurálni):
   - CKF_ENTRUST_READY ("Entrust Compliant" flag) kötelező értéke: **FALSE**[65]
   - CKF_ALWAYS_SENSITIVE ("No Clear PINs" flag) kötelező értéke: **TRUE** (SET)[66]
   - CKF_AUTH_PROTECTION ("Session Protection" flag) kötelező értéke: **TRUE** (SET)[67]
   - CKF_MODE_LOCKED ("Lock Security Mode" flag) kötelező értéke: **TRUE** (SET)[68]
   - CKF_NO_PUBLIC_CRYPTO ("No Public Cryptography" flag) kötelező értéke: **TRUE** (SET)[69]

4. Az üzembe helyezés során a HIMK-ek[70] számára új értékeket kell beállítani, a gyári beállítású alap (default) HIMK értéket törölni kell.

5. Az üzembe helyezés során az Adminisztrátori kriptográfiai tisztviselő gyári beállítású alap (default) azonosítóját és jelszavát le kell cserélni.

6. Valamennyi operátornak (Adminisztrátori kriptográfiai tisztviselő, Adminisztrátor, Token kriptográfiai tisztviselő, Token felhasználó) titokban kell tartaniuk saját PIN kódjukat.

7. Minden új slot konfigurálásánál megfelelő hosszúságú PIN kódot kell választani. A CSA8000 a megadott hitelesítési adatokat bájtos alakban kezeli. Minden egymást követő sikertelen hitelesítési kísérlet után a CSA8000 5 másodperccel megnöveli a válaszadás késleltetését, így téve gyakorlatilag kipróbálhatatlanná egy támadó számára az összes szóba jöhető érték kipróbálását. Ahhoz, hogy magas fokú védelem legyen biztosítva **minimálisan 6 jegyű, véletlenszerű PIN kódot kell használni.** A hitelesítő adatokat bekérő alkalmazásnak ellenőriznie kell ezt a szintaktikát, s csak az ennek megfelelőket szabad továbbküldenie a CSA8000 felé.

---

[65] Az "Entrust Compliant" flag beállítása azt jelentené, hogy az Entrust termékek széles termékskálájával kompatíbilis módon, de a FIPS 140-1-nek nem megfelelően működne az adapter.

[66] A "No Clear PINs" flag beállítása azt jelenti, hogy a felhasználói PIN kódok és egyéb más érzékeny információ csak titkosított formában juthat a host interfészen keresztül a kriptográfiai modulba.

[67] A "Session Protection" flag beállítása az alkalmazások és a CSA8000 kriptográfiai modul közötti biztonságos üzenet hitelesítést kényszeríti ki. Beállítása esetén az adapternek szóló valamennyi kérés, illetve az ezekre adott valamennyi válasz digitálisan aláírásra kerül. Az aláírásra használt kulcs a felhasználó PIN kódjából, valamint az alkalmazás és az adapter által közösen birtokolt kulcsból származtatódik.

[68] A "Lock Security Mode" flag beállítása megakadályozza a biztonsági beállítások későbbi módosítását. (True értékre való beállítása után már csak teljes újrakonfigurálással lehet a biztonsági értékeket módosítani.)

[69] A "No Public Cryptography" flag beállítása azt jelenti, hogy minden alkalmazás csak azután hajthat végre műveleteket a CSA8000 kriptográfia modullal, ha előzetesen hitelesítette magát a PKCS #11 interfészen keresztül.

[70] HIMK /Host Interface Master Key/ egy háromszoros hosszúságú DES kulcs. Minden operátornak, aki jogosult az adapter használatára, van egy ilyen titkos, véletlenszerűen generált kulcsa, saját token eszközén letárolva. A HIMK-ek másodpéldányai az adapter védett memóriájában tárolódnak. Ezekből a kulcsokból származtatódnak az egyes operátorok és az adapter közötti munkaszakaszok (session) kommunikációját védő titkosító kulcsok, melyek segítségével egy megbízható csatorna épül ki az operátorok és az adapter között.

10.2.3 A biztonságos aláírás-létrehozó eszközként történő használhatóság kiegészítő feltételei

Egy minősített aláírásokat létrehozó aláírónak a CSA8000 felhasználása során az alábbi kiegészítő feltételeket is be kell tartania:

8. RSA aláírási algoritmus használata esetén a minimális modulus hosszúság (MinModLen): 1020 bit legyen.

9. DSA aláírási algoritmus használata esetén a minimális p prímhosszúság (pMinLen) 1024 bit, a minimális q prímhosszúság (qMinLen) 160 bit legyen.

10. Digitálisan aláírni csak 8-cal osztható bithosszúságú blokkot lehet[71]

11. A minősített aláírások létrehozására használt magánkulcsot csak minősített aláírások létrehozására szabad felhasználni. (Nem szabad titkosításra, hitelesítésre és fokozott biztonságú aláírások létrehozására felhasználni.)

12. A minősített aláírások létrehozására használt magánkulcsot tilos menteni.

13. A minősített aláírások létrehozására használt magánkulcsot érvényességének lejárta után haladéktalanul törölni kell. /Ez az aláíró felelőssége, de az aláíró alkalmazásnak támogatást kell ehhez biztosítania./

14. Egy BALE-ként használt CSA8000 szerepkör kiosztásánál és felhasználói token inicializálásánál be kell tartani a következőket:

    Minősített aláírásokat csak olyan helyi felhasználó hozhat létre, aki a Token felhasználó szerepkört tölti be. (csak helyi Token felhasználó lehet az „aláíró").
    /A CSA8000 az alábbi szerepköröket támogatja (a hagyományos adminisztrátori szerepkör háromfelé osztásával):
    - Adminisztrátori kriptográfiai tisztviselő,
    - Adminisztrátor,
    - Token kriptográfiai tisztviselő,
    - Token felhasználó./

    Feltételezve, hogy az alábbi két lépésre már előzetesen sor került:
    - az Adminisztrátori kriptográfiai tisztviselő inicializálta az Adminisztrátort, aki képes feladata ellátására,
    - az Adminisztrátor inicializálja a felhasználói token Token kriptográfiai tisztviselőjének a PIN kódját,

    egy minősített aláírások létrehozására alkalmas felhasználói token létrehozásánál az alábbi lépéseket kell egymást követően, legalább kettős személyi ellenőrzés alatt betartani, illetve végrehajtani:

    1. A Token kriptográfiai tisztviselő inicializálja az aláíró felhasználói tokenét:
       - inicializálva a Token felhasználó kezdeti PIN kódját,
       - (a PIN kód átadásával) engedélyezve az aláírói kulcspár generálását.
    2. A Token felhasználó azonnal lecseréli saját PIN kódját.

[71] Mert az SHA-1 lenyomatoló függvény FIPS értékelése és tanúsítása csak bájt-orientált adatokra vonatkozik.

3. A Token felhasználó haladéktalanul legenerálja saját (aláírói) kulcspárját.
4. A Token kriptográfiai tisztviselő (vagy az érintett Token felhasználó) exportálja a legenerált nyilvános kulcsot.
5. A Token kriptográfiai tisztviselő (vagy az érintett Token felhasználó) a felhasználói tokenre tölti a nyilvános kulcsra (a hitelesítés-szolgáltatótól kapott) tanúsítványt.

A fenti folyamat után minősített aláírások létrehozására csak a helyi Token felhasználó (illetve a nevében eljáró program) képes, ha sikeresen hitelesítette magát PIN kódja megadásával.
Távoli felhasználók hálózatról való bejelentkezéssel és távoli hitelesítéssel nem aktivizálhatják a CSA8000 adapteren lévő magánkulcsukat (összhangban az SSCD védelmi profil megbízható útvonal követelményében /FTP_TRP.1/ szereplő „lokális felhasználó" megszorításával)

A CSA8000 párhuzamosan több tokent támogat, mindegyiken egy-egy Token felhasználónak biztosítva hozzáférést, összességében tehát több különböző Token felhasználónak nyújtva (aláírói) szolgáltatást.

A fenti 5 lépéses eljárás minden Token felhasználóval külön-külön elvégzendő.

A fenti sorrendiséggel és kettős személyi jelenléttel teljesíthetők a BALE-ra elvárt alábbi elvárások:

- Az „aláíró" generálja ugyan saját kulcspárját, de ezt az „adminisztrátor" engedélyezi számára.
- Az „adminisztrátor" engedélyezi és kontrollálja a legenerált nyilvános kulcs tanúsítvány készítés céljából való exportálását.
- Csak az „aláíró" generálhatja saját magánkulcsát, s csak ő aktivizálhatja is azt (aláírásra)./

15. Egy BALE-ként használt CSA8000 kriptográfia modulra biztosítani kell az alábbiakat:

1. Azt követően, hogy egy Token felhasználó minősített aláírások létrehozására használható kulcspárt generált rajta, **a token nem vehető ki slot-jából** (az erre speciális jogosultsággal felhatalmazott Adminisztrátor kivételével). /A CSA8000 adaptert úgy kell beállítani, hogy nullázza védett memória tartalmát, ha jogosulatlanul kiemelik a gazdagép PCI slot-jából, akár annak kikapcsolt állapotában is./
2. A CSA8000 bekapcsolt, működő gazdagépének **közvetlen környezete** olyan **fizikai védelem alatt álljon**, mely megakadályozza a PCI slot-jában elhelyezett CSA8000 speciális eszközökkel való manipulálását, fizikai támadását.

   /A fenti környezeti fizikai védelemmel biztosíthatók a BALE-ra (általában technikai ellenintézkedésekkel kielégítendő) alábbi elvárások:

   - A BALE garantálja, hogy egyetlen felhasználó sem képes a külső interfészek kisugárzásából a magánkulcsot, illetve a PIN kódot megismerni.

- A működő CSA8000 ellen ne lehessen kivitelezni alacsony áramerősséggel, magas áramfeszültséggel, illetve alacsony és magas órafrekvenciával manipuláló támadásokat./

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

17. A megbízható csatornák kialakításában közreműködő kulcsokat (HIMK) a host oldalon is védeni kell. A CSA8000 adapter és az alkalmazások közötti megbízható csatorna egy közös titok ismeretén alapul. Ezt a titkot (HIMK) a gazdagép oldalán is kellő biztonsággal meg kell védeni az illetéktelen felfedés ellen.

18. a) A CSA8000 adaptert felhívó aláíró alkalmazásoknak meg kell teremteni az aláírók számára annak lehetőségét, hogy egy sikeres hitelesítést követő aláírás(ok) után deaktivizálhassa az eszközt, azaz saját tokenén a magánkulcsát újra hitelesítés nélkül aktivizálhatatlan állapotba hozhassa[72].

    b) Az aláíró (Token felhasználó) kötelessége deaktivizálni a CSA8000 által védett saját magánkulcsát, amikor aláírási szándéka megszűnik, illetve amikor az eszköz feletti személyes kontroll felvállalását szünetelni kívánja[73].

19. Egy 3-as típusú BALE-ként használt CSA8000 adapter eszköz nem használható hitelesítés-szolgáltató hardver kriptográfiai moduljaként.

20. A Tanúsítvány csak a jelenlegi hardver és förmver verzióra érvényes /hardver verzió: G revizió, Cprov förmver verzió:1.10/. Új förmver verzió upgradje csak az alábbi követelmények együttes teljesülése esetén lehetséges:
    - az új förmver verziót a fejlesztő-gyártó cég digitális aláírása hitelesíti,
    - az új förmver verziót értékelte[74] egy FIPS 140 értékeléssel meghatalmazott (akkreditált) laboratórium, s erről egy új FIPS tanúsítvány is készül,
    - az új förmver verzió BALE-ként való felhasználhatóságát egy erre kijelölt hazai tanúsító szervezet megfelelőségi tanúsítványba foglalja[75], s mint ilyen, az új verzió is bekerül a HIF biztonságos elektronikus aláírási termék nyilvántartásába.

[72] Ez a tipikus BALE-k esetében nem feltétlenül megkívánt funkció. Ezeknél ugyanis az aláíró kiveszi és elteszi saját eszközét az olvasóból, automatikusan deaktivizálva azt.
[73] Ezzel helyettesítve a „hagyományos" BALE kivételét az olvasóból.
[74] Valószínűleg különböző feltételekkel és megkötésekkel, a FIPS 140 megfelelőséget biztosító üzemmód meghatározásával.
[75] Valószínűleg további, a BALE-ként való használhatóságra vonatkozó feltételek meghatározásával.

11. A tanúsításhoz figyelembe vett dokumentumok

11.1 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+

FIPS 140-1: Security Requirements for Cryptographic Modules

Derived Test Requirements for FIPS 140-1

11.2 A tanúsítási jelentéshez figyelembe vett egyéb dokumentumok

Kérelem /a tanúsítás elvégzésére/

Kérdőív a tanúsítás kérelmezéséhez

FIPS 140-1 Validation Certificate No. 160 /CSA8000 Cryptographic Adapter/

ERACOM: CSA8000 Cryptographic Adapter, Hardware Revision: G, Firmware Version: 1.1, FIPS 140-1 Non-Proprietary Cryptographic Module Security Policy

CSA8000 Adapter Installation Guide /Version: A4, Date: 7 May 2001/

Cprov Installation Guide /Version: 3.0, Revision A6, Last Modified: 7 May 2001/

Cprov Administration Manual /Version: 3.0, Revision A7/ May 2001/

Cprov Key Management Utility User Manual /KMU Version: 3.0 Beta, Revision A1/ May 2001/

12. Rövidítések

AES	Advenced Encryption Standard
API	Application Programming Interface
BALE	Biztonságos aláírás-létrehozó eszköz
CBC	Cipher Block Chaining
CC	Common Criteria
CEN	European Comittee for Standardization
Cprov	Cryptoki (PKCS #11) Provider
DCP	Data Ciphering Processor
DES	Data Encryption Standard /FIPS PUB 46-3, FIPS PUB 74, FIPS PUB 81/
DSA	Digital Signature Algorithm /FIPS PUB 186-2/
EAL	Evaluation Assurance Level
ECB	Electronic Code Book
EDC	Error Detecting Code
EEPROM	Electrically Erasable Programmable Read Only Memory
EMI	Electromagnetic Interference
EMC	Electromagnetic Compability
FCC	Federal Communications Commission
FIPS	Federal Information Processing Standards Publications
FIPS 140-1	Security Requirements for Cryptographic Modules
FIPS 186-2	Digital Signature Standard
HIK	Host Interface Key
HIMK	Host Interface Master Key
HMAC	Hashed (Keyed Message Authentication CodeIC
	Integrated Circuit
IDEA	International Data Encryption Algorithm
IEC	International Electrotechnical Comission
ISO	International Organization for Standardization
ISSS	Information Society Standardization System
IT	Information Technology
MAC	Message Authentication Code
OFB	Output Feedback Mode
PCI	Peripheral Component Interconnection
PIN	Personal Identification Number
PKCS	Public Key Cryptographic Standards
PKCS #1	RSA Cryptography Standard
PKCS #7	Cryptographic Message Syntax Standard
PKCS #10	Certification Request Syntax Standard
PKCS #11	Cryptographic Token Interface Standard
PP	Protection Profile
RAM	Random Access Memory
RISC	Reduced Instuction Set Computer
RSA	Rivest-Shamir-Adleman (public key cryptosystem) /ANSI X9.31/
RTC	Real Time Clock
SDRAM	Synchronous Dynamic Random Access Memory
SHA-1	Secure Hash Algorithm /FIPS PUB 180-1/
SSCD	Secure Signature Creation Device (lásd BALE)
Triple-DES	/FIPS PUB 46-3, ANSI X9.52/