Tanúsítási jelentés

Hung-TJ-028-2005

a ProtectServer Orange (korábbi nevén CSA8000 Adapter)

kriptográfiai modulról

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

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

Tartalom

1. A Tanúsítási jelentés tárgya, feladata és hatóköre 5

2. A CSA8000 legfontosabb tulajdonságainak összefoglalása 7

2.1 A kriptográfiai modul 7

2.2 Modul interfészek 7

2.3 Megbízható csatornák 7

2.4 Szolgáltatások és szerepkörök 8

2.5 Fizikai biztonság 9

2.6 Biztonságos kriptográfia 9

2.7 Ön-tesztek 10

3. A FIPS Tanúsítvány eredményeinek összefoglalása 11

4. A CSA8000 értékelési követelményei a FIPS 140-1 szerint 12

4.1. A kriptográfiai modul tervezése és dokumentálása 12

4.2 Modul interfészek 13

4.3 Szerepkörök és szolgáltatások 14

4.3.1 Szerepkörök 14

4.3.2 Szolgáltatások 14

4.3.3 Operátori hitelesítés 15

4.4. Véges állapotú automata modell 15

4.5. Fizikai biztonság 17

4.5.1 Közös követelmények 17

4.5.2 Több chipes, beágyazott kriptográfiai modulra vonatkozó követelmények 17

4.6. Szoftver biztonság 18

4.7 Az operációs rendszer biztonsága 18

4.8 Kriptográfiai kulcsgondozás 18

4.8.1 Általános követelmények 18

4.8.2 Kulcs generálásra vonatkozó követelmények 19

4.8.3 Kulcs szétosztásra vonatkozó követelmények 19

4.8.4 Kulcs bevitelére és kivitelére vonatkozó követelmények 19

4.8.5 Kulcs tárolásra vonatkozó követelmények 20

4.8.6 Kulcs megsemmisítésre vonatkozó követelmények 20

4.8.7 Kulcs archiválásra vonatkozó követelmények 20

4.9. Kriptográfiai algoritmusok 20

4.10 Elektromágneses interferencia, elektromágneses kompatibilitás 21

4.11 Ön-tesztek 21

4.11.1 Általános követelmények 21

4.11.2 Áram alá helyezési tesztek 21

4.11.2.1 Általános tesztek 21

4.11.2.2 Kriptográfiai algoritmus tesztek 22

4.11.2.3 Szoftver/förmver teszt 22

4.11.2.4 Kritikus funkciók tesztjei 22

4.11.2.5 Statisztikus véletlenszám generátor tesztek 23

4.11.3 Feltételhez kötött tesztek 24

4.11.3.1 Páronkénti konzisztencia teszt 24

4.11.3.2 Szoftver/förmver betöltési tesztek 24
4.11.3.3 Kézi kulcs bevitel tesztje 24
4.11.3.4 Folyamatos véletlenszám generátor teszt 24

5. A CSA8000 értékeléshez megkövetelt fejlesztői bizonyítékok 25

5.1. A kriptográfiai modul tervezése és dokumentálása 25

5.2 Modul interfészek 27

5.3 Szerepkörök és szolgáltatások 29
5.3.1 Szerepkörök 29
5.3.2 Szolgáltatások 29
5.3.3 Operátori hitelesítés 30

5.4 Véges állapotú automata modell 31

5.5 Fizikai biztonság 31
5.5.1 Közös követelmények 31
5.5.2 Több chipes, beágyazott kriptográfiai modulra vonatkozó követelmények 31

5.6. Szoftver biztonság 32

5.7. Az operációs rendszer biztonsága 33

5.8. Kriptográfiai kulcsgondozás 33
5.8.1 Általános követelmények 33
5.8.2 Kulcs generálásra vonatkozó követelmények 34
5.8.3 Kulcs szétosztásra vonatkozó követelmények 35
5.8.4 Kulcs bevitelére és kivitelére vonatkozó követelmények 35
5.8.5 Kulcs tárolásra vonatkozó követelmények 36
5.8.6 Kulcs megsemmisítésre vonatkozó követelmények 37
5.8.7 Kulcs archiválásra vonatkozó követelmények 37

5.9 Kriptográfiai algoritmusok 37

5.10 Elektromágneses interferencia, elektromágneses kompatibilitás 37

5.11 Ön-tesztek 37
5.11.1 Általános követelmények 37
5.11.2 Az áram alá helyezési tesztek 38
5.11.2.1 Általános tesztek 38
5.11.2.2 Kriptográfiai algoritmus tesztek 38
5.11.2.3 Szoftver/förmver teszt 39
5.11.2.4 Kritikus funkciók tesztjei 39
5.11.2.5 Statisztikus véletlenszám generátor tesztek 39
5.11.3 Feltételhez kötött tesztek 40
5.11.3.1 Páronkénti konzisztencia teszt 40
5.11.3.2 Szoftver/förmver betöltési tesztek 40
5.11.3.3 Kézi kulcs bevitel tesztje 40
5.11.3.4 Folyamatos véletlenszám generátor teszt 40

6. A minősített hitelesítés-szolgáltatókra vonatkozó járulékos funkcionális és biztonsági követelmények 41

6.1 Elektronikus aláírás hitelesítés szolgáltatásra vonatkozó követelmények 41

6.2 Időbélyegzés szolgáltatásra vonatkozó követelmények 43

6.3 Aláírás-létrehozó eszközön az aláírás-létrehozó adat elhelyezése szolgáltatásra vonatkozó követelmények 44

7. A Tanúsítási jelentés eredménye, érvényességi feltételei 45

7.1 A Tanúsítási jelentés eredménye 45

7.2 Az eredmények érvényességi feltételei 45
7.2.1 Általános érvényességi feltételek 46
7.2.2 A FIPS 140-1 megfelelőségből fakadó érvényességi feltételek 46
7.2.3 A minősített hitelesítés-szolgáltatáshoz történő használhatóság kiegészítő feltételei 47
7.2.4 Egyéb, az érvényességet befolyásoló megjegyzések 48
8. A tanúsításhoz figyelembe vett dokumentumok 49
8.1 Termékmegfelelőségi követelményeket tartalmazó dokumentumok 49
8.2 A tanúsítási jelentéshez figyelembe vett egyéb dokumentumok 49
9. Rövidítések 50

1. A Tanúsítási jelentés tárgya, feladata és hatóköre

Jelen Tanúsítási jelentés tárgya a CSA8000 kriptográfiai adapter, melyet minősített hitelesítés-szolgáltatás nyújtásához kapcsolódó különböző feladatok ellátására kívánnak felhasználni, mint "biztonságos" kriptográfiai modult.

A minősített hitelesítés-szolgáltatókra vonatkozó funkcionális és biztonsági követelményeket meghatározó EU-s dokumentumok (CEN 14167-1 munkacsoport egyezmény: "Elektronikus aláírásokhoz tanúsítványokat kezelő megbízható rendszerekre vonatkozó biztonsági követelmények", ETSI TS 101 456: "Minősített tanúsítványokat kibocsátó hitelesítés-szolgáltatókra vonatkozó szabályozási követelmények") és hazai jogszabályok (köztük legrészletesebben a 2/2002 (IV.26) MeHVM irányelve a minősített elektronikus aláírással kapcsolatos szolgáltatásokra és ezek szolgáltatóira vonatkozó biztonsági követelményekről) irányadók jelen Tanúsítási jelentéshez.

Ezen követelmények közül az egyik meghatározó fontosságú (mely több más követelményre is hatással van) elvárja, hogy a minősített hitelesítés-szolgáltatók[1] által használt kriptográfiai modul tanúsítvánnyal igazoltan feleljen meg az alábbi szabványok legalább egyikének:

- [FIPS 140-1], 3-as (vagy magasabb) biztonsági szint,
- [CEN:HSM-PP] (CMCSO-PP és CMCKG-PP[2]),
- [ITSEC] E3/high (vagy magasabb) biztonsági szint.

A CSA8000 kriptográfiai adapter FIPS 140-1 3-as szintű tanúsítvánnyal rendelkezik.

A FIPS 140-1 3-as biztonsági szintje igen szigorú követelményrendszert támaszt az általános célú kriptográfia modulok részére. Ugyanakkor nem tartalmaz számos olyan funkcionális és biztonsági követelményt, melyet a minősített hitelesítés-szolgáltatóknak ki kell elégíteniük saját kriptográfiai moduljukkal.

A fentiekből következően a jelen Tanúsítási jelentés fő feladata annak megállapítása, hogy:

- a CSA8000 kriptográfiai adapter alkalmas-e minősített hitelesítés-szolgáltatás nyújtásához való alkalmazásra, s ha igen, akkor mely kapcsolódó feladatokhoz használható,
- a FIPS 140-1 szerinti Tanúsítvány érvényessége, illetve a többi kielégítendő funkcionális és biztonsági követelmény teljesülése milyen korlátozásokat, feltételeket támaszt a kriptográfiai modul használatára.

Jelen Tanúsítási jelentés hatóköre ugyanakkor csak a minősített hitelesítés-szolgáltatás nyújtásához való alkalmasságra 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-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[3] RC2, RC4, MD2, MD5, Diffie-Hellman (kulcsegyeztetés)/.

[1] A követelmény nem minősített hitelesítés-szolgáltatóra is vonatkozik.
[2] Ez utóbbinak csak akkor, ha a minősített hitelesítés-szolgáltató biztosít aláírás-létrehozó eszközön az aláírás-létrehozó adat elhelyezése szolgáltatást is.
[3] Az értékeléskor az AES még nem volt FIPS jóváhagyott algoritmus.

A Tanúsítási jelentés további szerkezete a következő:

- A CSA8000 adapter legfontosabb tulajdonságainak összefoglalása (2. fejezet).
- A FIPS Tanúsítvány eredményeinek összefoglalása (3. fejezet).
- A FIPS 140-1-nek való megfelelőségből (3-as biztonsági szintből) adódó, kielégített követelmények /külön tárgyalva az értékelés követelményeit, s az értékeléshez megkövetelt fejlesztői bizonyítékokat/ (4. és 5. fejezetek).
- A FIPS követelményrendszerén túlmutató, minősített hitelesítés-szolgáltatókra vonatkozó funkcionális és biztonsági követelmények (6. fejezet).
- A minősített hitelesítés-szolgáltatás nyújtáshoz való alkalmasság megállapítása, valamint az alkalmazás feltételeinek és korlátainak a meghatározása (7. fejezet).
- A jelen Tanúsítási jelentéshez figyelembe vett dokumentumok jegyzéke (8. fejezet).
- Felhasznált rövidítések jegyzéke (9. fejezet).

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[4]. Bár bizonyos PKCS #11 tulajdonságokat nem támogat a modul, ugyanakkor biztosítja a PKCS #11 szabványnak való átfogó megfelelőséget, illetve bizonyos felhasználó-specifikus kiterjesztéseket[5] is támogat.
A CSA8000 Adapter kielégíti a FIPS 140-1 követelményeit, a 3. biztonsági szinten, a több chipes, 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 chipek, 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.

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,

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

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[6]-ok és a Token kriptográfiai tisztviselők ellenőrzéséért.
- 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

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

szolgáltatás kérésre vonatkozó üzenetet hitelesítenie kell[7]. 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.

Az adapter megfelel az otthoni használatra tervezett személyi számítógépekre és perifériákra vonatkozó, elektromágneses interferencia és elektromágneses kompatibilitás 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[8].

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	ECB, CBC, OFB

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

[8] 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).

üzemmódok	
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 (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"[9]ek a modul által támogatott valamennyi kriptográfiai algoritmusra,
- szoftver (förmver) integritás teszt (32 bites hiba detektáló kódot és SHA-1 lenyomatoló föggvényt 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).

[9] 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 Tanúsítvány eredményeinek összefoglalása

A CSA8000 Adaptert egy kriptográfiai modulok tesztelésére az Egyesült Államokban és Kanadában akkreditált laboratórium[10] 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 chipes, beágyazott/:	3-as szint
Szoftver biztonság:	3-as szint
Az operációs rendszer biztonsága:	nincs értékelve[11]
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[12], FIPS által jóváhagyott algoritmusok megvalósítását vizsgálta, tesztelte: **DES, Triple-DES**

Az elért általános biztonsági szint: 3-as

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

4. A CSA8000 értékelési követelményei a FIPS 140-1 szerint

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.[13]

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[14] biztonsági követelményeiből illetve a gyártó által előírt járulékos biztonsági követelményekből származnak.

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

4.2 Modul interfészek

KÖV_02.01:
A modult úgy kell megszerkeszteni, hogy a modulhoz tartozó minden információáramlás 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[15].

KÖV_02.04:
Az adat output interfészen keresztül történő minden adat outputot le kell tiltani hiba állapot vagy az öntesztek 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.

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.

[15] 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.

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[16].
Ha a modul több egyidejű operátort támogat[17], 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 ill. szerepköröket, amelyben a szóban forgó szolgáltatás végrehajtható.

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[18].

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

[16] 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.
[17] A CSA8000 támogat több egyidejű operátort.
[18] A CSA8000 nem biztosítja a megkerülés lehetőségét, így az erre vonatkozó követelményt (KÖV_03.10.) sem tartalmazza ez a fejezet.

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[19] 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.

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[20]:
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.

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:

[19] 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).
[20] 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,

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-teszt 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.[21]

KÖV_04.07:
Bármilyen hiba állapot esetén az adat output interfészen keresztül történő minden adat outputot le kell tiltani[22].

[21] 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.
[22] Ez a követelmény hasonló a 2. fejezet (Modul interfészek) KÖV_02.04 követelményéhez.

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.

4.5. Fizikai biztonság

4.5.1 Közös követelmények[23]

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 chipes, beágyazott kriptográfiai modulra vonatkozó követelmények

KÖV_05.07[24]:
Több chipes, beágyazott kriptográfiai modul esetén a modulban lévő chipeknek olyan termék minőségűeknek kell lenniük, amelyek magukban foglalnak standard passziválási technikát is.

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

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

KÖV_05.10:
Több chipes, 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[25]:
Több chipes, beágyazott kriptográfiai modul esetében, ha a modul valamilyen szellőzőnyílást tartalmaz, azt olyan módon kell megtervezni, hogy az meggátoljon minden észrevétlen szondázást.

[23] Vagyis a kriptográfiai modul mindhárom lehetséges fizikai konfigurációjára (egy chipből álló, több chipes, beágyazott, illetve több chipes, önmagában álló) vonatkozik.
[24] Ez a fejezet nem tartalmazza a csak az egy chipből álló kriptográfiai modulokra vonatkozó KÖV_05.02 - KÖV_05.06 követelményeket.
[25] 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 chipes, 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[26].

4.7 Az operációs rendszer biztonsága

Nincsenek követelmények[27].

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.

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

4.8.2 Kulcs generálásra vonatkozó követelmények

KÖV_08.04:
Egy kriptográfiai modul opcionálisan ki lehet egészítve egy belső kulcs generálási funkcióval[28]. 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[29], 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[30], 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.

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.

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

KÖV_08.15[31]:
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.

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.

[31] 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.

4.10 Elektromágneses interferencia, elektromágneses kompatibilitás

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

KÖV_10.03[32]:
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.

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[33] 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:

[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_10.02-t.
[33] FIPS 140-1

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

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[34].

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.

[34] 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[35]:
A statisztikai teszteknek igény esetén meghívhatóknak kell lenniük. Idevonatkozó követelmény a KÖV_11.09 is.

[35] 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[36].

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[37].

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.

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

5. A CSA8000 értékeléshez megkövetelt fejlesztői bizonyítékok

Az alábbiakban áttekintjük azokat a fejlesztői bizonyítékokat (dokumentálást, egyéb információ szolgáltatást), melyet a fejlesztő cég biztosított a vizsgálatok elvégzéséhez a CSA8000 értékelését végző laboratórium számára.

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 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 chipből álló modul, több chipes, beágyazott modul vagy több chipes, 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[38], 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.

[38] A CSA8000 adapter felvesz áramot.

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.

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[39],
- A kriptográfia megkerülése[40].

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.

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:

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

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 chipből álló modul, több chipes, beágyazott modul vagy több chipes, önmagában álló kriptográfiai modul[41]. 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 chipes, beágyazott kriptográfiai modulra vonatkozó követelmények

FB_05.07.01:
A több chipes, beágyazott modul chipjeinek 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 chipre 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 chipes 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:

[41] A CSA8000 esetében ez: több chipes, beágyazott modul.

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:

- A modul több chipes 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[42].

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.

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).

[42] 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.

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[43].

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,

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

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[44], 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.

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[45],
  - 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:

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

- memória kártya/token (pl. mágnes csíkos kártyák, IC chip készülékek),
- intelligens kártyák/tokenek[46],
- 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[47], 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.

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.

[46] A CSA8000 magán kulcsainak mentésére és visszatöltésére intelligens kártyák használhatók.
[47] 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.

5.8.6 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[48], lásd az FB_08.01.01. alatti 7a-tól 7d-ig terjedő tételeket a fejlesztői dokumentációra vonatkozó követelményeket illetően.

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[49].
Megjegyzés: A fejlesztő beépíthet a kriptográfiai modulba más (azaz nem FIPS által jóváhagyott) kriptográfiai algoritmusokat is[50].

5.10 Elektromágneses interferencia, elektromágneses kompatibilitás

FB_10.01.01:
A fejlesztőnek egy FCC bizonyítványt kell szolgáltatnia arra vonatkozóan, hogy a kriptográfiai modul, mint egy jelsugárzó egység, 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 hibajelzést.

FB_11.03.01:

[48] A CSA8000 támogatja a HIMK titkos kulcsok és a különböző magán kulcsok archiválását (komponensekre bontva, kódolt formában, intelligens kártyákon tárolva).
[49] A CSA8000 rendelkezik ilyen tanúsítvánnyal a DES, Triple-DES, DSA, SHA-1 és RSA kriptográfiai algoritmusokra.
[50] 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).

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.

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[51]. 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.

[51] 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[52]. 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[53]. 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.

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

[52] 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.
[53] A CSA8000 rendelkezik ilyen tanúsítvánnyal (DSA, SHA-1, RSA).

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[54]. 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)[55]:
  - 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

FB_11.21.02:
Ha a hiba detektáló kódot alkalmazzák[56], 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[57], a fejlesztőnek dokumentálnia kell a folyamatos véletlenszám generátor tesztet.

[54] 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.
[55] A CSA8000 ezt a technikát alkalmazza.
[56] Mint a CSA8000 esetében.

6. A minősített hitelesítés-szolgáltatókra vonatkozó járulékos funkcionális és biztonsági követelmények

Az alábbiakban áttekintjük azokat az irányadó követelményrendszerekből adódó követelményeket, melyek egy minősített hitelesítés-szolgáltató által használt "biztonságos" kriptográfiai modulra vonatkoznak. Azokra a funkcionális és biztonsági követelményekre szorítkozunk, melynek teljesülését egy 3-as biztonsági szintű FIPS 140-1 értékelés/tanúsítás nem biztosítja automatikusan.
Az alábbiakban a CEN 14167-1 munkacsoport egyezmény jelöléseit alkalmazzuk, lábjegyzetként pedig egyenként utalunk a magyar jogszabályokban megfogalmazott megfelelő követelményekre.

6.1 Elektronikus aláírás hitelesítés szolgáltatásra vonatkozó követelmények

Ezen szolgáltatás keretében a követelmények a minősített hitelesítés-szolgáltató saját kulcsainak gondozására irányulnak. Az alábbiakban a kulcsok alábbi kategóriáit fogjuk megkülönböztetni[58]:

1. **Minősített tanúsítvány aláíró kulcsok.** A tanúsítvány előállítás kulcspárja minősített tanúsítványok létrehozásához.
2. **Infrastrukturális kulcsok**. Ezeket a kulcsokat a megbízható rendszerek olyan folyamatokhoz használják, mint pl. tanúsítvány állapot válaszok aláírása, kulcs-egyeztetés, alrendszer hitelesítés, napló aláírás, tárolt vagy továbbított adatok rejtjelezése stb. (A rövid életciklusú párbeszéd kulcsokat nem tekintjük infrastrukturális kulcsoknak.)
3. **Megbízható rendszervezérlési kulcsok.** Ezeket a kulcsokat személyek használják a megbízható rendszer használatára vagy kezelésére, és hitelesítési-, aláírási- vagy bizalmassági szolgáltatásokat biztosíthatnak a rendszerrel kölcsönhatásba kerülő személyek számára.
4. **Rövid életciklusú munkaszakasz kulcsok**. Egyszeri tranzakciókhoz, rövid ideig használatban lévő kulcsok.

[KM1.1][59]
A minősített tanúsítvány aláíró kulcsokat biztonságos kriptográfiai modulban kell előállítani.

[KM1.2][60]
A [KM1.1]-ben említett kriptográfiai modulnak tanúsítvánnyal igazoltan meg kell felelnie az alábbi szabványok legalább egyikének:

- [FIPS 140-1], 3-as (vagy magasabb) biztonsági szint,
- [CEN: CMCSO-PP, HSM-PP],
- [ITSEC][61].

[KM1.3][62]
A kriptográfiai modul a minősített tanúsítvány aláíró kulcsokat csak kettős ellenőrzés alatt állíthatja elő[63].

[KM1.4][64]

---

[57] Mint ahogy a CSA8000, mely egy hardver véletlenszám generátort alkalmaz, kombinálva egy FIPS által jóváhagyott (pszeudó) véletlenszám generálási technikával (FIPS 186-2).
[58] Mely kulcs kategóriák megegyeznek a 2/2002 MeHVM 73. pontjában definiáltakkal.
[59] Lásd a 2/2002 MeHVM rendelet 75. pontját.
[60] Lásd a 2/2002 MeHVM rendelet 75. pontját.
[61] A kriptográfiai modul [ITSEC] szerint is kiértékelhető, amennyiben a gyártó/szolgáltató bizonyítja, hogy minimálisan ITSEC E3/high szerinti értékelést alkalmazva az [ITSEC]-ben használt biztonsági követelmények kielégítik a fenti szabványok egyikét. Ha ezek a kritériumok teljesülnek, el kell fogadni, hogy a modul teljesíti a [KM1.2], [KM1.5] és [TS4.2] előírásait is.
[62] Lásd a 2/2002 MeHVM rendelet 76. pontját.
[63] Megjegyzés: A kettős ellenőrzési követelmény teljesíthető akár közvetlenül a kriptográfiai modul által, akár úgy, hogy a hitelesítés-szolgáltató kettős személyi ellenőrzést alkalmaz.

Az infrastrukturális kulcsokat biztonságos kriptográfiai modulban kell előállítani.

[KM1.5][65]
A [KM1.4]-ben említett kriptográfiai modulnak tanúsítvánnyal igazoltan meg kell felelnie legalább a [FIPS-140-1] 2-es szintjének, vagy más ennek megfelelő szabványnak [66].

[KM1.6][67]
A rendszervezérlési kulcsokat biztonságos kriptográfiai modulban kell előállítani[68].

[KM1.7][69]
Minden kulcselőállításnak meg kell felelnie az alábbiak valamelyikének:
- valódi (hardver) véletlen generálás legalább 128 bit szabadsági fokkal,
- pszeudó véletlen generálás egy legalább 128 bit hosszúságú "seed" kulcs mellett[70].

[KM6.1][71]
Minden magán- vagy titkos kulcsot biztonságosan kell tárolni.

[KM6.2][72]
A minősített tanúsítványokat aláíró kulcsot biztonságos kriptográfiai modulban kell tárolni, mely megfelel a [KM1.2]-ben rögzített tanúsítvánnyal történő igazolási követelményeknek.
A titkos/magán infrastrukturális kulcsokat biztonságos kriptográfiai modul(ok)ban kell tárolni, mely(ek) megfelel(nek) a [KM1.5]-ben rögzített tanúsítvánnyal történő igazolási követelményeknek.

[KM6.3][73]
A magán- vagy titkos rendszervezérlési kulcsokat biztonságos kriptográfiai modul(ok)ban kell tárolni.

[KM6.4][74]
Bármilyen, biztonságos kriptográfiai modulban tárolt kulcs modulból történő exportálásakor a modulnak gondoskodnia kell a kulcs védelméről. Érzékeny kulcsadatok nem védett módon történő tárolása tilos.
Minősített tanúsítvány aláíró kulcs csak további biztonsági mechanizmusok alkalmazása esetén tárolható és menthető. Ez megtehető például az "m az n-ből" technikák alkalmazásával, ahol m azon komponensek darabszáma a teljes n komponensből, amelynek ismeretében a kulcs inicializálása sikeresen elvégezhető. A hiba esetén alkalmazandó helyreállításra az m = 60% * n érték javasolt (azaz ha n=3, akkor m=2, ha n=4 akkor m=3, ha n=5 akkor m=3,…).
[CG1.4][75]
A minősített tanúsítvány aláírására használt kulcsot csak a minősített tanúsítványok, illetve esetlegesen a rájuk vonatkozó visszavonási listák aláírására szabad felhasználni.

[CG1.6] [76]
A megbízható rendszer által kibocsátott minősített tanúsítványnak meg kell felelnie a Törvény 2. mellékletében meghatározott követelményeknek. Különösen az alábbi tulajdonságoknak kell meglenniük[77]:

---

[64] Lásd a 2/2002 MeHVM rendelet 77. pontját.
[65] Lásd a 2/2002 MeHVM rendelet 77. pontját.
[66] Lásd [KM1.2] alatti megjegyzést.
[67] Lásd a 2/2002 MeHVM rendelet 78. pontját.
[68] Megjegyzés: Ennek a biztonságos kriptográfiai modulnak legalább a [FIPS-140-1] 1-es szintjének, vagy más megfelelő szabványnak kell megfelelnie.
[69] Lásd a 2/2002 MeHVM rendelet 79. pontját.
[70] Lásd a 2/2002 MeHVM rendelet irányelvek 1. sz. mellékletében felsorolt jóváhagyott kulcs generáló algoritmusok listáját.
[71] Lásd a 2/2002 MeHVM rendelet 104. pontját.
[72] Lásd a 2/2002 MeHVM rendelet 106. és 107. pontját.
[73] Lásd a 2/2002 MeHVM rendelet 108. pontját.
[74] Lásd a 2/2002 MeHVM rendelet 109. pontját.
[75] Lásd a 2/2002 MeHVM rendelet 94. és 160.pontját.
[76] Lásd a 2/2002 MeHVM rendelet 162/e alpontját.

1….
2…
3…
4…
5. A megbízható rendszer által a minősített tanúsítvány aláírásához használt aláírási algoritmusok/kulcsok az alábbiak valamelyike lehet:[78]
   - RSA (minimális modulus hosszúság (MinModLen): 1020 bit),
   - DSA (minimális p prímhosszúság (pMinLen): 1024 bit, minimális q prímhosszúság (qMinLen): 160 bit),
   - ECDSA-Fp (qMinLen = 160, r0Min = 10000, MinClass = 200),
   - ECDSA-F2m (qMinLen = 160, r0Min = 10000, MinClass = 200),
6…

6.2 Időbélyegzés szolgáltatásra vonatkozó követelmények

[TS4.1][79]
Az időbélyegzés-szolgáltató aláíró kulcsait biztonságos kriptográfiai modulban kell előállítani és tárolni.

[TS4.2][80]
A TS4.1-ben említett kriptográfiai modulnak tanúsítvánnyal igazoltan meg kell felelnie az alábbi szabványok legalább egyikének:
- [FIPS 140-1] 3-as (vagy magasabb) biztonsági szint,
- [CMCSO-PP, HSM-PP],
- ITSEC[81]

[TS4.3][82]
Az időbélyegzés-szolgáltató rendszervezérlési kulcsait biztonságos kriptográfiai modulban kell tárolni.

[TS4.4][83]
Az időbélyegzéshez használt aláíró kulcsokat kizárólag az adott időbélyegzés-szolgáltató által létrehozott időbélyegek aláírására szabad használni.

[TS4.6][84]
Az időbélyegzés-szolgáltató által használt aláíró algoritmusoknak/kulcsoknak, meg kell felelniük a [CG1.6] alatt felsorolt kriptográfiai követelményeknek.

[77] Csak az 5. Releváns a kriptográfiai modulra.
[78] Lásd a 2/2002 MeHVM rendelet irányelvek 1. sz. mellékletében felsorolt jóváhagyott aláíró algoritmusok listáját.
[79] Lásd a 2/2002 MeHVM rendelet 75. és 212. pontját.
[80] Lásd a 2/2002 MeHVM rendelet 75. és 212. pontját.
[81] Lásd a [KM1.2] alatti megjegyzést.
[82] Lásd a 2/2002 MeHVM rendelet 104. és 213. pontját.
[83] Lásd a 2/2002 MeHVM rendelet 214. pontját.
[84] Lásd a 2/2002 MeHVM rendelet 216. pontját.

6.3 Aláírás-létrehozó eszközön az aláírás-létrehozó adat elhelyezése szolgáltatásra vonatkozó követelmények

[KM1.7][85]
Minden kulcselőállításnak[86] meg kell felelnie az alábbiak valamelyikének:
- valódi (hardver) véletlen generálás legalább 128 bit szabadsági fokkal,
- pszeudó véletlen generálás egy legalább 128 bit hosszúságú "seed" kulcs mellett[87].

[KM3.4][88]
Biztosítani kell, hogy az elektronikus aláírásra szolgáló aláírói kulcsok különbözzenek minden más funkcióra szolgáló kulcstól, mint például a titkosításra szolgálóktól.

[SP1.4][89]
Ha a kulcspár előállítása az aláírás-létrehozó eszközön kívül történik, a kulcspárt előállító kriptográfiai eszköznek tanúsítvánnyal igazoltan meg kell felelnie az alábbi szabványok, szabványjellegű dokumentumok legalább egyikének:
- [FIPS 140-1], 3-as (vagy magasabb) biztonsági szint,
- [CMCKG-PP, HSM-PP],
- [CEN SSCD][90].

[SP1.5][91]
Ha a kulcspár előállítása az aláírás-létrehozó eszközön kívül történik, a kulcspárt biztonságos módon kell az aláírás-létrehozó eszközbe juttatni. A kriptográfiai eszköz és az aláírás létrehozó eszköz között biztonságos útvonalnak kell lennie. Ennek az útvonalnak forráshitelesítést, sérthetetlenséget és bizalmasságot kell biztosítania megfelelő kriptográfiai mechanizmusok használatával.

[85] Lásd a 2/2002 MeHVM rendelet 79. pontját.
[86] Így az aláírás-létrehozó eszközön elhelyezendő aláíró magánkulcs generálása is.
[87] Lásd a 2/2002 MeHVM rendelet irányelvek 1. sz. mellékletében felsorolt jóváhagyott kulcs generáló algoritmusok listáját.
[88] Lásd a 2/2002 MeHVM rendelet 95. pontját.
[89] Lásd a 2/2002 MeHVM rendelet 226. pontját.
[90] Lásd a [KM1.2] alatti megjegyzést.
[91] Lásd a 2/2002 MeHVM rendelet 227. pontját.

7. A Tanúsítási jelentés eredménye, érvényességi feltételei

7.1 A Tanúsítási jelentés eredménye

A ProtectServer Orange (korábbi nevén CSA8000 Adapter)
/Eracom Technologies Group, Eracom Technologies Australia, Pty. Ltd./

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

a Tanúsítás érvényességi feltételeinek[92] együttes teljesülése esetén

ALKALMAS

minősített hitelesítés-szolgáltató által végzett alábbi tevékenységek biztonságos elvégzéséhez:

Valamennyi szolgáltatásra vonatkozóan:

Infrastrukturális kulcsok generálására, tárolására és felhasználására az alábbi célokra:
- tanúsítvány állapot válaszok aláírása,
- tanúsítvány visszavonási listák aláírása,
- naplózott adatállomány aláírása,
- a minősített hitelesítés-szolgáltató megbízható rendszerében a különböző alrendszerek közötti hitelesítésre, kulcsegyeztetésre, tárolt vagy továbbított adatok aláírására.

Megbízható rendszervezérlési kulcsok generálására, tárolására és felhasználására az alábbi célokra:
- a minősített hitelesítés-szolgáltató megbízható rendszerével kölcsönhatásba kerülő személyek által a megbízható rendszer használatára irányuló hitelesítésre és aláírásra.

Elektronikus aláírás hitelesítés szolgáltatás keretén belül:

(Minősített) tanúsítvány aláíró kulcsok generálására, tárolására, (minősített) tanúsítványok létrehozásához való felhasználására, mentésére és helyreállítására.

Időbélyegzés szolgáltatás keretén belül:
Időbélyeg aláíró kulcsok generálására, tárolására, időbélyegző[93] aláírására történő felhasználására.

Aláírás-létrehozó eszközön az aláírás-létrehozó adat elhelyezése szolgáltatás keretén belül:
Az előfizetői (aláírói) kulcspár generálására[94].

7.2 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.

[92] Lásd a 7.2 “Az eredmények érvényességi feltételei” fejezet 1.-16. feltételeit.
[93] Mely időbélyegzőt a 2001 évi XXXV. törvény az elektronikus aláírásról minősített időbélyegzőként említi.
[94] Amennyiben a kulcspár előállítása az aláírás-létrehozó eszközön kívül történik.

Amennyiben a CSA8000 adaptert egy minősített hitelesítés-szolgáltató kívánja felhasználni biztonságkritikus tevékenységeihez (az általa kibocsátott tanúsítványok aláírására, időbélyeg válaszai aláírására), további követelményeknek kell megfelelni, melyek a felhasználhatóságot tovább korlátozzák, kiegészítő feltételek betartását követelve meg.

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

7.2.1 Általános érvényességi feltételek

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

1. A 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.

7.2.2 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**[95]
    - CKF_ALWAYS_SENSITIVE (“No Clear PINs” flag) kötelező értéke: **TRUE** (SET)[96]
    - CKF_AUTH_PROTECTION (“Session Protection” flag) kötelező értéke: **TRUE** (SET)[97]
    - CKF_MODE_LOCKED (“Lock Security Mode” flag) kötelező értéke: **TRUE** (SET)[98]
    - CKF_NO_PUBLIC_CRYPTO (“No Public Cryptography” flag) kötelező értéke: **TRUE** (SET)[99]
4. Az üzembe helyezés során a HIMK-ek[100] számára új értékeket kell beállítani, a gyári beállítású alap (default) HIMK értéket törölni kell.

---

[95] 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.

[96] 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.

[97] 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.

[98] 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.)

[99] 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.

[100] 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

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

6. Az operátoroknak titokban kell tartaniuk saját PIN kódjukat.

7. Minden új slot konfigurálásánál a PIN kód hossza legalább 4 legyen.

7.2.3 A minősített hitelesítés-szolgáltatáshoz történő használhatóság kiegészítő feltételei

Egy minősített hitelesítés-szolgáltatónak 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[101]

11. A minősített tanúsítvány aláírására használt kulcsot csak a minősített tanúsítványok, illetve esetlegesen a rájuk vonatkozó visszavonási listák aláírására szabad felhasználni.

12. Bármilyen, biztonságos kriptográfiai modulban tárolt kulcs modulból történő exportálásakor a modulnak gondoskodnia kell a kulcs védelméről. Érzékeny kulcsadatok nem védett módon történő tárolása tilos. Minősített tanúsítvány aláíró kulcs csak további biztonsági mechanizmusok alkalmazása esetén tárolható és menthető[102]:. Ez megtehető például az alábbiak valamelyikével is:

- az "m az n-ből" technika alkalmazásával (melyet jelenleg a CSA8000 nem támogat, de szabványos felületén keresztül később megvalósítható), ahol m azon komponensek darabszáma a teljes n komponensből, amelynek ismeretében a kulcs inicializálása sikeresen elvégezhető. A hiba esetén alkalmazandó helyreállításra az m = 60% * n érték javasolt (azaz ha n=3, akkor m=2, ha n=4 akkor m=3, ha n=5 akkor m=3,…).
- az alábbi (CSA8000 által támogatott) módszerrel:
  - a mentés intelligens kártyákra[103] történnek,
  - a mentés kódolva van a triple-DES titkosító algoritmus alkalmazásával,
  - a mentés kódolására alkalmazott titkosító kulcs (Key Encryption Key) legalább két véletlen komponensből van előállítva, s ennek megfelelően legalább két erre felhatalmazott személy együttes jelenléte szükséges a magánkulcs helyreállításához.

13. Az időbélyegzéshez használt aláíró kulcsokat csak időbélyegek aláírására szabad használni.

---

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.

[101] Mert az SHA-1 lenyomatoló függvény FIPS értékelése, tanúsítása csak byte-orientált adatokra

[102] S ily módon felelve meg a 3/2005 IHM rendelet szolgáltatói magánkulcsra vonatkozó 22. § követelményeinek.

[103] token

14. Amennyiben az aláírás-létrehozó eszközön az aláírás-létrehozó adat elhelyezése szolgáltatás keretén belül az előfizetői (aláírói) kulcspár generálása az aláírás-létrehozó eszközön kívül (a CSA8000 kriptográfiai hardverben) történik, biztosítani kell, hogy az elektronikus aláírásra szolgáló aláírói kulcsok különbözzenek minden más funkcióra szolgáló kulcstól, mint például a titkosításra szolgálóktól.

15. Amennyiben az aláírás-létrehozó eszközön az aláírás-létrehozó adat elhelyezése szolgáltatás keretén belül az előfizetői (aláírói) kulcspár generálása az aláírás-létrehozó eszközön kívül (a CSA8000 kriptográfiai modulban) történik, biztosítani kell, hogy a CSA8000 kriptográfiai modul és az aláírás létrehozó eszköz között biztonságos útvonal legyen. Ennek az útvonalnak forráshitelesítést, sérthetetlenséget és bizalmasságot kell biztosítania megfelelő kriptográfiai mechanizmusok használatával.

16. 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[104] egy FIPS 140 értékeléssel meghatalmazott (akkreditált) laboratórium, s erről egy új FIPS tanúsítvány is készül,
    - az új förmver verzió minősített hitelesítés-szolgáltatáshoz történő felhasználhatóságát egy erre kijelölt hazai tanúsító szervezet megfelelőségi tanúsítványba foglalja[105], s mint ilyen, az új verzió is bekerül az NHH biztonságos elektronikus aláírási termék nyilvántartásába.

7.2.4 Egyéb, az érvényességet befolyásoló megjegyzések

17. A National Institute of Standards and Technology (NIST) által kibocsátott tanúsítványok visszavonásig érvényesek. Így a tanúsítványokban szereplő hardver, förmver és szoftver konfigurációk változatlan formában használhatók.

18. A FIPS 140-1 szerint tanúsított modulok továbbra is biztonságosnak tekinthetők. A FIPS 140-1 szerinti tanúsítványok azonban 2002. május 26. után nem adhatók ki.

19. Nyilvános források között jelenleg nem található olyan információ, mely befolyásolná a modul biztonságos működését. Ezt a vizsgálatot legalább 3 évente szükséges elvégezni.

[104] Valószínűleg különböző feltételekkel és megkötésekkel, a FIPS 140 megfelelőséget biztosító üzemmód meghatározásával.
[105] Valószínűleg további feltételekkel és megkötésekkel, a minősített hitelesítés-szolgáltatáshoz történő felhasználhatóság kiegészítő szempontjainak meghatározásával.

8. A tanúsításhoz figyelembe vett dokumentumok

8.1 Termékmegfelelőségi követelményeket tartalmazó dokumentumok

Az elektronikus aláírásról szóló 2001. évi XXXV. törvény

3/2005. (III.18.) IHM rendelet az elektronikus aláírással kapcsolatos szolgáltatásokra és ezek szolgáltatóira vonatkozó részletes követelményekről

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

FIPS 140-1: Security Requirements for Cryptographic Modules

Derived Test Requirements for FIPS 140-1

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

8.2 A tanúsítási jelentéshez figyelembe vett egyéb dokumentumok

Kérelem /a tanúsítás elvégzésére/

Kérdőív a tanúsítás kérelmezéséhez

CEN 14167-2 munkacsoport egyezmény: Cryptographic Module for CSP Signing Operation – Protection Profile (CMCSO-PP, HSM-PP)

CEN 14167-3 munkacsoport egyezmény: : Cryptographic Module for CSP Key Genaration Services – Protection Profile (CMCKG-PP, HSM-PP)

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/

Eracom Technologies official notification about name change of CSA 8000 Adapter

Frequently Asked Questions for the Cryptographic Module Validation Program

9. Rövidítések

AES	Advenced Encryption Standard
API	Application Programming Interface
CBC	Cipher Block Chaining
CEN	European Comittee for Standardization
CMCKG	Cryptographic Module for CSP Key Generation Services
CMCSO	Cryptographic Module for CSP Signing Operations
Cprov	Cryptoki (PKCS #11) Provider
CSE	Communications Security Establishment
DAC	Data Authentication Code
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/
ECB	Electronic Code Book
EDC	Error Detecting Code
EEPROM	Electrically Erasable Programmable Read Only Memory
EMI	Electromagnetic Interference
EMC	Electromagnetic Compability
ETSI	European Telecommunication Standards Institute
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 Code
HSM	Hardware Security Module
IDEA	International Data Encryption Algorithm
ISSS	Information Society Standardization System
IT	Information Technology
ITSEC	Information Technology Security Evaluation Criteria
MAC	Message Authentication Code
NIST	National Institute of Standards and Technology
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-PP	Secure Signature Creation Device – Protection Profile
Triple-DES	/FIPS PUB 46-3, ANSI X9.52/
TS	Technical Specification