Tanúsítási jelentés

Hung-TJ-40-2008

a Luna CA^3 kriptográfiai token

kriptográfiai modulról

/SafeNet Inc./

/hardver verzió: 2,
förmver verzió: 3.102/

Verzió:	1.0
Fájl:	HUNG_TJ_40_2008_v10.pdf
Minősítés:	Nyilvános
Oldalak:	49

Változáskezelés

Verzió	Dátum	A változás leírása
v0.1	2008.01.21	A szerkezet felállítása
v0.9	2008.02.04	Egyeztetésre kiadott változat
v1.0	**2008.02.13**	**Végleges verzió**

A tanúsítási jelentést készítette:

Juhász Judit
HunGuard Kft
Tanúsítási divízió

Tartalom

1. A Tanúsítási jelentés tárgya, feladata és hatóköre 6

2. A Luna CA^3 legfontosabb tulajdonságainak összefoglalása 7

2.1 A kriptográfiai modul 7

2.2 Biztonsági szabályok 7

2.3 Működés szabályzat 8

2.3.1 Fix szabályok 8

2.3.2 Változtatható szabályok 8

2.4 Azonosítás és hitelesítés 9

2.4.1 Belépés 9

2.4.2 Nagy rendelkezésre állású mentés támogatása 9

2.4.3 Hitelesítési adatok és megbízható út 9

2.4.4 Belépési hibák korlátai 9

2.4.5 N-ből M aktiválás 9

2.5 Token Hozzáférési Szabályozás 10

2.5.1 Objektum újrafelhasználás 10

2.6 Fizikai biztonság 10

3. A FIPS Tanúsítvány eredményeinek összefoglalása 11

4. A Luna CA^3 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

4.5.3 Több chipes, önmagában álló 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 18

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 Luna CA[3] 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, önmagában álló 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 36
5.8.7 Kulcs archiválásra vonatkozó követelmények 36

5.9 Kriptográfiai algoritmusok 36

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 37
5.11.2.1 Általános tesztek 37
5.11.2.2 Kriptográfiai algoritmus tesztek 38
5.11.2.3 Szoftver/förmver teszt 38
5.11.2.4 Kritikus funkciók tesztjei 38
5.11.2.5 Statisztikus véletlenszám generátor tesztek 38
5.11.3 Feltételhez kötött tesztek 39
5.11.3.1 Páronkénti konzisztencia teszt 39
5.11.3.2 Szoftver/förmver betöltési tesztek 39
5.11.3.3 Kézi kulcs bevitel tesztje 39
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

8. A tanúsításhoz figyelembe vett dokumentumok 48

8.1 Termékmegfelelőségi követelményeket tartalmazó dokumentumok 48

8.2 A tanúsítási jelentéshez figyelembe vett egyéb dokumentumok 48

9. Rövidítések 49

1. A Tanúsítási jelentés tárgya, feladata és hatóköre

Jelen Tanúsítási jelentés tárgya a Luna CA^3 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 Luna CA^3 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 Luna CA^3 PCI 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 Luna CA^3 kriptográfiai adapter egyéb, köztük a FIPS 140-1 tanúsítvánnyal igazolt tulajdonságaira, beleértve az alábbiakat:

- A FIPS 140-es Tanúsítvány érvényességébe tartozó, FIPS által jóváhagyott titkosító algoritmusra /DES, DES MAC, TripleDES, Triple DES MAC, RSA, SHA-1, DSA/,
- a Luna CA^3 adapter által megvalósított azon kriptográfiai algoritmusokra, melyek nem FIPS által jóváhagyott algoritmusok, s így már a FIPS értékelés sem terjedt ki rájuk /RC2, RC4, RC5, CAST, CAST 3, CAST 5, CAST MAC, CAST 3 MAC, CAST 5 MAC, MD2, MD5, Diffie-Hellman (kulcsegyeztetés), RSA (kódolás, dekódolás)/.

A Tanúsítási jelentés további szerkezete a következő:

- A Luna CA^3 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).

[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.

2. A Luna CA^3 legfontosabb tulajdonságainak összefoglalása

2.1 A kriptográfiai modul

A Luna modul biztonságosan tárolja az adatokat és a kulcselemeket a kriptográfiai határon belül. Kriptográfiai műveleteket hajt végre egy külső alkalmazás által szolgáltatott adaton, a benne tárolt kulcselemek segítségével. Rendelkezik tehát kulcsmenedzsment, objektummenedzsment és kriptográfiai képességekkel.

Mielőtt a Luna token kriptográfiai vagy kulcs/objektum menedzsment műveleteket hajthatna végre, egy valós kezelői azonosítót (más néven felhasználói számot) és megfelelő hitelesítési adatokat kell kapnia. Ez a két bemeneti adat a „LOGIN" folyamat során kerül a modulba. Ha a belépés sikeres volt, lehetőség nyílik a token beállított szabályain alapuló műveletek elvégzésére. A Luna CA^3 modulba való belépéshez a hitelesítési adatot a Luna PIN Entry Device-on (PED) keresztül kell megadni, mely biztonságos adatutat szolgáltat, függetlenül a gazdaszámítógéptől.

Két típusú felhasználót lehet megkülönböztetni: a super-usereket és a normal usereket. A super-userekre a későbbiekben Security Officerként (SO), a normal userekre Userként fog hivatkozni a dokumentum. A tokennek csak egy SO felhasználója lehet. Az SO tudja végrehajtani az összes kriptográfiai, kulcs- és objektummenedzsment műveletet, valamint azon funkcióhalmazokat, melyet SO funkcióknak hívnak. Ezek az SO funkciók csak az SO részére állnak rendelkezésre, ezekkel lehet a token szabályait beállítani.
A modulban nincs meghatározva, hogy hány felhasználót hozhat létre az SO. Minden felhasználó az SO által meghatározott szabályok szerint tudja használni a tokent. Viszont minden user rendelkezik egy egyedi azonosítóval, melyet az SO felügyelete alatt generálnak a felhasználó létrehozásakor. Ez védi a User adatait a modulon belül.

A Luna CA^3 a FIPS 140-1 előírásainak megfelelően védi a kritikus biztonsági paramétereket. A kritikus biztonsági paraméterek (CSP) az SO és a Userek hitelesítési kódjához, a klónozási tartomány azonosítóhoz és az N-ből M titokmegosztáshoz kötődnek. Ezeket a CSP-ket a tokenekben csak biztonságos adatutakon keresztül lehet kicserélni, függetlenül a gazdaszámítógéptől. A biztonságos adatút egy dedikált adatporton keresztül biztosított, mely egy PC Card olvasó közvetlenül a modulban. A felhasználói interfész ehhez az adatporthoz egy PIN beíró eszköz (PED). A PED felhasználásával a felhasználó tárolni tudja a pszeudovéletlen hitelesítési kódját, a klónozási tartományazonosítót vagy az N-ből M titkot egy Datakey memóriakulcson. Ezen CSP-k bármelyikét csak úgy lehet bevinni a tokenbe, ha a User rendelkezik a tokennel, a PED-del, egy olvasóval, mely képes biztosítani a kommunikációt a PED és a modul között és egy Datakey kulccsal, mely tartalmazza a hitelesítési adatot, a klónozási tartomány azonosítót és az N-ből M megosztásokat.

2.2 Biztonsági szabályok

A Luna modul biztonsági működését a következő biztonsági szabályok határozzák meg:

- Működési Szabályzat
- Azonosítási és Hitelesítési Szabályzat
- Token Hozzáférési Szabályzat
- Fizikai Biztonsági Szabályzat

Ezek a szabályok kiegészítik egymást annak érdekében, hogy biztosítsák a kriptográfiai elemek biztonságos kezelését a modul teljes életciklusában, és az egyéb adatokhoz és funkciókhoz való megfelelően ellenőrzött hozzáférést. A változtatható paraméterek, melyek a modul különböző viselkedéséért felelősek, a magasszintű Működési Szabályzatban vannak implementálva, kétfajta beállításhalmazon keresztül. Ezek a fix szabályok és a változtatható szabályok.
Az Azonosítási és Hitelesítési Szabályzat felelős a biztonsági beállítások betartatásáért. A fő funkcionális biztonsági szabályzat a Token Hozzáférési Szabályzat.

Biztonsági audit funkciókat nem nyújt a modul, hanem feltételezi, hogy az audit folyamatok a működési környezet részei.

2.3 Működés szabályzat

A Luna modul a Működési Szabályzat Vektorok elvét alkalmazza a token általános viselkedésének szabályozására. A vektorok szabályozzák a hozzáférést bizonyos kritikus műveletekhez, mint a token klónozás, és az olyan biztonságilag kritikus paraméterek beállítása, mint a maximális sikertelen belépési kísérletek száma. A Működési Szabályzat két alszabályzatra van osztva, mindkettő szabályzat vektorok segítségével. Ezek a Fix Szabályok és a Változtatható Szabályok. A Fix Szabályok gyártás során kerülnek beállításra, később nem módosíthatók. A Változtatható Szabályokat az SO állítja be az inicializációs folyamat során, később újabb inicializálással ezek megváltoztathatók.

2.3.1 Fix szabályok

A fix szabályokat a Fix Szabályzat Vektor (FPV) beállításai határozzák meg. Az FPV tartalmazza azokat a beállításokat, melyek szükségesek azon szabályok betartatásához, melyek mellett a modul változatos felhasználási területeken és környezetekben képes működni.

Egyetlen felhasználó, még az SO sem tudja ezeket a beállításokat megváltoztatni. Az FPV a gyártás során kerül a modulba, és egészen addig működik, amíg a modult meg nem semmisítik, vagy a förmverét le nem törlik. Az FPV integritását ugyanúgy védik, mint a futtatható kódokét. Ez a mechanizmus a 32 bites Ciklikus Redundancia Ellenőrzés (CRC).
Az FPV egy 32 bites vektor, ami négy részre van osztva. A vektorban a következő funkciókat lehet beállítani:

- A megengedett sikertelen SO belépési kísérletek száma
- Titkos kulcs szabályok
- Nyilvános kulcs szabályok
- Token biztonsági szabályok
- Termékazonosítás

2.3.2 Változtatható szabályok

A változtatható szabályokat a Token Szabályzat Vektor (TPV) beállításai határozzák meg. A TPV tartalmazza azokat a beállításokat, melyek szükségesek azon szabályok betartatásához, melyeket a helyi szervezet ír elő. Például itt határozza meg az egyik bit, hogy a modul végrehajthat-e aláírási műveletet máshol generált aláíró kulccsal vagy ez csak a modulban generált kulcs felhasználásával történhet. A TPV-t a modul SO-ja módosíthatja. A TPV tartalmát használja fel a belső kód ahhoz, hogy a felhasználók által végrehajtott műveleteket érvényesítse.

A TPV egy 32 bites vektor, ami négy 8 bites részre van osztva. Ezek a következők:

A megengedett sikertelen user belépési kísérletek száma: Ez a mező határozza meg, hogy hány egymást követő hibás belépési próbálkozás után zárja ki a modul a felhasználót, és törli adatait. Ezzel a biztonsági beállítással lehet megakadályozni a felhasználó adataihoz és kulcsaihoz való illetéktelen hozzáférést, valamint a hitelesítési adatok illegális megváltoztatását. Az alapbeállítás 10 próbálkozást enged meg.

Az, hogy a User ki lesz zárva vagy az adatai is törlődnek, a „User törlése” bit beállításától függ. Ha ez a bit nincs beállítva, a sok hibás próbálkozás után a felhasználó ki lesz zárva. Ha ez megtörténik, az SO-nak kell újra aktiválnia a felhasználót. Az SO új jelszót is tud adni a felhasználónak. Ha a „User törlése” bit be van állítva, a túl sok hibás próbálkozás után a felhasználó törlődik. Ekkor a User azonosítója és titkos adatai (a kulcselemek is) törlődnek. Az SO-nak új felhasználót kell létrehoznia a munka folytatásához. Az új felhasználónak nem lesz kapcsolata a törölt felhasználóval. Alapbeállítás szerint a „User törlése” bit be van állítva.

Minimális/maximális Hitelesítő Kód Hosszúság: ennek a mezőnek nincs hatása a Luna CA^3 működésére, mert ebben az esetben a hitelesítési kód pszeudovéletlen módon generálódik, és a PED kártyán tárolódik. Hossza 48 byte. A felhasználó létrehozásakor az SO egy maximum 16 számjegyből álló PIN kódot kérhet a PED-en keresztül, a 48

byte-os generált titok mellé. A PIN kód a PED-en belül egyesül a token által generált titokkal, és ezzel kialakul a kártyán tárolt érték.

Helyi szabályok

Helyi szabályok – kiterjesztett TPV

2.4 Azonosítás és hitelesítés

A Luna modul identitás alapú azonosítást használ. A felhasználók egy felhasználói számmal vannak azonosítva a modulban. Az SO egy speciális számot kap. A token három szerepkört azonosít: nyilvános, Token User és Security Officer. A nyilvános hozzáférés nem azonosított és nem hitelesített, így a funkcióknak csak olyan limitált halmazát képesek használni, mint kapcsolat kezdeményezése a modullal és előre definiált diagnosztika elindítása. Ezzel a jogosultsággal nem lehet kriptográfiai műveleteket végezni. Az SO egy kiemelt szerepkör, akinek első feladata a modul kezdeti konfigurációja, valamint a biztonsági adminisztráció, pl. a felhasználók létrehozása. A Token User szerepkör a hitelesített felhasználóknak jár normális működési körülmények között.

2.4.1 Belépés

Egy felhasználónak ahhoz, hogy User vagy SO szerepkört tölthessen be, kriptográfiai műveleteket hajthasson végre és a nyilvános hozzáférésen túli funkciókat érhessen el, azonosítania és hitelesíteni kell magát. A Token User-nek ehhez felhasználói számmal és érvényes hitelesítési adatokkal (pl. jelszó vagy Datakey eszközön tárolt adat) kell rendelkeznie, csak ezeknek az adatoknak a bevitele után tud hozzáférni a személyes adatokhoz és a token szolgáltatásaihoz. Az SO-nak csak érvényes hitelesítési adatokat kell szolgáltatnia. Ha az N-ből M hitelesítés aktiválva van, egyetlen Token User vagy SO sem érheti el a modult addig, amíg az N-ből M hitelesítés feltételei nem teljesülnek.

2.4.2 Nagy rendelkezésre állású mentés támogatása

A Luna CA^3 támogatja az indirekt belépést, aminek segítségével két Luna CA^3 modul között megoldható az azonnali adatmentés. Engedélyezett egy mentésre használt Luna CA^3 használata, ahol a hitelesítés közös az elsődleges modullal, ugyanabban a tartományban vannak, és ezáltal automatikusan tudja visszaállítani az adatokat az elsődleges eszköz hibája esetén.

2.4.3 Hitelesítési adatok és megbízható út

A hitelesítési adatok több fajtája létezik. A Luna CA^3 modulok esetében az adat elsődleges formátuma a token által generált véletlen adat, mely a PED kártyáján van tárolva, a felhasználó ezt adja meg a hitelesítés során. A modul elvárja, hogy a hitelesítési adatok és az N-ből M megosztások a gazda IT környezettől független adatúton kerüljenek bele. Az SO a felhasználó létrehozásakor egy maximum 16 számjegyből álló PIN kódot is kérhet, mely a generált adattal kombinálódva további bizalmat szolgáltat. A hitelesítési adat 48 byte-ból áll.

2.4.4 Belépési hibák korlátai

A Luna modul alkalmazza a maximális belépési próbálkozások számának szabályait. A szabályok különbözőek az SO és a Token Userek esetében. Ha a Token User túllépi azt az egymás utáni „y” próbálkozást, ami be van állítva, a token feljegyzi ezt az eseményt, és a szabályzatnak megfelelően kezeli a helyzetet. Ha az SO túllépi a három egymás utáni próbálkozást, adatai törlésre kerülnek, a modult újra kell inicializálni a működés folytatásához.

2.4.5 N-ből M aktiválás

A Luna CA^3 modul támogatja az N-ből M aktiválást. Az N-ből M aktiválás lényege, hogy a titokadatot N részre bontja fel, melyből legalább M résszel kell rendelkezni ahhoz, hogy vissza lehessen állítani az eredeti titkot. A modul ezt a Shamir küszöb séma alapján tudja végrehajtani. Ez lehetőséget nyújt arra, hogy a titkot n résztvevő között osszák szét annak a veszélye nélkül, hogy a titok kiderül.

Az N-ből M aktiválást akkor kell végrehajtani, amikor még semmilyen állandó érzékeny adat nincs a modulban. Ellenkező esetben fennáll a veszélye annak, hogy az aktiválás előtt tárolt adatok megsérülnek a visszaállításkor. Az N-ből M aktiválást az SO-nak kell beállítania.

Az N-ből M adatdarabok egynél több token között is megoszthatók a tartományon belül. Ezt az inicializáláskor kell beállítani. Az N-ből M titkok biztonsági mentéséhez is ez az eljárás használható.

Az M és az N értéke legalább kettő kell, hogy legyen.

2.5 Token Hozzáférési Szabályozás

A Token Hozzáférési Szabályozás (TAC) a modulon tárolt összes objektumra vonatkozik, különösen a nyilvános és titkos kulcs objektumokra, és lefedi a következő műveleteket:

Létesítés
Olvasás
Másolás
Módosítás
Megsemmisítés
Generálás
Származtatás
Becsomagolás
Kicsomagolás
Használat (titkosítás, detitkosítás, aláírás, ellenőrzés)
Klónozás

A szabályok a következő állításokkal összegezhetők:

Egy felhasználó akkor hajthat végre egy műveletet egy objektumon, ha a következő két pontból egy teljesül:
Az objektum nyilvános objektum, azaz a PRIVATE attribútum hamis, vagy
A felhasználó birtokolja az objektumot.
Azok a megengedett műveletek, melyek a Fix és a Változtatható Szabályokban engedélyezettek.

A modul nem enged annál finomabb hozzáférési szabályozást, minthogy egy objektum nyílt vagy bizalmas (azaz egy objektumnak nem lehet két gazdája úgy, hogy a többi felhasználó nem fér hozzá). Az objektum tulajdonjoga teljes hozzáférést jelent az adott objektumhoz, ezt azonban a tulajdonos nem tudja átruházni más felhasználókra. Az objektum attribútumai a következők lehetnek: bizalmas, érzékeny, módosítható, kibontható.

2.5.1 Objektum újrafelhasználás

A Token Hozzáférési Szabályozást támogatja az Objektum Újrafelhasználási Szabályozás. Ez azt határozza meg, hogy ha az erőforrások egy objektumot használnak, akkor minden ehhez az objektumhoz tartozó információt töröljenek, mielőtt egy másik objektumhoz férnek hozzá.

2.6 Fizikai biztonság

A Luna hardverek olyan módon vannak összeállítva, hogy ellenálljanak a kártyához való fizikai hozzáférésnek, és ne lehessen a bennük található áramkört a tartalom sérülése kiszedni. Bizonyítékot adnak minden fizikai behatásról, és garantálják, hogy egy ilyen próbálkozás olyan állapotban hagyja a modult, hogy az használhatatlan legyen vagy legalább annyira sérüljön meg, hogy a rajta levő adatok ne legyenek visszaállíthatóak.

3. A FIPS Tanúsítvány eredményeinek összefoglalása

A Luna CA[3] egy kriptográfiai modulok tesztelésére az Egyesült Államokban és Kanadában akkreditált laboratórium[3] 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, önmagában álló/:	3-as szint
Szoftver biztonság:	3-as szint
Az operációs rendszer biztonsága:	nincs értékelve[4]
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/SHA-1, RSA,**

Az értékelés az alábbi titkosításhoz kapcsolódó[5], FIPS által jóváhagyott algoritmusok megvalósítását vizsgálta, tesztelte: **DES, DES MAC, Triple-DES, Triple-DES MAC**

Az elért általános biztonsági szint: 3-as

[3] a DOMUS IT Laboratory /NVLAP LAB CODE 200017-0/
[4] Minthogy a nevezett IT terméknek nincs saját operációs rendszere
[5] jelen Tanúsítási jelentés hatókörén kívül álló,

4. A Luna CA^3 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 Luna CA^3 értékelését végző laboratórium vizsgálta és igazolta.

Az alábbi jelölést alkalmazzuk:

KÖV_x.y: a FIPS 140-1 x. fejezetének y. biztonsági követelménye.[6]

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

[6] Csak azokat a követelményeket adjuk meg, mely a Luna CA^3 kriptográfiai modulra ténylegesen vonatkoznak, ezért a követelmények sorszámozása nem mindig folyamatos.
[7] FIPS 140-1

4.2 Modul interfészek

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

KÖV_02.02:
A modulnak legalább a következő négy logikai interfészt tartalmaznia kell:
adat input interfész,
adat output interfész,
vezérlési input interfész,
státusz output interfész.

KÖV_02.03:
A modul tartalmazhatja a következő logikai interfészeket is:
elektromos áram interfész,
karbantartói hozzáférési interfész[8].

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.

[8] A Luna CA[3] 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[9].
Ha a modul több egyidejű operátort támogat[10], 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[11].

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

[9] Mivel a Luna CA[3] 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.
[10] A Luna CA[3] támogat több egyidejű operátort.
[11] A Luna CA[3] 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[12] 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[13]:
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:

[12] 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).
[13] 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-tesz állapotok: olyan állapotok, amelyek a modul ön-tesztjének végrehajtására szolgálnak /lásd 11. fejezet (Ön-teszt)/,
- Hiba állapotok: olyan állapotok, amelyekbe a modul hiba fellépésekor kerül (pl. sikertelen ön-teszt, titkosítás megkísérlése olyan esetben, amikor működéshez szükséges kulcsok vagy más kritikus biztonsági paraméterek hiányoznak, vagy kriptográfiai hibák lépnek fel). A hiba állapotok felölelhetnek működést kizáró (hard) hibákat, amelyek egy készülék hibáját jelzik és a modul karbantartását vagy javítását igénylik, és felölelhetnek helyreállítható (soft) hibákat, amelyek a modul inicializálását vagy “reset”-elését igényelhetik.

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

- Nem-inicializált állapotok: olyan állapotok, amelyekben nincsenek a modulba betöltve a működéshez szükséges biztonsági paraméterek,
- Üresjárati állapotok: olyan állapotok, amelyekben a modul elvileg működőképes, de éppen nem nyújt biztonsági szolgáltatásokat, illetve nem hajt végre kriptográfiai funkciókat. A kriptográfiai kulcsok és biztonsági paraméterek be vannak töltve, és a modul adatra vagy vezérlő inputra vár.
- Biztonsági zár állapotok: olyan állapotok, amelyekben a modul az adott pillanatban nem működőképes, bár a kriptográfiai kulcsok és paraméterek be vannak töltve. Ezen állapotok arra szolgálnak, hogy védelmet nyújtsanak a modul számára a jogosulatlan felhasználással szemben az operátor ideiglenes távolléte esetén.
- Megkerülési állapotok: olyan állapotok, amelyek kriptográfiai műveletek nélküli szolgáltatásokat tesznek lehetővé (pl. nyílt szövegek továbbítását a modulon keresztül),
- Karbantartási állapotok: olyan állapotok, amelyek a modul karbantartására és szervizelésre szolgálnak, beleértve a karbantartási tesztek végrehajtását.[14]

KÖV_04.07:
Bármilyen hiba állapot esetén az adat output interfészen keresztül történő minden adat outputot le kell tiltani[15].
KÖV_04.08:

[14] A Luna CA[3] kriptográfiai modulnak nincs se biztonsági zár, se karbantartási, se megkerülési állapota, így ez a fejezet nem tartalmazza az ezekre vonatkozó KÖV_04.09 és KÖV_04.10 követelményeket.
[15] Ez a követelmény hasonló a 2. fejezet (Modul interfészek) KÖV_02.04 követelményéhez.

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[16]

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.

4.5.3 Több chipes, önmagában álló kriptográfiai modulra vonatkozó követelmények

KÖV_05.15[17]:
Több chipes, önmagában álló kriptográfiai modul esetén a modulban lévő chipeknek olyan termék minőségűeknek kell lenniük, amelyek magukban foglalnak standard passziválási technikát is.

KÖV_05.16:
Több chipes, önmagában álló kriptográfiai modul esetén a modult termék szintű több chipes formában kell megvalósítani.

KÖV_05.17:
Több chipes, önmagában álló kriptográfiai modul esetében a modult egy fém vagy kemény műanyag házzal kell beburkolni mely tartalmazhat nyílásokat és eltávolítható fedeleket.

KÖV_05.18:
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_05.19:
Több chipes, beágyazott kriptográfiai modul esetében, ha a modul valamilyen szellőzőnyílást tartalmaz, azt olyan módon kell megtervezni, hogy az meggátoljon minden észrevétlen szondázást.

[16] Vagyis a kriptográfiai modul mindhárom lehetséges fizikai konfigurációjára (egy chipből álló, több chipes, beágyazott, illetve több chipes, önmagában álló) vonatkozik.
[17] Ez a fejezet nem tartalmazza a csak az egy chipből álló kriptográfiai modulokra vonatkozó KÖV_05.02 - KÖV_05.06 követelményeket, valamint a csak a több chipes, beágyazott kriptográfiai modulokra vonatkozó KÖV_05.07 - KÖV_05.14 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[18].

4.7 Az operációs rendszer biztonsága

Nincsenek követelmények[19].

4.8 Kriptográfiai kulcsgondozás

4.8.1 Általános követelmények

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

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

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

4.8.2 Kulcs generálásra vonatkozó követelmények

KÖV_08.04:

[18] Ez a fejezet nem tartalmazza a csak a 4-es biztonsági szintre vonatkozó KÖV_06.07 - KÖV_06.10 követelményeket.
[19] Mivel a Luna CA[3] kriptográfiai modulnak nincs saját operációs rendszere.

Egy kriptográfiai modul opcionálisan ki lehet egészítve egy belső kulcs generálási funkcióval[20]. 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[21], 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[22], 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.

KÖV_08.15[23]:

[20] A Luna CA^3 megvalósít belső kulcs generálási funkciót.
[21] A Luna CA^3 alkalmaz véletlenszám generátort.
[22] A Luna CA^3 véletlenszám generátora alkalmaz kezdeti *(seed)* kulcsot.

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.

[23] 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[24]:
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[25] 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:

[24] 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.
[25] 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[26].

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.

[26] Mivel a Luna CA[3] 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[27]:
A statisztikai teszteknek igény esetén meghívhatóknak kell lenniük. Idevonatkozó követelmény a KÖV_11.09 is.

[27] 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[28].

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[29].

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.

[28] A Luna CA^3 adapterbe lehetséges kívülről szoftvert betölteni (upgrade céljából). Ilyenkor csak az Chrysalis-ITS Inc. gyártó cég digitálisan aláírt szoftverét fogadja el a modul.
[29] A Luna CA^3 modul nem támogatja a kézi kulcsbevitelt.

5. A Luna CA^3 értékeléshez megkövetelt fejlesztői bizonyítékok

Az alábbiakban áttekintjük azokat a fejlesztői bizonyítékokat (dokumentálást, egyéb információ szolgáltatást), melyet a fejlesztő cég biztosított a vizsgálatok elvégzéséhez a Luna CA^3 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[30], 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.

[30] A Luna CA[3] 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[31],
- A kriptográfia megkerülése[32].

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:

[31] A Luna CA[3] modulban nincsenek karbantartói tesztek.
[32] A Luna CA[3] 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[33]. 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, önmagában álló kriptográfiai modulra vonatkozó követelmények

FB_05.15.01:
A több chipes, önmagában álló 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_05.16.01:
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_05.17.01:
A modult egy fém vagy kemény műanyag burkolattal kell befedni, mely tartalmazhat nyílásokat vagy eltávolítható fedeleket. Ennek a keménységét a fejlesztői dokumentációban le kell írni.

[33] A Luna CA[3] esetében ez: több chipes, önmagában álló modul.

FB_05.18.01:

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_05.20.01:
A fejlesztői dokumentációnak rögzítenie kell, hogy a KÖV_05.10-ben specifikált két 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, 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.

FB_05.21.01:
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).

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 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[34].

5.8. Kriptográfiai kulcsgondozás

5.8.1 Általános követelmények

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

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

[34] Mivel a Luna CA[3] kriptográfiai modulnak nincs saját operációs rendszere.

   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[35], 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.

[35] A Luna CA[3] egy hardver véletlenszám generátort alkalmaz, kombinálva egy FIPS által jóváhagyott véletlenszám generálási technikával (FIPS 186-2).

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

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[36], 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[37].
Megjegyzés: A fejlesztő beépíthet a kriptográfiai modulba más (azaz nem FIPS által jóváhagyott) kriptográfiai algoritmusokat is[38].

[36] A Luna CA[3] támogatja a titkos kulcsok és a különböző magán kulcsok archiválását (komponensekre bontva, kódolt formában, intelligens kártyákon tárolva).
[37] A Luna CA[3] rendelkezik ilyen tanúsítvánnyal a DES, Triple-DES, DSA, SHA-1 és RSA kriptográfiai algoritmusokra.
[38] A Luna CA[3] megvalósít több FIPS által nem jóváhagyott kriptográfiai algoritmust is, köztük az alábbiakat: RSA (kódolás,dekódolás), CAST, CAST 3, CAST 5, CAST MAC, CAST 3 MAC, CAST 5 MAC, RC2, RC4, MD2, MD5, Diffie-Hellman (kulcsegyeztetés).

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 hiba jelzést.

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

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. 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.

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[39]. 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[40]. 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:

[39] A Luna CA[3] a gyártó cég (Chrysalis-ITS, Inc.) 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.
[40] A Luna CA[3] rendelkezik ilyen tanúsítvánnyal (DSA, SHA-1, RSA).

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.

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[41]. 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):
  - 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

[41] A Luna CA[3] által alkalmazott technika az új szoftver digitális aláírása (RSA algoritmussal) a fejlesztő cég által, illetve az upgrade betöltésekor az aláírás ellenőrzése az adminisztrátor által.

FB_11.21.02:
Ha a hiba detektáló kódot alkalmazzák, 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[42], a fejlesztőnek dokumentálnia kell a folyamatos véletlenszám generátor tesztet.

[42] Mint ahogy a Luna CA[3], mely egy hardver véletlenszám generátort alkalmaz, kombinálva egy FIPS által jóváhagyott (pszeudó) véletlenszám generálási technikával (FIPS 186-2).

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[43]:

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][44]
A minősített tanúsítvány aláíró kulcsokat biztonságos kriptográfiai modulban kell előállítani.

[KM1.2][45]
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][46].

[KM1.3][47]
A kriptográfiai modul a minősített tanúsítvány aláíró kulcsokat csak kettős ellenőrzés alatt állíthatja elő[48].

[43] Mely kulcs kategóriák megegyeznek a 2/2002 MeHVM irányelv 73. pontjában definiáltakkal.
[44] Lásd a 2/2002 MeHVM irányelv 75. pontját.
[45] Lásd a 2/2002 MeHVM irányelv 75. pontját.
[46] 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.
[47] Lásd a 2/2002 MeHVM irányelv 76. pontját.
[48] Megjegyzés: A kettős ellenőrzési követelmény teljesíthető akár közvetlenül a kriptográfiai modul által, akár úgy, hogy a hitelesítés-szolgáltató kettős személyi ellenőrzést alkalmaz.

[KM1.4][49]
Az infrastrukturális kulcsokat biztonságos kriptográfiai modulban kell előállítani.

[KM1.5][50]
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 [51].

[KM1.6][52]
A rendszervezérlési kulcsokat biztonságos kriptográfiai modulban kell előállítani[53].

[KM1.7][54]
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[55].

[KM6.1][56]
Minden magán- vagy titkos kulcsot biztonságosan kell tárolni.

[KM6.2][57]
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][58]
A magán- vagy titkos rendszervezérlési kulcsokat biztonságos kriptográfiai modul(ok)ban kell tárolni.

[KM6.4][59]
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][60]
A minősített tanúsítvány aláírására használt kulcsot csak a minősített tanúsítványok, illetve esetlegesen a rájuk vonatkozó visszavonási listák aláírására szabad felhasználni.

[49] Lásd a 2/2002 MeHVM irányelv 77. pontját.
[50] Lásd a 2/2002 MeHVM irányelv 77. pontját.
[51] Lásd [KM1.2] alatti megjegyzést.
[52] Lásd a 2/2002 MeHVM irányelv 78. pontját.
[53] Megjegyzés: Ennek a biztonságos kriptográfiai modulnak legalább a [FIPS-140-1] 1-es szintjének, vagy más megfelelő szabványnak kell megfelelnie.
[54] Lásd a 2/2002 MeHVM irányelv 79. pontját.
[55] Lásd a 2/2002 MeHVM irányelv irányelvek 1. sz. mellékletében felsorolt jóváhagyott kulcs generáló algoritmusok listáját.
[56] Lásd a 2/2002 MeHVM irányelv 104. pontját.
[57] Lásd a 2/2002 MeHVM irányelv 106. és 107. pontját.
[58] Lásd a 2/2002 MeHVM irányelv 108. pontját.
[59] Lásd a 2/2002 MeHVM irányelv 109. pontját.
[60] Lásd a 2/2002 MeHVM irányelv 94. és 160.pontját.

[CG1.6] [61]
A megbízható rendszer által kibocsátott minősített tanúsítványnak meg kell felelnie a Törvény 2. mellékletében meghatározott követelményeknek. Különösen az alábbi tulajdonságoknak kell meglenniük[62]:

1….
2…
3…
4…
5. A megbízható rendszer által a minősített tanúsítvány aláírásához használt aláírási algoritmusok/kulcsok az alábbiak valamelyike lehet:[63]
   - 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][64]
Az időbélyegzés-szolgáltató aláíró kulcsait biztonságos kriptográfiai modulban kell előállítani és tárolni.

[TS4.2][65]
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[66]

[TS4.3][67]
Az időbélyegzés-szolgáltató rendszervezérlési kulcsait biztonságos kriptográfiai modulban kell tárolni.

[TS4.4][68]
Az időbélyegzéshez használt aláíró kulcsokat kizárólag az adott időbélyegzés-szolgáltató által létrehozott időbélyegek aláírására szabad használni.

[TS4.6][69]
Az időbélyegzés-szolgáltató által használt aláíró algoritmusoknak/kulcsoknak, meg kell felelniük a [CG1.6] alatt felsorolt kriptográfiai követelményeknek.

[61] Lásd a 2/2002 MeHVM irányelv 162/e alpontját.
[62] Csak az 5. Releváns a kriptográfiai modulra.
[63] Lásd a 2/2002 MeHVM irányelv irányelvek 1. sz. mellékletében felsorolt jóváhagyott aláíró algoritmusok listáját.
[64] Lásd a 2/2002 MeHVM irányelv 75. és 212. pontját.
[65] Lásd a 2/2002 MeHVM irányelv 75. és 212. pontját.
[66] Lásd a [KM1.2] alatti megjegyzést.
[67] Lásd a 2/2002 MeHVM irányelv 104. és 213. pontját.
[68] Lásd a 2/2002 MeHVM irányelv 214. pontját.
[69] Lásd a 2/2002 MeHVM irányelv 216. pontját.

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

[KM1.7][70]
Minden kulcselőállításnak[71] 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[72].

[KM3.4][73]
Biztosítani kell, hogy az elektronikus aláírásra szolgáló aláírói kulcsok különbözzenek minden más funkcióra szolgáló kulcstól, mint például a titkosításra szolgálóktól.

[SP1.4][74]
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][75].

[SP1.5][76]
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.

[70] Lásd a 2/2002 MeHVM irányelv 79. pontját.
[71] Így az aláírás-létrehozó eszközön elhelyezendő aláíró magánkulcs generálása is.
[72] Lásd a 2/2002 MeHVM irányelv irányelvek 1. sz. mellékletében felsorolt jóváhagyott kulcs generáló algoritmusok listáját.
[73] Lásd a 2/2002 MeHVM irányelv 95. pontját.
[74] Lásd a 2/2002 MeHVM irányelv 226. pontját.
[75] Lásd a [KM1.2] alatti megjegyzést.
[76] Lásd a 2/2002 MeHVM irányelv 227. pontját.

7. A Tanúsítási jelentés eredménye, érvényességi feltételei

7.1 A Tanúsítási jelentés eredménye

A Luna CA[3] kriptográfiai modul
/SafeNet, Inc./

tanúsítás tárgyát képező verziója
/Hardver verzió: 2, Förmver verzió: 3.102/

a Tanúsítás érvényességi feltételeinek[77] 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[78] aláírására történő felhasználására.

Aláírás-létrehozó eszközön az aláírás-létrehozó adat elhelyezése szolgáltatás keretén belül:
Az előfizetői (aláírói) kulcspár generálására[79].

Fokozott biztonságú elektronikus aláírás létrehozására, melyhez megbízható kriptográfiai alaptámogatást és védett futtatási környezetet biztosít.

7.2 Az eredmények érvényességi feltételei

A Luna CA[3] modul 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.

[77] Lásd a 7.2 "Az eredmények érvényességi feltételei" fejezet 1.-16. feltételeit.
[78] Mely időbélyegzőt a 2001 évi XXXV. törvény az elektronikus aláírásról minősített időbélyegzőként említi.
[79] Amennyiben a kulcspár előállítása az aláírás-létrehozó eszközön kívül történik.

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

Amennyiben a Luna CA^3 modult 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 Luna CA^3 modul szolgáltatásait igénybe vevő különböző munkaköröket (Security Officer, User) betöltő személyek:
   kompetensek, jól képzettek és megbízhatóak, valamint
   betartják a különböző útmutatók (Luna® PKI HSM Installation Guide, Luna® PKI HSM Planning & Integration Guide) által leírt, kötelező tevékenységeket.

7.2.2 A FIPS 140-1 megfelelőségből fakadó érvényességi feltételek

Az alábbi feltételek ahhoz elengedhetetlenek, hogy a Luna CA^3 token megfeleljen a FIPS 140-1 3-as biztonsági szintjének.

2. A biztonságos működéshez csak a tokenhez tartozó alkatrészeket, szoftvereket szabad használni. Ezek a következők:
   Chrysalis-ITS® dual-slot Luna® Dock PC Card Reader
   Luna® Pin Entry Device (PED)
   PED Kulcsok (Datakey® Device)
   Enabler (termékkonfiguráló) szoftver
   Cryptographic API Software

3. A Token Szabályzat Vektor (TPV) bitjeit a következő beállításokkal kell használni:
   TPV_USER_ZEROIZE = 1
   TPV_USER_FW_UPDATE = 0
   TPV_M_OF_N_ACTIVATION = 1
   TPV_KEY_ATTRIB_LOCK = 1
   TPV_KEY_SINGLE_FUNCTION = 0
   TPV_SIGNING_KEY_LOCAL = 1
   TPV_DISABLE_CLONING_BY_USER = 1

4. Mind a Security Officer, mind a User szintű felhasználók generálásánál 6 jegyű PIN kódot kell megadni a PED-en keresztül.

5. Az N-ből M aktiválás beállításakor M és N értékeket, úgy kell megválasztani, hogy $M \geq 2$ és $N \geq M$. Ezt az SO és a User jogosultságú felhasználók generálásakor is figyelembe kell venni.

6. Ha a Luna CA^3 tokent többet nem használják, azt olyan módon kell megsemmisíteni vagy tárolni, hogy semmilyen áramköréhez ne lehessen hozzáférni úgy, hogy abból használható információt lehessen kinyerni.

7. A tokenhez mind fizikai, mind hálózati értelemben csak arra felhatalmazott személyek illetve folyamatok férhetnek hozzá, a token által meghatározott protokollon keresztül.

8. A tokent olyan helyen kell működtetni, ahol nem lehet kitéve erős elektromágneses sugárzásnak, így kikerülve azt, hogy egy rosszindulatú személy megváltoztathassa a token adatait.

7.2.3 A minősített hitelesítés-szolgáltatáshoz történő használhatóság kiegészítő feltételei

Egy minősített hitelesítés-szolgáltatónak a Luna CA^3 modul felhasználása során az alábbi kiegészítő feltételeket is be kell tartania:

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

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

11. Digitálisan aláírni csak 8-cal osztható bithosszúságú blokkot lehet

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

13. 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 alábbiak valamelyikével is:

- az "m az n-ből" technika alkalmazásával (melyet a Luna CA^3 modul támogat), 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 módszerrel:
- a mentés intelligens kártyákra (tokenekre) 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.

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

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 Luna CA^3 kriptográfiai hardverben) történik, biztosítani kell, hogy az elektronikus aláírásra szolgáló aláírói kulcsok különbözzenek minden más funkcióra szolgáló kulcstól, mint például a titkosításra szolgálóktól.

16. A Tanúsítvány csak a jelenlegi hardver és förmver verzióra érvényes / Hardver verzió: 2, Förmver verzió: 3.102/. 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 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, s mint ilyen, az új verzió is bekerül az NHH biztonságos elektronikus aláírási termék nyilvántartásába.

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 v1.3.1 Policy Requirements for Certification Authorities Issuing Qualified Certificates

ETSI TS 102 176-1 V2.0.0 Algorithms and Parameters for Secure Electronic Signatures; Part 1: Hash functions and asymmetric algorithms

CEN 14167-1:2003 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/

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. 214 /Luna CA^3/

Luna® Token Security Policies /Luna CA^3 v3/ Document Number CR-1356

HUNG-TJ-21-2004 Tanúsítási jelentés

9. Rövidítések

CEN	European Comittee for Standardization
CMCKG	Cryptographic Module for CSP Key Generation Services
CMCSO	Cryptographic Module for CSP Signing Operations
CSP	Critical Security Parameter
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
FPV	Fix Policy Vector
HMAC	Hashed (Keyed) Message Authentication Code
HSM	Hardware Security Module
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
PED	PIN Entry Device
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
SO	Security Officer
SHA-1	Secure Hash Algorithm /FIPS PUB 180-1/
SSCD-PP	Secure Signature Creation Device – Protection Profile
TAC	Token Access Control
Triple-DES	/FIPS PUB 46-3, ANSI X9.52/
TPV	Token Policy Vector
TS	Technical Specification