Tanúsítási jelentés

Hung-TJ-070-2015

Luna® PCI-e kriptográfiai modul

Hardware verzió: VBD-05-0100, VBD-05-0101

és VBD-05-0103;

Firmware verzió: 6.2.1

kriptográfiai modulról

mint elektronikus aláírási termék

/ SafeNet Inc. /

Verzió:	1.0
Fájl:	Hung-TJ-070_2015_v02.pdf
Minősítés:	Nyilvános
Oldalak:	72

Változáskezelés

Verzió	Dátum	A változás leírása
v0.1	2015.03.27	A szerkezet felállítása
v02	2015.04.13	Egyeztetésre kiadott változat
v0.9	**2015.04.14**	**Egyeztetésre kiadott változat**
v1.0	2015.04.27	Végleges verzió

A tanúsítási jelentést készítette:

dr. Szabó István
HunGuard Kft.
Tanúsítási divízió

Tartalom

1. A Tanúsítási jelentés tárgya, feladata és hatóköre

Jelen Tanúsítási jelentés tárgya Luna® PCI-e kriptográfiai modul *Hardware verzió: VBD-05-0100, VBD-05-0101 és VBD-05-0103; Firmware verzió: 6.2.1*, 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 és hazai jogszabályok (lásd 9.1 fejezet) irányadók jelen Tanúsítási jelentéshez.

Ezen követelmények közül a CWA14167-1:2003 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]),
- [CC] EAL4 (vagy magasabb) biztonsági szint
- [ITSEC] E3/high (vagy magasabb) biztonsági szint.

A Luna® PCI-e kriptográfiai modul FIPS 140-2 3-as szintű tanúsítvánnyal rendelkezik.

A FIPS 140-2 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® PCI-e kriptográfiai modul alkalmas-e minősített hitelesítés-szolgáltatás nyújtásához való alkalmazásra, s ha igen, akkor mely kapcsolódó feladatokhoz használható,
- a FIPS 140-2 szerinti Tanúsítvány érvényessége, illetve a többi kielégítendő funkcionális és biztonsági követelmény teljesülése milyen korlátozásokat, feltételeket támaszt a kriptográfiai modul használatára.

[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.

Jelen Tanúsítási jelentés hatóköre ugyanakkor csak a minősített hitelesítés-szolgáltatás nyújtásához való alkalmasságra és ennek feltétel-rendszerének meghatározására szorítkozik. Nem terjed ki a Luna® PCI-e kriptográfiai modul egyéb, köztük a FIPS 140-2 Tanúsítvánnyal igazolt tulajdonságaira, beleértve az alábbiakat:

- A FIPS 140-es Tanúsítvány érvényességébe tartozó, FIPS által jóváhagyott titkosító algoritmusra
- a Luna® PCI-e kriptográfiai modul által megvalósított azon kriptográfiai algoritmusokra, melyek a FIPS tanúsítvány kiadásának időpontjában nem FIPS által jóváhagyott algoritmusok, s így már a FIPS értékelés sem terjedt ki rájuk.

A Tanúsítási jelentés további szerkezete a következő:

- A Luna® PCI-e kriptográfiai modul legfontosabb tulajdonságainak összefoglalása (2. fejezet).
- A FIPS Tanúsítvány eredményeinek összefoglalása (3. fejezet).
- A FIPS 140-2-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 Luna® PCI-e kriptográfiai modul sebezhetőség vizsgálata (7. fejezet).
- A minősített hitelesítés-szolgáltatás nyújtáshoz való alkalmasság megállapítása, valamint az alkalmazás feltételeinek és korlátainak a meghatározása (8. fejezet).
- A jelen Tanúsítási jelentéshez figyelembe vett dokumentumok jegyzéke (9. fejezet).
- Felhasznált rövidítések jegyzéke (10. fejezet).

2. A Luna® PCI-e kriptográfiai modul legfontosabb tulajdonságainak összefoglalása

A Luna® PCI-e kriptográfiai modul egy többchipes beágyazott hardver kriptográfiai modul PCI-e kártya formájában, és általában egy számítástechnikai vagy biztonságos kommunikációs eszközön helyezkedik el. A kriptográfiai modul a saját biztonságos borításán belül található, ami fizikai behatolás elleni védelmet nyújt. A modul kriptográfiai határa a PCI-e kártyán a biztonságos borításon belül lévő összes komponenst magába foglalja.

A modul egyértelmű módon konfigurálható FIPS 2-es vagy 3-as üzemmódba. Ebben az esetben kizárólag FIPS jóváhagyott algoritmusok alkalmazhatóak. A FIPS 3-as szintű üzemmód kikényszeríti továbbá a megbízható útvonalon történő hitelesítést. A FIPS mód kiválasztása a kriptográfiai modul inicializálását vonja maga után, a beállítás változtatása nem lehetséges a modul védett memória tartalmának törlése nélkül.

A kriptográfiai modulhoz való közvetlen (elektronikus) hozzáférés a megbízható útvonalat biztosító PIN beviteli eszköz (PED) soros interfészén, vagy pedig a PCI-e kommunikációs interfészén keresztül történik. A modul biztonságos kulcsgenerálást és tárolást biztosít szimmetrikus és aszimmetrikus kulcspárokhoz, szimmetrikus és aszimmetrikus kriptográfiai szolgáltatások mellett. A kulcsokhoz és kriptográfiai szolgáltatásokhoz való hozzáférés felhasználók és felhasználói alkalmazások számára a PKCS#11 programozói interfészen keresztül biztosított. A modul több felhasználói definíciónak vagy „partíciónak” adhat helyet, amelyek kriptográfiai szempontból elkülönülnek, és a felhasználói alkalmazások számára virtuális tokenként jelennek meg. Minden egyes partíciót külön kell hitelesíteni, hogy a használathoz rendelkezésre álljon.

A modul az alábbi értékek védelmét hivatott biztosítani:
1. Felhasználó által generált magán kulcsok,
2. Felhasználó által generált titkos kulcsok,
3. Kriptográfiai szolgáltatások,
4. A modul biztonsági szempontból kritikus paraméterei.

A modult egy TCP/IP hálózati környezetben üzemeltethető biztonsági eszközön belüli kulcsmenedzsment és kriptográfiai feldolgozó kártyaként való működésre tervezték. A befogadó (hoszt) eszköz használható egy belső hálózatos környezetben, ahol a kulcsmenedzsment biztonsága elsődleges követelmény. Továbbá telepíthető olyan környezetekben, ahol elsősorban kriptográfiai gyorsítóként használják, mely esetben általában külső hálózatokhoz csatlakozik. Feltételezés, hogy az modult egy belső hoszt számítógép tartalmazza, amelyen megfelelően biztonságos operációs rendszer fut, és tartalmaz egy olyan interfészt, melyet lokálisan kapcsolódott vagy távoli adminisztrátorok használnak, valamint egy olyan interfészt, ami a hoszt számítógépen futó alkalmazói programok számára a modul kriptográfiai funkcióihoz biztosít hozzáférést. További feltételezés, hogy a hosztgépén az alkalmazói programok közül csak azok ismert verzióinak telepítése engedélyezett.

Feltétel, hogy képzett és megbízható adminisztrátorok feleljenek az eszköz és a kriptográfiai modul kezdeti konfigurálásáért és folyamatos karbantartásáért.
További feltétel, hogy a kriptográfiai modulhoz való fizikai hozzáférést és a kommunikációs kapcsolatokat felügyelet alatt kell tartani, vagy azáltal, hogy a modul elérése közvetlen helyi kapcsolaton keresztül történik, vagy olyan távoli csatlakozással, amit a hoszt operációs rendszer és alkalmazói szolgáltatás ellenőriz.

2.1. Működtetési szabályzat

A modulhoz a Működtetési szabályzat adja meg a modul egészére és a tartalmazott partíciókra vonatkozó vezérlési, működtetési szabályokat. Minden szinten, legyen az a modul vagy annak partíciója, adott egy rögzített képesség-készlet, ami a működtetési szabályokat a vonatkozó szabályelemek engedélyezésével/tiltásával vagy finomhangolásával, aminek eredménye az előzetesen meghatározott képességekkel megegyező vagy azoktól szigorúbb állapot kialakítása.

A konfigurálható szabályozási elemek készlete a kapcsolódó képesség-készlet megfelelő részhalmaza, azaz a képesség-készlet nem minden eleme finomítható. Az, hogy mely képesség-készlet elemnek van kapcsolódó szabályozási eleme, előre meghatározott, a partíció „személyre szabottsága” vagy a modulra szabott gyári korlátozások alapján. Például a modul „hazai algoritmusok és kulcsméretek elérhetőségére” vonatkozó képesség-készletnek nincs megfelelő konfigurálható szabályozási paramétere.

Létezik több rögzített beállítás, melyekhez nincs kapcsolódó képesség-készlet paraméter. Ezek a kriptográfiai modul működését befolyásoló paraméterek, amelyek eredendően rögzítettek, és emiatt ezeket az SO sem tudja konfigurálni. A specifikus beállítások az alábbiak:

- Titkos kulcsok nem érzékennyé állításának engedélyezése/tiltása – tiltás a rögzített.
- Magánkulcsok nem érzékennyé állításának engedélyezése/tiltása – tiltás a rögzített.
- Titkos kulcsok nem priváttá tételének engedélyezése/tiltása – tiltás a rögzített.
- Privát kulcsok nem priváttá tételének engedélyezése/tiltása – tiltás a rögzített.
- Az objektum létrehozás interfészen keresztül történő titkos kulcs létrehozás engedélyezése/tiltása – tiltás a rögzített.
- Az objektum létrehozás interfészen keresztül történő magánkulcs létrehozás engedélyezése/tiltása – tiltás a rögzített.

Továbbá, a szabályozási készlet paraméterek a képesség-készlet elemeket csak még szigorúbb irányba finomíthatják. Ha egy szabályozási készlet paraméter létezik is a képesség-készlet egy összetevőjének a finomítására, akkor sem lehetséges a szabályozási készlet elemnek más értéket adni, mint amit a képesség-készlet paraméter tartalmaz. Specifikusan, ha egy képesség-készlet paraméter engedélyezettre van beállítva, a kapcsolódó szabályzati elem beállítható engedélyezettre is, meg tiltottra is. Azonban, ha a képesség-készlet paraméter tiltott állapotban van, akkor a kapcsolódó szabályozási paraméter is csak tiltottra állítható. Így az SO sem használhatja a szabályozási paraméterek finomhangolását a képességek definíciójában beállított korlátozás feloldására.

2.1.1. A modul képességei

Az alábbi felsorolás a modul szinten biztosított képességeket tartalmazza:

- Nem FIPS algoritmusok elérhetőségének engedélyezése/letiltása.
- A hitelesítés megbízható útvonallal engedélyezése/letiltása (engedélyezett a megbízható útvonal konfigurációban).
- Partíció csoportok engedélyezése/letiltása.
- Klónozás engedélyezése/letiltása.
- Maszkolás engedélyezése/letiltása.
- Kimaszkolás engedélyezése/letiltása.
- Korean algoritmusok engedélyezése/letiltása.
- Partíció PIN SO általi resetjének (alapállapotba állítás) engedélyezése/letiltása.
- Hálózati replikálás engedélyezése/letiltása. (tiltás állítás)
- Felhasználó hitelesítő adat cseréjének kikényszerítésének engedélyezése/letiltása.
- Távoli PED műveletek engedélyezése/letiltása.
- A Master Tamper Kulcs elosztott tárolás engedélyezése/letiltása.
- A gyorsító engedélyezése/letiltása.
- A High Assurance mód engedélyezése/letiltása

2.1.2. A partíciókra vonatkozó képességek

Az alábbi lista a partíció szinten biztosított képességeket sorolja fel. Minden képesség-paraméter „egy funkcionalitás engedélyezés/letiltása” logikai érték, ahol a hamis (vagy 0) érték a funkcionalitás letiltását jelenti, az igaz (vagy 1) pedig az engedélyezését. A többi paraméter egész értéket vehet fel, a jelzett számú biten.

- Egyes kulcs tulajdonságok megváltoztatása a kulcs generálása után engedélyezése/letiltása.
- A felhasználói kulcsmenedzsment képességek engedélyezése/letiltása.
- Sikertelen kérdés-válasz (challenge-response) validálás esetén a sikertelen bejelentkezési kísérletek számláló növelésének engedélyezése/letiltása.
- 3-as szintű üzemmódban való működés kérdés (challenge) nélkül engedélyezése/letiltása.
- Aktiválás engedélyezése/letiltása.
- Automatikus aktiválás engedélyezése/letiltása.
- Magas rendelkezésre állás (HA) engedélyezése/letiltása.
- Többcélú kulcsok engedélyezése/letiltása.
- RSA blinding nélküli műveletek engedélyezése/letiltása.
- Nem helyi kulcsokkal végzett aláírási műveletek engedélyezése/letiltása.

- Raw RSA műveletek engedélyezése/letiltása.
- Magánkulcsok becsomagolásának engedélyezése/letiltása.
- Magánkulcsok kicsomagolásának engedélyezése/letiltása.
- Titkos kulcsok becsomagolásának engedélyezése/letiltása.
- Titkos kulcsok kicsomagolásának engedélyezése/letiltása.
- Megerősítés nélküli RSA aláírás engedélyezése/letiltása.
- Sikertelen partíció felhasználói bejelentkezések száma a partíció zárolása/törlése előtt (A maximális érték 15, az alapértelmezett 10).

Az alábbi képességek csak akkor konfigurálhatóak, ha a kapcsolódó képesség engedélyezett és be van kapcsolva:

- Magánkulcs klónozás engedélyezése/letiltása.
- Titkos kulcs klónozás engedélyezése/letiltása.
- Magánkulcs maszkolás engedélyezése/letiltása.
- Titkos kulcs maszkolás engedélyezése/letiltása.
- Magánkulcs kimaszkolás engedélyezése/letiltása.
- Titkos kulcs kimaszkolás engedélyezése/letiltása.

Az alábbi táblázat a modul és a partíciók képességeit összesíti, megmutatva a következő termékekre konfigurált modulra a jellemző képesség beállításokat:

- Luna PCI-e:
  - Kulcs export (CKE), és
  - Klónozás (CL);
- Luna SA:
  - Kulcs export (CKE),
  - Klónozás (CL) és
  - Aláírás, klónozás tiltva (SNC).

Az X jelölés a modul minden egyes konfigurációjára az alap képesség beállítást mutatja. A kiszürkített sorok jelzik, hogy a vonatkozó képesség beállítás nem használt semelyik modul konfiguráció esetén alapbeállításként.

1. táblázat A modulképességek és szabályok

Leírás	Képesség	CKE	CL	SNC	Szabályzat	Megjegyzés
Nem FIPS algoritmusok rendelkezésre állása	Engedélyezve	X	X	X	Aktív	Az SO beállíthatja a nem FIPS algoritmusok rendelkezésre állásának aktívvá vagy inaktívvá tételére vonatkozó szabályzatot a HSM inicializálása során.
					Inaktív	
	Tiltva				Inaktív	A kriptográfiai modulnak csak FIPS jóváhagyott algoritmusok használatával szabad működnie.
Jelszavas hitelesítés	Engedélyezve				Aktív	Az SO beállíthatja a szabályt, hogy aktív vagy inaktív legyen-e a jelszavak megbízható útvonal nélküli használata a hitelesítéshez.
					Inaktív	
	Tiltva	X	X	X	Inaktív	A kriptográfiai modulnak a megbízható útvonal és a modul által generált titkok használatával kell működnie a hitelesítés végrehajtásához.
Hitelesítés megbízható útvonallal	Engedélyezve	X	X	X	Aktív	Az SO beállíthat szabályt, hogy aktív vagy inaktív legyen-e a hitelesítéshez használt megbízható útvonal és modul által generált kulcsok alkalmazása.
					Inaktív	
	Tiltva				Inaktív	A HSM-nek jelszavas hitelesítéssel kell működnie, megbízható útvonal nélkül.[3]
Távoli PED műveletek	Engedélyezve	X	X	X	Aktív	A kriptográfiai modul a megbízható útvonalon történő hitelesítésre használhat távoli PED eszközt.
					Inaktív	
	Tiltva				Inaktív	A kriptográfiai modul a megbízható útvonalon történő hitelesítésre nem használhat távoli PED eszközt.
Klónozás	Engedélyezve	X	X		Aktív	Az SO beállíthat szabályt arra, hogy aktív vagy inaktív legyen-e a HSM egészére vonatkozóan a klónozási funkció rendelkezésre állása.
					Inaktív	
	Tiltva			X	Inaktív	A HSM-nek klónozás nélkül kell működnie.
Maszkolás	Engedélyezve				Aktív	Az SO beállíthat szabályt, hogy aktív vagy inaktív legyen-e a HSM egészére vonatkozóan a maszkolási funkció rendelkezésre állása.
					Inaktív	
	Tiltva	X	X	X	Inaktív	A HSM-nek maszkolás nélkül kell működnie.
Kimaszkolás	Engedélyezve	X	X	X	Aktív	Az SO beállíthatja a kriptográfiai modul egészre, hogy használható-e a kimaszkolás funkció.
					Inaktív	
	Tiltva				Inaktív	A kriptográfiai modul csak kimaszkolás nélkül működhet.
Korean algoritmusok	Engedélyezve				Aktív	Az SO beállíthatja a kriptográfiai modul egészre, hogy használható-e a korean algoritmus.
					Inaktív	

[3] A szabály egy és csak egy hitelesítési módot engedélyezhet („felhasználói jelszó” vagy „megbízható útvonal”). Ezért a hitelesítési képességek egyike vagy mindkettő közülük engedélyezett kell, hogy legyen, és amennyiben a képességek egyike letiltott vagy a szabály ki van kapcsolva, akkor a szabálybeállítást a másikra be kell kapcsolni.

Leírás	Képesség	CKE	CL	SNC	Szabályzat	Megjegyzés
	Tiltva	X	X	X	Inaktív	A kriptográfiai modul nem használhat Korean algoritmust.
Partíció reset (alapállapotba állítás)	Engedélyezve	X	X	X	Aktív Inaktív	Az SO beállíthat szabályt, hogy aktív legyen-e a partíció reset (alapállapotba állítás), ha az zárolt állapotba kerül a sikertelen bejelentkezési kísérletek maximális számának túllépése következtében.
	Tiltva				Inaktív	Egy partíció nem kerülhet alapállapotba, és újra létre kell hozni azt a sikertelen bejelentkezési kísérletek maximális számának túllépése esetén.
Hálózat replikálás	Engedélyezve		X		Aktív Inaktív	Az SO beállíthat szabályt, hogy aktív legyen-e a modul kulcskészletének hálózaton keresztül történő replikálása egy másodlagos modulra.
	Tiltva	X		X	Inaktív	A modul nem replikálható hálózaton keresztül.
Felhasználói PIN csere kikénysze-rítése	Engedélyezve	X	X	X	Aktív Inaktív	Ez a képesség a vásárlóhoz való szállítás előtt beállítódik. Ha be van kapcsolva, akkor kikényszeríti, hogy a felhasználó megváltoztassa a PIN-jét az első bejelentkezéskor.
	Tiltva				Inaktív	A felhasználónak nem kell megváltoztatnia a PIN-t az első bejelentkezéskor.
Távoli hitelesítés	Engedélyezve				Aktív Inaktív	Ez a képesség a vásárlóhoz való szállítás előtt beállítódik. Lehetővé teszi a távoli hitelesítés használatát.
	Tiltva	X	X	X	Inaktív	A távoli hitelesítés nem engedélyezhető a modulon.
A külső MTK megosztott tárolása	Engedélyezve	X	X	X	Aktív Inaktív	Ez a képesség a felhasználónak történő kiszállítás előtt van állítva. Engedélyezi egy MTK rész külső tárolóra helyezését.
	Tiltva				Inaktív	Külső tárolón lévő MTK darab nem engedélyezett.
Gyorsítás	Engedélyezve	X	X	X	Aktív Inaktív	Ez a képesség a felhasználónak történő kiszállítás előtt van állítva. Engedélyezi az alaplapi kriptográfiai gyorsító használatát.
	Tiltva				Inaktív	A modulban a távoli hitelesítés tiltva van.
HA CGX mód	Engedélyezve				Aktív Inaktív	Ez a képesség a felhasználónak történő kiszállítás előtt van állítva. Engedélyezi a HACGX mód használatát.
	Tiltva	X	X	X	Inaktív	A HA CGX mód tiltott a modulban.

2. táblázat Partíciók képességei és szabályok

Leírás	Előfeltétel	Képesség	KE	CL	NC	Szabályzat	Megjegyzés
Kérdés (challenge) nélküli megbízható útvonal művelet	Megbízható útvonal hitelesítés aktív	Engedélyezve	X	X	X	Aktív	Az SO beállíthat szabályt, hogy bejelentkezést megbízható útvonallal csak PED-es megbízható útvonal használatával lehet végrehajtani, és kérdés-válasz (challenge-response) érvényesítés nem szükséges. Inaktívnak kell lennie, ha az aktiválás vagy automatikus aktiválás engedélyezve van.
						Inaktív	
		Tiltva				Inaktív	Kérdés-válasz validálás szükséges, valamint PED-es megbízható útvonalas bejelentkezés a partícióhoz való hozzáféréshez.
Felhasználói kulcsok menedzsmentje képesség[4]	Megbízható útvonal hitelesítés aktív. Challenge nélküli megbízható útvonal művelet inaktív	Engedélyezve	X	X	X	Aktív	Az SO beállíthat szabályt, hogy engedélyezett legyen-e a normál PKCS#11 felhasználó szerepkör a kulcsmenedzsment funkciók végrehajtásához. Ha engedélyezett, akkor a Crypto Officer (kriptográfiai felelős) kulcsmenedzsment funkciói rendelkezésre állnak. Ha nem engedélyezett, csak a Crypto User szerepkör funkciói elérhetőek.
						Inaktív	
		Tiltva				Inaktív	Csak a Crypto User szerepkör funkciói állnak rendelkezésre.
Sikertelen kérdés-válasz validálások számlálása	Hitelesítés megbízható útvonallal aktív	Engedélyezve	X	X	X	Aktív	Az SO beállíthat szabályt, hogy a maximális sikertelen bejelentkezésekhez viszonyított sikertelen kérdés-válasz validálásokat számolja-e a rendszer. Engedélyezni kell, ha akár az aktiválás, akár az automatikus aktiválás engedélyezve van.
						Inaktív	
		Tiltva				Inaktív	A kérdés-válasz validálások sikertelenségét nem számolja a maximális login hibákhoz.
Aktiválás	Hitelesítés megbízható útvonallal aktív	Engedélyezve	X	X	X	Aktív	Az SO beállíthat szabályt, hogy a PED-es megbízható útvonalon keresztül megadott hitelesítési adat cachelhető lehet-e a modulba, lehetővé téve ezáltal minden további partíció hozzáférést az első bejelentkezés után, kizárólag a kérdés-válasz validálás alapján.
						Inaktív	
		Tiltva				Inaktív	PED-es megbízható útvonalas hitelesítés szükséges a partícióhoz való minden hozzáféréskor.

[4] Ez a képesség/szabály a felhasználónak a kulcsmenedzsment funkciók fölötti nagyobb felügyeletet biztosítja. A szabály letiltásával a Security Officer a partíciót olyan állapotba állítja, melyben a kulcsértékek zárolva vannak, és csak a kapcsolódó alkalmazások használhatják, vagyis csak a Crypto User általi hozzáférés lehetséges.

Leírás	Előfeltétel	Képesség	KE	CL	NC	Szabályzat	Megjegyzés
Automatikus aktiválás	Hitelesítés megbízható útvonallal aktív	Engedélyezve				Aktív	Az SO beállíthat szabályt, hogy engedélyezve legyen az aktiválási adatok alkalmazásszerveren történő tárolása rejtjelezett formában, lehetővé téve, hogy a partíció egy újraindítás után a hitelesítési állapotába térhessen vissza. Ez elsődlegesen arra szolgál, hogy az eszköz áramellátási probléma utáni újraindulása esetén a partíciók automatikusan újraindulhassanak.
						Inaktív	
		Tiltva	X	X	X	Inaktív	Az aktiválási adatok külső helyen nem cachelhetők.
Magas rendelkezésre állás	Hálózatos replikálás aktív	Engedélyezve	X	X		Aktív	Az SO beállíthat szabályt, ami engedélyezi a magas rendelkezésre állási tulajdonságot.
						Inaktív	
		Tiltva			X	Inaktív	A magas rendelkezésre állás nem engedélyezhető.
Többcélú kulcsok	-	Engedélyezve	X	X	X	Aktív	Az SO beállíthat szabályt, ami engedélyezi a kulcsok egynél több célra való használatát, például egy RSA magánkulcs digitális aláírásra és megoldásra is használható lehet.
						Inaktív	
		Tiltva				Inaktív	Kulcsok csak egyetlen célra használhatók.
Attribútumok módosítása	-	Engedélyezve	X	X	X	Aktív	Az SO beállíthat szabályt a kulcs tulajdonságok módosításának engedélyezésére.
						Inaktív	
		Tiltva				Inaktív	A kulcstulajdonságok nem módosíthatók.
RSA blinding nélküli működés	-	Engedélyezve	X	X	X	Aktív	Az SO beállíthatja az RSA műveletekre vonatkozóan a blinding mód használatát. A blinding mód az RSA digitális aláírási műveletekkel szembeni időzítés-elemzésen alapuló támadások kiküszöbölésére szolgál, de az aláírási művelet végrehajtási teljesítményére jelentős negatív kihatással van.
						Inaktív	
		Tiltva				Inaktív	A blinding mód nem használt RSA műveletek esetén.
Aláírás nem helyi kulcsokkal	-	Engedélyezve	X	X	X	Aktív	Az SO beállíthatja, hogy külsőleg generált magánkulcsokkal lehessen aláírni, melyeket a partícióba importáltak.
						Inaktív	
		Tiltva				Inaktív	Külsőleg generált magánkulcsok nem használhatók aláírási műveletekre.

Leírás	Előfeltétel	Képesség	KE	CL	NC	Szabályzat	Megjegyzés
Raw RSA műveletek	-	Engedélyezve	X	X	X	Aktív Inaktív	Az SO beállíthatja, hogy raw (feltöltés (padding) nélküli) formátumot lehessen használni RSA műveletek esetén.
		Tiltva				Inaktív	Raw RSA nem használható.
Magánkulcs becsomagolás	-	Engedélyezve	X			Aktív Inaktív	Az SO beállíthatja, hogy a magánkulcsokat becsomagolva lehessen exportálni.
		Tiltva		X	X	Inaktív	Magánkulcsok nem csomagolhatók be és nem exportálhatók a partícióról.
Magánkulcs kicsomagolás	-	Engedélyezve	X	X	X	Aktív Inaktív	Az SO beállíthatja, hogy magánkulcsok kicsomagolhatók lehessenek és a partícióba lehet azokat importálni.
		Tiltva				Inaktív	Magánkulcsok nem kicsomagolhatók és nem importálhatók a partícióba.
Titkos kulcs becsomagolás	-	Engedélyezve	X	X	X	Aktív Inaktív	Az SO beállíthatja, hogy titkos kulcsokat becsomagolva lehessen exportálni.
		Tiltva				Inaktív	Titkos kulcsok nem csomagolhatók be és nem exportálhatók a partícióról.
Titkos kulcs kicsomagolás	-	Engedélyezve	X	X	X	Aktív Inaktív	Az SO beállíthatja, hogy titkos kulcsok kicsomagolhatók lehessenek és a partícióba lehessen őket importálni.
		Tiltva				Inaktív	Titkos kulcsok nem kicsomagolhatók és nem importálhatók a partícióba.
Magánkulcs klónozás	Klónozás aktív, hitelesítés megbízható útvonallal aktív	Engedélyezve		X		Aktív Inaktív	Az SO beállíthatja, hogy magánkulcsok egyik partícióról a másikra klónozhatók legyenek.
		Tiltva	X		X	Inaktív	Magánkulcsok nem klónozhatók.

Leírás	Előfeltétel	Képesség	KE	CL	NC	Szabályzat	Megjegyzés
Titkos kulcs klónozás	Klónozás aktív, hitelesítés megbízható útvonallal aktív	Engedélyezve	X	X	X	Aktív	Az SO beállíthatja, hogy titkos kulcsok egyik partícióról a másikra klónozhatók legyenek.
						Inaktív	
		Tiltva				Inaktív	Titkos kulcsok nem klónozhatók.
Magán kulcs maszkolás	Maszkolás aktív	Engedélyezve				Aktív	Az SO beállíthatja, hogy magánkulcsok maszkolhatók legyenek partíción kívüli tároláshoz.
						Inaktív	
		Tiltva	X	X	X	Inaktív	Magánkulcsok nem maszkolhatók partíción kívüli tároláshoz.
Titkos kulcs maszkolás	Maszkolás aktív	Engedélyezve				Aktív	Az SO beállíthatja, hogy titkos kulcsok maszkolhatók legyenek partíción kívüli tároláshoz.
						Inaktív	
		Tiltva	X	X	X	Inaktív	Titkos kulcsok nem maszkolhatók partíción kívüli tároláshoz.
Magánkulcs kimaszkolása	Maszkolás aktív	Engedélyezve	X	X	X	Aktív	Az SO beállíthatja, hogy magánkulcsok kimaszkolhatók és a partícióra visszatehetők legyenek.
						Inaktív	
		Tiltva				Inaktív	Magánkulcsok nem maszkolhatók ki és nem tehetők vissza a partícióra.
Titkos kulcs kimaszkolása	Maszkolás aktív	Engedélyezve	X	X	X	Aktív	Az SO beállíthatja, hogy titkos kulcsok kimaszkolhatók és a partícióra visszatehetők legyenek.
						Inaktív	
		Tiltva				Inaktív	Titkos kulcsok nem maszkolhatók ki és nem tehetők vissza a partícióra.
Minimális/maximális jelszó hossz	Hitelesítés felhasználói jelszóval aktív	7-16 karakter				Konfigurálható	Nem vonatkozik megbízható útvonal modulokra.
Sikertelen partíció felhasználói loginok száma engedélyezve	-	Minimum: 1 Maximum: 10				Konfigurálható	Az SO beállíthatja; az alapértelmezett maximális érték 10.

2.2. FIPS jóváhagyott üzemmód

Az SO vezérli a modul működését a FIPS PUB 140-2-ben definiált FIPS-jóváhagyott üzemmódban, a megfelelő Modul Szabályzat beállítások engedélyezésével vagy letiltásával (feltéve, hogy ezek mindegyikére lehetőség van modul képesség szintjén). A FIPS-jóváhagyott módban történő működéshez az alábbi szabálybeállítások szükségesek:

- „Nem FIPS algoritmusok rendelkezésre állnak" lehetőséget le kell tiltani.

Továbbá, FIPS 3-as szintű műveleteknél:

- „Hitelesítés megbízható útvonallal" lehetőséget be kell kapcsolni (következménye, hogy a jelszavas hitelesítés tiltott vagy kikapcsolt), és
- „Kérdés (challenge) nélküli megbízható útvonal művelet" lehetőséget le kell tiltani, ha az aktiválás vagy automatikus aktiválás be van kapcsolva.
- A „Sikertelen kérdés-válasz (challenge-response) validálások számlálása" lehetőséget engedélyezni kell, ha az aktiválás vagy automatikus aktiválás be van kapcsolva.
- Raw RSA műveleteket csak kulcs átvitelre szabad használni FIPS üzemmódban.

A „hitelesítés megbízható útvonallal" esetén szintén beállíthatók szabályok, olyan esetben, amikor a „Nem FIPS algoritmusok rendelkezésre állnak" engedélyezve van.
Amennyiben az SO olyan szabályopciót választ (például bekapcsolja a „Nem FIPS algoritmusok rendelkezésre állnak" opciót), amely nem jóváhagyott üzemmódba állítja a modult, akkor megjelenik egy figyelmeztetés és az SO-nak meg kell erősítenie a választását. Az SO megállapíthatja a FIPS üzemmódot úgy, hogy összeveti a kijelzett képességet és szabálybeállításokat a 2.1 és 2.2 alfejezetben írtakkal.

2.3. Az operátor, szubjektum és objektum leírása

2.3.1. Operátor

Az operátor olyan egyed, amely a modulban valamely művelet végrehajtása érdekében jár el. Egy operátor közvetlenül leképezhető felelős személyre vagy szervezetre, vagy hozzárendelhető felelős személy vagy szervezet és a felelős egyén vagy szervezet nevében eljáró ágens (alkalmazói program) együttesére.

Egy tanúsítási szervezet (CA) esetében például, a szervezet felhatalmazhat egy egyént vagy egyének együtt eljáró kisebb csoportját, hogy a szervezet szolgáltatásának részeként egy kriptográfiai modult üzemeltessenek. Az operátor lehet az egyén vagy csoport, különösen, ha a modul helyben hozzáférhető. Az operátor lehet egyén vagy csoport (akik helyben kezelik a modult (elsősorban aktiválási céloknál, lásd 2.4.2-es szakaszt)) és a hálózathoz kapcsolt hosztgépen futó CA alkalmazás együttese.

2.3.2. Szerepkörök

A „Hitelesítés megbízható útvonallal" konfiguráció esetén a Luna kriptográfiai modul három hitelesített operátori szerepkört támogat, melyek: Crypto User, Crypto Officer minden egyes partícióhoz (közös nevük Partiton User - partíció felhasználók), valamint a Security Officer (biztonsági felelős) modul szinten. A kriptográfiai modul támogat még egy nem hitelesített operátori szerepkört, a nyilvános felhasználót (Public User), elsődlegesen állapotinformációkhoz való hozzáférés és hitelesítés előtti diagnosztizálás biztosítása céljából.

Az SO privilegizált szerepkör, és csak modul szinten létezik. Elsődleges célja a modul kezdeti konfigurálása a működés elindításához, és biztonsági adminisztrátori feladatok (mint például partíció létrehozás) végrehajtása. A Crypto Officer a kulcsmenedzsment szerepkör az egyes partíciókhoz, az opcionális Crypto User pedig egy olvasási jogú szerepkör, ami az operátort csak kriptográfiai műveletek végrehajtására korlátozza.

A Public Useren kívüli bármelyik másik szerepkör felvétele előtt az operátort azonosítani és hitelesíteni kell. Az alábbi feltételeknek kell teljesülni a hitelesített szerepkörök egyikébe kerüléshez:

- Egy operátor sem veheti fel a Crypto Officer, Crypto User vagy Security Officer szerepkört azonosítás és hitelesítés előtt;

- Senki/semmi sem veheti fel a Crypto Officer vagy Crypto User szerepkört a Security Officer szerepkörrel együtt.

Az SO létrehozhatja a Crypto User szerepkört a Crypto User számára generált kérdés (challenge) értékkel. A Crypto Officer és Crypto User szerepköröket támogató partíció esetén a Security Officer csak a Crypto User szerepkör számára korlátozhatja a hozzáférést a „Felhasználói kulcsok menedzsmentje" szabály (lásd 1 táblázat) kikapcsolásával.

2.3.3. Bejelentkezési/azonosító adatok

A modul az alábbi User (ami magába foglalja mind a Crypto Officer, mind a Crypto User szerepkört partíciónként[5]) és SO bejelentkezési adatokat tartja nyilván:

- Partíció ID vagy SO ID száma;
- Partíció felhasználó rejtjelezett vagy SO rejtjelezett hitelesített adata (checkword);
- Partíció felhasználó hitelesítési kérdés (challenge) titok (minden szerepkörre egy, ha szükséges);
- Partíció felhasználó zárolása jelölő.

Egy hitelesített felhasználót partíció felhasználónak (Partition User) nevezünk. A bejelentkezési adatok kezelésének képessége az SO-ra és a Partition Userre van korlátozva. A különleges korlátozások az alábbiak:

1. Csak a Security Officer szerepkör hozhatja létre (inicializálhatja) és törölheti az alábbi biztonsági tulajdonságokat:
   - Partition ID.
   - Checkword.
2. Ha a partíció reset engedélyezett és be is van kapcsolva, akkor az SO szerepkör csak az alábbi biztonsági tulajdonságot módosíthatja:
   - Zárolási jelölő a Partition Userre.
3. Csak a Partition User módosíthatja az alábbi biztonsági tulajdonságot:
   - A Partition User checkwordje.
4. Csak a Security Officer szerepkör módosíthatja az alábbi biztonsági tulajdonság alapértékét, illetve kérdezheti le, módosíthatja és törölheti azt:
   - A Security Officer checkwordje.

2.3.4. Szubjektum

A szubjektumot egy modul munkaszakaszként definiáljuk. A munkaszakasz logikai eszközt biztosít a modulhoz kapcsolódó alkalmazás és a modulon belül a parancsok feldolgozása közötti összerendeléshez. Minden munkaszakaszt a Session ID, a Partition ID és az Access ID (hozzáférési ID) azonosít, ami az alkalmazás kapcsolathoz rendelt egyedi azonosító. Lehetőség van arra, hogy több nyitott munkaszakasz legyen a modulhoz ugyanazzal az AccessID/ Partition ID kombinációval.
Lehetséges egynél több partíció ID-hez munkaszakaszokat nyitni, vagy megnyitott munkaszakaszokhoz több AccessID-t rendelni. A távoli hosztrendszereken futó alkalmazásoknak, amelyek adatokat és kriptográfiai szolgáltatásokat kérnek a modultól, először az eszközön belül lévő kommunikációs szolgáltatáshoz kell kapcsolódniuk, ami egy egyedi Access ID-t létesít a kapcsolathoz, majd engedélyezi az alkalmazásnak, hogy egy munkaszakaszt nyisson a modulon belüli partíciók egyikével. Egy helyi alkalmazás (például parancssoros adminisztrátori interfész) közvetlenül nyit egy munkaszakaszt a megfelelő partícióval a modulban, a kommunikációs szolgáltatás meghívása nélkül.

2.3.5. Operátor és szubjektum összekötése

Egy operátornak munkaszakaszon keresztül kell egy partíciót elérnie. A partícióhoz a munkaszakasz hitelesítés nélküli állapotban nyílik meg, és az operátornak hitelesítenie kell magát mielőtt a kriptográfiai funkciókhoz és privát objektumokhoz a partíción belül bármilyen hozzáférési jog megadása megtörténne. Amikor az operátor azonosítása és hitelesítése sikeresen végrehajtódott, a munkaszakasz állapota hitelesítetté válik, és a Crypto Officer vagy Crypto User szerepkörben a Partition ID által reprezentált Partiton Userhez lesz hozzárendelve. Minden más munkaszakasz,

[5] Egy partíció a modulon belül egy azonosított entitást reprezentál.

amelyet ugyanazzal az Access ID/Partition ID kombinációval nyitottak, ugyanazt a hitelesítési állapotot kapja, és ugyanahhoz a Partition Userhez fog kapcsolódni.

2.3.6. Objektum

Egy objektum lehet bármilyen formázott adat, ami a felejtő vagy a nem felejtő memóriában tárolódik egy operátor nevében. Kiemelt objektumok a magán (aszimmetrikus) kulcsok és titkos (szimmetrikus) kulcsok.

2.3.7. Objektum műveletek

Az objektumokon a műveleteket csak egy Partition User végezheti el. A végrehajtható műveleteket a felhasználó bejelentkezési állapotához kapcsolt szerepkör (Crypto Officer vagy Crypto User) korlátozza. (Lásd 2.5 szakaszt).
Új objektumok többféle módon képezhetők. Az alábbi lista az új objektumokat előállító műveleteket azonosítja:

- létrehozás,
- másolás,
- generálás,
- kicsomagolás,
- származtatás.

Meglévő objektumok módosíthatók és törölhetők. A tulajdonságok egy részhalmazának értéke módosítási művelet révén megváltoztatható. Az objektumok a megsemmisítés művelet segítségével törölhetők. A konstans műveletek nem eredményezik egy objektum létrehozását, módosítását vagy törlését. A konstans műveletek közé tartoznak:

- egy objektum méretének lekérdezése;
- egy tulajdonság méretének lekérése;
- egy tulajdonság értékének lekérdezése;
- egy tulajdonság értékének használata kriptográfiai műveletben;
- illeszkedő tulajdonságon alapuló objektumok keresése;
- objektum klónozása;
- objektum becsomagolása; és
- objektum maszkolása vagy kimaszkolása.

A privát és titkos kulcsokat mindig érzékeny objektumokként kezeli a rendszer, így a bizalmasság védelme érdekében a kulcsértéket tartósan rejtjelezett formában tárolja. A felejtő memóriában lévő kulcsobjektumok kulcsértékei nincsenek titkosítva, de aktív törlésük megtörténik a modul újraindítása vagy egy fizikai manipulálási esemény hatására. Az operátorok nem kapnak közvetlen hozzáférést a kulcsértékekhez semmilyen célból.

2.4. Azonosítás és hitelesítés

2.4.1. Hitelesítési adatok generálása és megadása

A modul megköveteli, hogy a Partiton User és az SO hitelesítve legyen az operátor és a modul között megosztott titok ismeretének bizonyítása által. A „Hitelesítés megbízható útvonallal" opcióra konfigurált modult a PED használatával kell inicializálni az SO hitelesítési adatainak megadásához.

A „Hitelesítés megbízható útvonallal" opció esetén a modul generálja a hitelesítéshez használt titkot, ami egy 48 bájtos véletlen érték, és Partiton User esetén opcionálisan egy hitelesítési kérdés (challenge) titkot. A hitelesítési titok (vagy titkok) az operátorhoz egy fizikailag különálló megbízható útvonalon jutnak el (lásd 2.4.2 fejezetet), és az operátornak a megbízható útvonalon és egy logikailag különálló megbízható csatornán (challenge titkon alapuló válasz esetén) keresztül kell megadnia az(oka)t a bejelentkezési folyamat során. Ha Crypto Officer és Crypto User szerepkörökkel lett egy partíció létrehozva, egy külön challenge titok generálódik minden egyes szerepkörre.

A Luna® PED eszközzel az alábbi típusú iKey-ek használhatóak:

- Narancs (RPV) iKey a Remote PED Vector (RPD) tárolására,
- Kék (SO) iKey az SO hitelesítő adat tárolására,
- Fekete (User) iKey a felhasználó hitelesítő adatának tárolására,
- Piros (Domain) iKey a klónozáshoz szükséges adatok tárolására,
- Lila (MTK visszaállító) iKey az MTK szelet külső tárolására.

Egy használatba vett iKey eszközt, mint egy azonosító hitelesítő eszközt biztonságos módon kell kezelni, használni, amiért a LUNA® PCI-e működési környezetében lévő irányító és üzemeltető részlegek felelősek.

2.4.2. Megbízható útvonal

A Megbízható útvonal módban a felhasználó azonosítása alapértelmezetten egy kétszakaszos folyamat. Az első fázis az „Aktiválás", ami egy megbízható útvonalat garantáló eszköz (PED) használatával hajtódik végre. A PED vagy direkten közvetlen vezetékkel, vagy távolról biztonságos hálózati csatornán kapcsolódik kriptográfiai modulhoz. Az Aktiválás során használt hitelesítő adat elsődleges formája a 48 bájtos érték, melyet a modul véletlenszám generálással hoz létre, és a Black (User) iKey[6]-en tárolódik le a fizikai megbízható útvonalon keresztül.
Az iKey-n lévő adatot kell aztán megadni a modul számára a megbízható útvonal használatával az egyes aktiválási folyamatok részeként. Az aktiválás végrehajtása után a felhasználói partíció adata készen áll a modulon belül a használatra. A kulcskészlethez és kriptográfiai szolgáltatásokhoz való hozzáférés azonban nem engedélyezett, amíg a hitelesítés második szakasza, a „User Login", vagyis a felhasználói bejelentkezés meg nem történik. Ez általában egy partíció challenge titkának megadását követeli meg a bejelentkezési művelet részeként. Ugyanakkor, az SO és a felhasználó hitelesítéséhez, amikor a Partíció Szabályzat inaktívra állítja a partícióhoz[7] való bejelentkezéshez a kérdés-válasz hitelesítés használatát, akkor az iKey adat megadása (ami az aktiválás) elegendő a teljes hitelesítéshez.

Az alapértelmezett Partíció szabályzat lehetővé teszi a kérdés-válasz hitelesítést a „User Login" fázisban. A partícióhoz a hitelesítési kérdés titkot (vagy titkokat, ha a Crypto Officer és Crypto User szerepkörök használtak) a modul generálja, és ez a megbízható útvonalat biztosító eszköz kijelzőjén egy 16 karakter hosszú karaktersorozatként megjelenő 75 bites érték. A challenge titok ezután kerül egy megbízható egyéb csatornán keresztül minden egyes külső entitáshoz, aki számára engedélyezett a partícióhoz való csatlakozás, és ez a külső entitás használja fel a modulból származó véletlen, egyszeri challengere adandó válaszhoz. A rejtjelezett egyszeri válasz a kriptográfiai modulhoz jut, ahol megtörténik a „User Login" megerősítésének ellenőrzése.

[6] Vagy Black (User) PED kulcs. Jelen dokumentumban az iKey és PED kulcs külön jelzés hiányában egyenértékűnek tekintendő.
[7] A kérdés-válasz hitelesítés letiltható például olyan esetben, amikor mind a kriptográfiai modul, mind pedig a kapcsolódó alkalmazási szerver ugyanabban a fizikailag biztonságos környezetben helyezkedik el, és a felhasználónak mindig személyesen jelen kell lennie az alkalmazás elindításához és a PED-del a kriptográfiai modulon történő hitelesítéshez.

Ezáltal, amikor a challenge titok szükséges, akkor mind a megbízható útvonalas aktiválás, mind pedig a kérdés-válasz folyamat külső entitás általi sikeres befejezése követelmény egy partícióhoz való hitelesítéshez, és annak kriptográfiai funkcióihoz és anyagaihoz való hozzáféréshez.

A PED távoli működtetése

A PED eszközt üzemeltethető hagyományos módon közvetlenül helyileg a kriptográfiai modulhoz kapcsolva, vagy távolról a menedzsment munkaállomásról annak USB portjára csatlakoztatva. A távoli PED műveletet kiterjeszti a fizikai megbízható útvonalat felhasználva egy saját protokollt, ami mint a távoli PED eszközt mind a kriptográfiai modult kölcsönösen hitelesíti, és egy egyszer használatos AES kulcs kialakítása után a PED és a modul közötti kommunikációt rejtjelezi. A biztonságos kommunikációs csatorna kialakítása után minden iterakció a kriptográfiai modul és a PED valamint az iKey-ek között ugyanolyan módon zajlik, mintha a PED helyileg lenne a modulhoz csatlakoztatva.

A modul és a PED közötti logikai csatorna az alábbi módon van védve. A kriptográfiai modul inicializáláskor a modul generál 256 bit véletlent (Remote PED Vektor (RPV)), amit a biztonsági paraméterek tárolójába ment és kiírja a narancs (RPV) iKey-re Ez utóbbit Remote PED Key-nek (RPK) is nevezünk.

A biztonságos kapcsolat kialakításához az RPK-t be kell helyezni a PIN-be. A PED kiolvassa az RPV-t A PED valamint a kriptográfiai modul végrehajtanak egy ephemeral Diffie-Hellman kulcs egyeztetés folyamatot A származtatott kulcsot az RPV-vel XOR-olva alakítják ki a munkaszakasz kulcsot. Egy véletlen nonce értéket rejtjelezve hajtják végre a kölcsönös hitelesítést. Minden kommunikáció a PED és a kriptográfiai modul között AES 256 algoritmussal rejtjelezett.

2.4.3. N-ből M aktiválás

A Luna kriptográfiai modul minden szerepkör tekintetében támogatja az M az N-ből titok megosztáson alapuló hitelesítési sémát. Az M az N-ből hitelesítés kikényszeríti több személy jelenlétét a szerepkörhöz társított funkció végrehajtásához.
Az M az N-ből hitelesítés a Shamir titokmegosztási sémán alapul. A kriptográfiai modul egy véletlenszerűen generált hitelesítő adatot szétvág N szeletre, és ezeket darabonként kiírja egy-egy iKey-re. Bármely M darab ezekből a szeletekből a hozzátartozó iKey kulcsal megadva a PED-nek alkalmas az eredeti hitelesítő adat visszaállítására.

2.4.4. A sikertelen bejelentkezésekre vonatkozó korlátozások

A modul megvalósít egy, a maximális bejelentkezési próbálkozásokra vonatkozó szabályzatot is. A szabály különbözik az SO hitelesítő adat keresése és a Partition User hitelesítő adatának kikeresése esetén.

Az SO hitelesítő adat keresése esetén a szabály az alábbi:

- Amennyiben három (3) egymás utáni SO bejelentkezés sikertelen, akkor a modultörlés funkció végrehajtódik.

Partiton User hitelesítő adatának keresése esetén két válasz valamelyike következik be, a partícióra vonatkozó szabályok függvényében:

1. Ha a „Partiton reset” engedélyezett és aktív, akkor „n” darab (ahol „n”-t a HSM inicializálása során az SO állítja be) egymást követő operátori bejelentkezés sikertelensége után a modul bejegyzi az eseményt a Partiton User bejelentkezési adataiban, zárolja a Partiton User-t, és törli a felejtő memória tárhelyet. Az SO-nak kell a zárolást feloldania a partíción, annak érdekében, hogy a Partiton User visszatérhessen a működésbe.
2. Ha a „Partiton reset” nem engedélyezett vagy inaktív, akkor a fizikai megbízható útvonalon végrehajtott „n” darab egymást követő sikertelen Partiton User bejelentkezési kísérlet után a modul törli a partíciót. Az SO-nak törölnie kell a partíciót és újra ki kell alakítania azt. A partíción tárolt minden objektum, ideértve a magán- és titkos kulcsokat, végérvényesen törlődik.

2.5. Hozzáférés ellenőrzés

A hozzáférés ellenőrzési szabály a modul által érvényre juttatott fő biztonsági funkció. Ez irányítja egy szubjektum jogait a privilegizált funkciók végrehajtása tekintetében, és a modulban tárolt objektumokhoz való hozzáférést is. A 2.3.7 fejezetben részletezett objektum műveleteket fedi le.

Egy szubjektumnak a modulban tárolt objektumokhoz való hozzáférése az alábbi szubjektum és objektum tulajdonságok alapján valósul meg:

- Szubjektum tulajdonságok:
  - Session ID
  - A munkaszakaszhoz rendelt Access ID és Partition ID
  - Session hitelesítési állapot (hitelesített partíció egyedhez és szerepkörhöz kötődően)
- Objektum tulajdonságok:
  - **Tulajdonos**. Egy privát objektum birtokosa a létrehozó szubjektumhoz kapcsolódó Partition User. A tulajdonlást belső kulcsmenedzsment juttatja érvényre.
  - **Privát**. Igaz érték esetén az objektum privát, hamis érték esetén nyilvános.
  - **Érzékeny**. Igaz érték esetén az objektum érzékeny, hamis érték esetén nem érzékeny.
  - **Kivehető**[8]. Igaz érték esetén az objektum kivehető a modulból, hamis érték esetén nem.
  - **Módosítható**. Igaz érték esetén az objektum módosítható, hamis esetén nem lehet módosítani.

Az objektumokhoz tartozik egy szám címke, ami a partícióra vonatkozik, és csak a birtokos Partition ID-hoz kötődő szubjektum számára hozzáférhető. Csak általános adatok és tanúsítvány objektumok lehetnek nem érzékenyek.
Az érzékeny objektumok a partíció titkos kulcsának segítségével titkosítva vannak, hogy az értékük védett legyen a külső egyedek általi megismerés ellen. Kulcsobjektumok mindig érzékeny objektumokként jönnek létre, és kizárólag egy bejelentkezett Partition User által használhatók kriptográfiai műveletekben. A kivehetőnek jelölt kulcsobjektumok exportálhatók a modulból a csomagolás művelet alkalmazásával, ha ezt a partíció szabálykészlete megengedi és az engedély aktív. A 3 táblázat összegzi a hozzáférés ellenőrzési szabályzatban használt objektum tulajdonságokat.

3. táblázat A hozzáférés ellenőrzési szabályzat érvényre juttatásában használt objektum tulajdonságok

Tulajdonság	Értékek	Hatás
MAGÁN	TRUE – Az objektum privát az objektum létrehozásakor Access Owner-ként (hozzáférési tulajdonos) azonosított operátor számára, ő a tulajdonosa.	Az objektum csak az objektumot birtokló operátor egyedhez kötött szubjektumok (session-k) számára hozzáférhető.
	FALSE – Az objektum nem privát egy operátoregyed számára.	Az objektum hozzáférhető minden olyan szubjektum számára, aki/ami ahhoz a partícióhoz kötődik, amelyben az objektum tárolódik.

[8] A kivétel a kulcsnak a modul hatásköréből való kivételét jelenti. Általában a csomagolás művelettel történik, de a maszkolás művelet is szóba jöhet egy kivétel megvalósítására, amikor a tárolóhoz engedélyezett a klónozás.

Tulajdonság	Értékek	Hatás
ÉRZÉKENY	TRUE – Nyílt kulcsokat reprezentáló tulajdonság értékek nem megengedettek (érték titkosított).	A kulcsok titkosított formában tárolódnak.
	FALSE – Megengedett nyílt adatokat reprezentáló tulajdonság értékek létezése.	Nyílt adatok az objektummal tárolódnak és minden szubjektum számára hozzáférhetők, ha az objektumhoz való hozzáférés engedélyezése másként nem rendelkezik.
MÓDOSÍTHATÓ	TRUE – Az objektum tulajdonság értékei módosíthatók.	Az objektum „írható” és a tulajdonság értékei módosíthatók egy másolási vagy tulajdonság beállítási művelet során.
	FALSE – Az objektum értékei nem módosíthatók.	Az objektum csak olvasható és csak duplikátum készíthető róla.
KIVEHETŐ	TRUE – Az objektumban tárolt kulcs kivehető a Luna kriptográfiai modulból a csomagolás művelet használatával.	Egy kulcs kivételének képessége megengedi kulcsok megosztását más kriptográfiai modulokkal, és a kulcsok archiválását.
	FALSE – Az objektumban tárolt kulcs nem vehető ki a Luna kriptográfiai modulból.	A kulcsok soha nem hagyhatják el a modul hatáskörét.

A modul nem tesz lehetővé semmilyen hozzáférési finomítást a tulajdonos és nem tulajdonos közti megkülönböztetésen kívül (vagyis például egy privát objektum nem lehet hozzáférhető két Partition User által vagy másik Partition Userre korlátozott). Egy privát objektum tulajdonlása a tulajdonosnak hozzáférést biztosít az objektumhoz a megengedett műveleteken keresztül, de nem teszi lehetővé, hogy a tulajdonos a jogok egy részét egy másik operátorra ruházza át. A megengedett műveletek azok, amelyeket a HSM és a partíció képesség és szabály beállítások engedélyeznek.

A szabályzatot az alábbi állítások összegzik:

- Egy szubjektum végrehajthat egy megengedett műveletet egy objektumon, ha az objektum olyan partícióban van, amelyhez a szubjektum hozzá van rendelve, és az alábbi két feltétel egyike teljesül:
  1. Az objektum egy „Public” (nyilvános) objektum, azaz a PRIVATE tulajdonság FALSE, vagy
  2. A szubjektum az objektumot birtokló Partition Userhez van hozzárendelve.

- Megengedett műveletek az objektum tulajdonság definíció által engedélyezettek az alábbi megszorítások keretein belül:
  1. Egy Partition User a Crypto User szerepkörben csak a User műveletekhez fér hozzá, és
  2. A HSM és a Partíció képesség és szabály beállítások által kiszabott megszorítások.

2.5.1 Objektum védelem

A modul kriptográfiailag védi a belső flash memóriában tárolt érzékeny objektumok tartalmát. Az érzékeny értékek védelmét a modul AES256 algoritmussal, három különböző védelmi szerepkört ellátó kulccsal biztosítja. A felhasznált három kulcs az alábbiak:

- User Storage Key (USK)/Security Officer Master Key (SMK) – Ezt a kulcsot a modul a felhasználó vagy az SO létrehozásakor generálja. A felhasználói kulcsok kriptográfiai elkülönítésére szolgál.

- Master Tamper Key (MTK) – Ez a kulcs elemmel rendelkező RAM-ban tárolódik. Rejtjelezi generálásuk után a kulcsokat, így azokat csak a kriptográfiai processzor képes felhasználni, illetve biztosítja, a kriptográfiai processzor által átadott információt hitelességét.
- Key Encryption Key (KEK) Ez a kulcs elemmel rendelkező RAM-ban tárolódik. Ez a kulcs szintén rejtjelez minden érzékeny objektumot, a célja, hogy a megvalósítsa a semlegesítés funkciót. A KEK törlődik, amennyiben megsemmisítés jelet kap. Ez megakadályozza az érzékeny objektumhoz történő hozzáférés lehetőségét, azokban az esetekben, amikor a modul másképp nem tud reagálni.

2.5.2. Objektum újrahasználat

A hozzáférés ellenőrzési szabályzatot egy objektum újrahasználat szabályzat egészíti ki. Az objektum újrahasználat szabály megköveteli, hogy egy objektumhoz allokált erőforrások információtartalma törlődjön, mielőtt azokat egy másik objektum számára újra lefoglalná a rendszer.

2.5.3. Privilegizált funkciók

A modulnak kizárólag az SO szerepkörre kell korlátoznia az alábbi funkciók végrehajtását:

- Modul inicializálás
- Partíció létrehozás és törlés
- A modul és a partíciók szabályainak konfigurálása
- Modul törlés
- Förmver frissítés

2.6. A kriptográfiai kulcsok menedzsmentje

A kriptográfiai kulcsok menedzsmentje funkció a kulcsok bizalmasságát védi azok teljes életciklusában. A modul által biztosított, FIPS PUB 140-2 jóváhagyott kulcsmenedzsment funkciók az alábbiak:

(1) Determinisztikus véletlenszám generálás az NIST SP 800-90 10.2.1 fejezetének megfelelően.
(2) Kriptográfiai kulcsok generálása az alábbi szabványoknak megfelelő módon:
    a. RSA 1024-4096 bites kulcspárral a FIPS PUB 186-2 szerint.
    b. TDES 112, 168 bittel (SP 800-67, ANSI X9.52).
    c. AES 128, 192, 256 bittel (FIPS PUB 197).
    d. DSA 1024, 2048 és 3072bites kulcspárral a FIPS PUB 186-3 szerint.
    e. ECDSA (SP 800-57 szerinti paraméterekkel) a FIPS PUB 186-3 szerint.
    f. Diffie-Hellman kulcs pár
    g. Kulcs származtatás NIST SP 800-108 szerint (Counter & Feedback módokban).
(3) Diffie-Hellman (2048-3072 bit) kulcsegyeztetési, kulcs kialakítási módszer 112 és 128 bit közötti rejtjelezési erősséget biztosít
(4) EC Diffie-Hellman (ECDH) (SP 800-57 szerinti paraméterekkel) kulcsegyeztetési NIST SP 800-56A alapján.
(5) Biztonságos kulcstárolás (AES 256 bite rejtjelezést használva) és kulcs hozzáférés a PKCS#11 szabványnak megfelelően.
(6) A kriptográfiai kulcsok megsemmisítése az alábbi három mód egyike szerint hajtódik végre a PKCS#11 és FIPS PUB 140-2 szabványokkal összhangban:
    a. Egy Luna kriptográfiai modulon lévő objektum, amelyet a PKCS#11 C_DestroyObject funkciójával töröltek, érvénytelen jelet kap és a Partition User kulcsával vagy egy Luna kriptográfiai modul általános titkos kulcsával rejtjelezett marad mindaddig, ameddig a szóban forgó memóriahely (flash vagy RAM) újraallokálásra nem kerül a Luna kriptográfiai modul más adatai számára; ekkor törlődik és felülíródik az újraallokálás előtt.
    b. A Luna kriptográfiai modul olyan objektumai, amelyek sikertelen hitelesítés következtében lettek megsemmisítve, felülíródnak (minden flash blokk a Partition User memóriában 1-re állítódik). Ha SO-ra vonatkozik a sikertelen hitelesítés, akkor a Luna kriptográfiai modulon kulcs és adattárolásra használt minden flash blokk felülíródik.

c. A Luna kriptográfiai modulon lévő objektumok, amelyeket a C_InitTokennel (ami API-n keresztül rendelkezésre álló, SO által elérhető parancs a Luna kriptográfiai modul inicializálásához) lettek megsemmisítve, felülíródnak, az SO és a Partition Userek által használt flash memória többi részével együtt.

A kulcsok mindig privát vagy titkos kulcsobjektumokként tárolódnak az érzékeny tulajdonság bekapcsolásával. A kulcsérték ezért titkosított formában tárolódik, a tulajdonos Partititon User titkos kulcsával rejtjelezve. A kulcsokhoz való hozzáférés soha nem közvetlenül történik a hívó alkalmazás számára. Az adott kulcshoz egy kezelő (handle) a visszatérési érték, amelyet az alkalmazás a soron következő hívásokban használhat a kriptográfiai műveletek végrehajtása céljából.

A privát és titkos kulcsobjektumok a modulba importálhatók a kicsomagolás, kimaszkolás (ha a klónozás engedélyezett HSM szinten) vagy származtatás műveletek segítségével a hozzáférés ellenőrzési szabályoknak megfelelően. Bármely ily módon importált, külsőleg beállított kulcstulajdonságot a modul figyelmen kívül hagy, és beállítja a saját hozzáférés ellenőrzési szabályaival összhangban lévő értékre.

2.7. Kriptográfiai műveletek

Az általános jellege miatt, a modul kriptográfiai processzora és förmvere kriptográfiai algoritmusok és mechanizmusok széles skáláját támogatja. A jóváhagyott kriptográfiai funkciók és algoritmusok, melyek a FIPS 140-2 szempontjából lényegesek, az alábbiak:

1. Szimmetrikus rejtjelezés/dekódolás (kulcs becsomagolás/kicsomagolás): TDES 168 bittel és AES 128, 192 valamint 256 bittel a PKCS #11 szerint.
2. Szimmetrikus rejtjelezés/dekódolás: TDES 112, 168 bittel (SP 800-67, ANSI X9.52).
3. Szimmetrikus rejtjelezés/dekódolás: AES 128, 192, 256 bittel (FIPS PUB 197).
4. Aszimmetrikus kulcs becsomagolás/kicsomagolás: RSA 1024-4096 (PKCS #1 V1.5 és OAEP)
5. Aláírás létrehozás/ellenőrzés: (FIPS PUB 186-3): RSA 1024-3072 bittel (PKCS #1 V1.5) és SHA-1, SHA-224, SHA-256, SHA-384, SHA-512;
   RSA 1024-3072 bittel (PSS) és SHA-1, SHA-224, SHA-256, SHA-384, SHA-512;
   RSA 1024-3072 bittel (X9.31) és SHA-1;
   DSA 1024-3072 bittel és SHA-1, SHA-224, SHA-256;
   ECDSA és SHA-1, SHA-224, SHA-256, SHA-384, SHA-512,
6. Aláírás létrehozás/ellenőrzés (FIPS PUB 186-2): RSA 1024-4096 bittel és SHA-1, SHA-224, SHA-256, SHA-384, SHA-512; DSA 1024 bittel és SHA-1.
7. Hash generálás SHA-1, SHA-224, SHA-256, SHA-384, SHA-512 (FIPS PUB 180-3).
8. Kulcsolt hash generálás HMAC használata a következőkkel: SHA-1, SHA-224, SHA-256, SHA-384, SHA-512 (FIPS PUB 198).
9. Üzenet hitelesítés: TDES MAC (FIPS PUB 113) és CMAC (NIST SP 800-38B).
10. Determinisztikus véletlenszám generálás (NIST SP 800-90 10.2.1 fejezetének megfelelően)

4. táblázat A SafeXcel 3120 kriptográfiai processzorban implementált algoritmus validálások tanúsítványai

Algoritmus validálások tanúsítványai	**Tanúsítvány szám**
Szimmetrikus algoritmus	
AES: (ECB, CBC, GCM); rejtjelezés/megoldás; Kulcsméret = 128, 192, 256	1743
Triple-DES: (ECB, CBC); rejtjelezés/megoldás KO 1,2	1130
Lenyomatoló algoritmus (SHS)	
SHA-1, SHA-224, SHA-256, SHA-384, SHA-512 (Byte Only)	1531
Üzenet hitelesítő kód (HMAC)	
HMAC-SHA-1, HMAC-SHA-224, HMAC-SHA-256, HMAC-SHA-384, HMAC-SHA-512	1021
Triple-DES MAC	1137
Aszimmetrikus algoritmus	
RSA: **FIPS186-2:** ALG[ANSIX9.31]; KEYGEN(Y); SIG (gen); SIG (ver) (MOD: 1024,	865

1536, 2048, 3072, 4096 PubKey Values: 3, 17, 65537); ALG[RSASSAPKCS1_ V1_5]; SIG(gen); SIG(ver); (MOD: 1024, 1536, 2048, 3072, 4096); ALG[RSASSA-PSS]; SIG(gen); SIG(ver); (MOD: 1024, 1536, 2048, 3072, 4096)	
DSA: **FIPS186-3: PQG(gen):** [(1024,160) SHA(1); (2048, 224) SHA(224); (2048,256)SHA(256); (3072,256)SHA(256);] **KEYGEN:** [(1024,160); (2048,224); (2048,256) (3072,256)] **SIG(gen):** [(1024,160) SHA(1); (2048,224) SHA(1 , 224); (2048,256) SHA(1 , 224 , 256); (3072,256) SHA(1 , 224 , 256);] **SIG(ver):** [(1024,160) SHA(1); (2048,224) SHA(1 , 224); (2048,256) SHA(1 , 224 , 256); (3072,256) SHA(1 , 224 , 256);]	230
Véletlenszám generálás	
NIST SP 800-90 DRBG (CTR) AES-256	114

5. táblázat A SafeXcel 1746 kriptográfiai processzorban implementált algoritmus validálások tanúsítványai

Algoritmus validálások tanúsítványai	**Tanúsítvány szám**
Szimmetrikus algoritmus	
AES: (ECB, CBC, CFB8); rejtjelezés/megoldás; Kulcsméret = 128, 192, 256)	1756
Triple-DES: (ECB, CBC, CFB8); rejtjelezés/megoldás KO 1,2	1137
Üzenet hitelesítő kód (HMAC)	
Triple-DES MAC	1137
Aszimmetrikus algoritmus	
DSA: **FIPS186-2: SIG(gen); SIG(ver)** MOD (1024) **FIPS 186-3: SIG(gen):** [(1024,160) SHA(1, 224, 256); (2048,224) SHA(224 , 256); (2048,256) SHA(256); (3072,256) SHA(256)] **SIG(ver):** [(1024,160) SHA(1, 224, 256); (2048,224) SHA(224 , 256); ; (2048,256) SHA(256); (3072,256) SHA(256)]	548
ECDSA: **FIPS186-2: SIG(gen):** CURVES(P-192 P-224 P-256 P-384 P-521 K-163 K-233 K-283 K-409 K-571 B-163 B-233 B-283 B-409 B-571) **SIG(ver):** CURVES(P-192 P-224 P-256 P-384 P-521 K-163 K-233 K-283 K-409 K-571 B-163 B-233 B-283 B-409 B-571) **FIPS186-3: SIG(gen):** CURVES(P-192: (SHA-1, 224, 256, 384, 512) P-224: (SHA-1, 224, 256, 384, 512) P-256: (SHA-1, 224, 256, 384, 512) P-384: (SHA-1, 224, 256, 384, 512) P-521: (SHA-1, 224, 256, 384, 512) K-163: (SHA-1, 224, 256, 384, 512) K-233: (SHA-1, 224, 256, 384, 512) K-283: (SHA-1, 224, 256, 384, 512) K-409: (SHA-1, 224, 256, 384, 512) K-571: K-283: (SHA-1, 224, 256, 384, 512) B-163: (SHA-1, 224, 256, 384, 512) B-233 (SHA-1, 224, 256, 384, 512) B-283: (SHA-1, 224, 256, 384, 512) B-409: (SHA-1, 224, 256, 384, 512) B-571: (SHA-1, 224, 256, 384, 512) **SIG(ver):** CURVES(P-192: (SHA-1, 224, 256, 384, 512) P-224: (SHA-1, 224, 256, 384, 512) P-256: (SHA-1, 224, 256, 384, 512) P-384: (SHA-1, 224, 256, 384, 512) P-521: (SHA-1, 224, 256, 384, 512) K-163: (SHA-1, 224, 256, 384, 512) K-233: (SHA-1, 224, 256, 384, 512) K-283: (SHA-1, 224, 256, 384, 512) K-409: (SHA-1, 224, 256, 384, 512) K-571: K-283: (SHA-1, 224, 256, 384, 512) B-163: (SHA-1, 224, 256, 384, 512) B-233 (SHA-1, 224, 256, 384, 512) B-283: (SHA-1, 224, 256, 384, 512) B-409: (SHA-1, 224, 256, 384, 512) B-571: (SHA-1, 224, 256, 384, 512)	233

6. táblázat A förmverben implementált algoritmus validálások tanúsítványai

Algoritmus validálások tanúsítványai	Tanúsítvány szám
Szimmetrikus algoritmus	
AES: (ECB, CBC, OFB, CFB8, CFB128 GCM); rejtjelezés/megoldás; Kulcsméret = 128, 192, 256)	1750
Triple-DES: (ECB, CBC, CFB8, CFB64); rejtjelezés/megoldás KO 1,2	1134
Lenyomatoló algoritmus (SHS)	
SHA-1, SHA-224, SHA-256, SHA-384, SHA-512 (Byte Only)	1537
Üzenet hitelesítő kód (HMAC)	
HMAC-SHA-1, HMAC-SHA-224, HMAC-SHA-256, HMAC-SHA-384, HMAC-SHA-512	1027
Triple-DES MAC	1134
CMAC (A tesztelt kulcsméretek: 128 192 256)	1750
Aszimmetrikus algoritmus	
RSA: **FIPS186-2**: [ANSIX9.31]; KEYGEN; SIG (gen); SIG (ver) (MOD: 1024, 1536, 2048, 3072, 4096 PubKey Values: 3, 17, 65,537); [RSASSA-PKCS1_V1_5]; SIG(gen); SIG(ver); (MOD: 1024, 1536, 2048, 3072, 4096); SHA(1, 224, 256, 384, 512); [RSASSA-PSS]; SIG(gen); SIG(ver); (MOD: 1024, 1536, 2048, 3072, 4096) SHA(1, 224, 256, 384, 512)) **FIPS 186-3:** [ANSIX9.31]; SIG(gen); SIG (ver) (MOD: 1024 SHA(1, 224, 256, 384, 512); 2048 SHA(1, 224, 256, 384, 512); 3072); SHA(1, 224, 256, 384, 512)); [RSASSA-PKCS1_V1_5]; SIG(gen); SIG(ver); (MOD: 1024 SHA(1, 224, 256, 384, 512); (2048 SHA(1, 224, 256, 384, 512); 3072; SHA(1, 224, 256, 384, 512); ALG[RSASSA-PSS]; SIG(gen); SIG(ver); (MOD: 1024 SHA(1, 224, 256, 384, 512), 2048 SHA(1, 224, 256, 384, 512), 3072 SHA(1, 224, 256, 384, 512))	870
DSA: **FIPS186-2: KEYGEN(Y); SIG(gen); SIG(ver)** MOD (1024) **FIPS186-3:** **KEYGEN:** [(1024,160); (2048, 224); (2048,256); (3072,256)] **SIG(gen):** [(1024,160) SHA(1); (2048, 224) SHA(224); (2048,256) SHA(256); (3072,256) SHA(256)] **SIG(ver):** [(1024,160) SHA(1); (2048, 224) SHA(224); (2048,256) SHA(256); (3072,256) SHA(256)]	546
ECDSA: **FIPS186-2: PKG:** CURVES(P-192 P-224 P-256 P-384 P-521 K-163 K-233 K-283 K-409 K-571 B-163 B-233 B-283 B-409 B-571) **SIG(gen):** CURVES(P-192 P-224 P-256 P-384 P-521 K-163 K-233 K-283 K-409 K-571 B-163 B-233 B-283 B-409 B-571) **SIG(ver):** CURVES(P-192 P-224 P-256 P-384 P-521 K-163 K-233 K-283 K-409 K-571 B-163 B-233 B-283 B-409 B-571) **FIPS186-3: PKG:** CURVES(P-192 P-224 P-256 P-384 P-521 K-163 K-233 K-283 K-409 K-571) **SIG(gen):** CURVES(P-192: (SHA-1, 224, 256, 384, 512) P-224: (SHA-1, 224, 256, 384, 512) P-256: (SHA-1, 224, 256, 384, 512) P-384: (SHA-1, 224, 256, 384, 512) P-521: (SHA-1, 224, 256, 384, 512) K-163: (SHA-1, 224, 256, 384, 512) K-233: (SHA-1, 224, 256, 384, 512) K-283: (SHA-1, 224, 256, 384, 512) K-409: (SHA-1, 224, 256, 384, 512) K-571: K-283: (SHA-1, 224, 256, 384, 512) B-163: (SHA-1, 224, 256, 384, 512) B-233 (SHA-1, 224, 256, 384, 512) B-283: (SHA-1, 224, 256, 384, 512) B-409: (SHA-1, 224, 256, 384, 512) B-571: (SHA-1, 224, 256, 384, 512) **SIG(ver):** CURVES(P-192: (SHA-1, 224, 256, 384, 512) P-224: (SHA-1, 224, 256, 384, 512) P-256: (SHA-1, 224, 256, 384, 512) P-384: (SHA-1, 224, 256, 384, 512) P-521: (SHA-1, 224, 256, 384, 512) K-163: (SHA-1, 224, 256, 384, 512) K-233: (SHA-1, 224, 256, 384, 512) K-283: (SHA-1, 224, 256, 384, 512) K-409: (SHA-1, 224, 256, 384, 512) K-571: K-283: (SHA-1, 224, 256, 384, 512) B-163: (SHA-1, 224, 256, 384, 512) B-233 (SHA-1, 224, 256, 384, 512) B-283: (SHA-1, 224, 256, 384, 512) B-409: (SHA-1, 224, 256, 384, 512) B-571: (SHA-1, 224, 256,	231

384, 512)	
Kulcs egyeztetés	
ECC: (ASSURANCES) **SCHEMES** [**Ephemeral Unified** (KARole(s): Initiator / Responder) (**EA:** P-192 SHA1 SHA224 SHA256 SHA384 SHA512) (**EB:** P-224 SHA224 SHA256 SHA384 SHA512) (**EC:** P-256 SHA256 SHA384 SHA512) (**ED:** P-384 SHA384 SHA512) (**EE:** P-521)] [**OnePassDH** (**No_KC:** [N/A]) (KARole(s): Initiator / Responder) (**EA:** P-192 SHA1 SHA224 SHA256 SHA384 SHA512 CMAC) (**EB:** P-224 SHA224 SHA256 SHA384 SHA512 HMAC) (**EC:** P-256 SHA256 SHA384 SHA512 HMAC) (**ED:** P-384 SHA384 SHA512 HMAC) (**EE:** P-521)]	23
Diffie-Hellman kulcsegyeztetési, kulcs kialakítási módszer 112 és 128 bit közötti rejtjelezési erősséget biztosítva	
Kulcs továbbítás	
RSA (kulcs csomagolási, kulcs kialakítási módszer 80 és 152 bit közötti rejtjelezési erősséget biztosít)	
Kulcs származtatás	
NIST SP 800-108 (Counter Mode)	

2.8. Öntesztek

A modul öntesztet biztosít a bekapcsoláskor és igény esetén a förmver sértetlenségének megállapítása, valamint a véletlenszám generátor és a megvalósított kriptográfiai algoritmusok mindegyikének ellenőrzése céljából.

7 táblázat Modul öntesztek

Teszt	**Mikor hajtódik végre**	**Hatás**
A betöltő SHA-1 algoritmussal ellenőrzi a firmvare integritását annak elindítása előtt.	Bekapcsolás	Modul leállás[9]
DRBG inicializálás funkció Ismert válasz teszt (Known Answer Test (KAT))	Bekapcsolás	Modul leállás
DRBG generálás funkció KAT	Bekapcsolás	Modul leállás
DRBG újrakulcsolás funkció KAT	Bekapcsolás	Modul leállás
DRBG lezárás funkció KAT	Bekapcsolás	Modul leállás
TDES KAT	Bekapcsolás/Igény	Modul leállás/Hiba – leállás
SHA-1 KAT	Bekapcsolás/Igény	Modul leállás/Hiba – leállás
SHA-224 KAT	Bekapcsolás/Igény	Modul leállás/Hiba – leállás
SHA-256 KAT	Bekapcsolás/Igény	Modul leállás/Hiba – leállás
SHA-384 KAT	Bekapcsolás/Igény	Modul leállás/Hiba – leállás
SHA-512 KAT	Bekapcsolás/Igény	Modul leállás/Hiba – leállás
HMAC SHA-1 KAT	Bekapcsolás/Igény	Modul leállás/Hiba – leállás
HMAC SHA-224 KAT	Bekapcsolás/Igény	Modul leállás/Hiba – leállás
HMAC SHA-256 KAT	Bekapcsolás/Igény	Modul leállás/Hiba – leállás
HMAC SHA-384 KAT	Bekapcsolás/Igény	Modul leállás/Hiba – leállás
HMAC SHA-512 KAT	Bekapcsolás/Igény	Modul leállás/Hiba – leállás
RSA KAT	Bekapcsolás/Igény	Modul leállás/Hiba – leállás
DSA KAT	Bekapcsolás/Igény	Modul leállás/Hiba – leállás
Diffie-Hellman KAT	Bekapcsolás/Igény	Modul leállás/Hiba – leállás
AES KAT	Bekapcsolás/Igény	Modul leállás/Hiba – leállás
AES-GCM KAT	Bekapcsolás/Igény	Modul leállás/Hiba – leállás
ECDH KAT	Bekapcsolás/Igény	Modul leállás/Hiba – leállás
ECDSA KAT	Bekapcsolás/Igény	Modul leállás/Hiba – leállás
KDF KAT	Bekapcsolás/Igény	Modul leállás/Hiba – leállás
DRBG conditional tests	Folyamatos	Hiba – leállás

[9] A hiba részletei egy modul leállást követő a duál-portból kinyerhetők.

HRNG conditional tests	Folyamatos	Hiba – leállás
RSA – Kulcspár összetartozás ellenőrzés	Generáláskor	Hiba
DSA – Kulcspár összetartozás ellenőrzés)	Generáláskor	Hiba
ECDSA – Kulcspár összetartozás ellenőrzés	Generáláskor	Hiba
Firmware betöltés teszt (4096-bit RSA aláírás ellenőrzéssel)	Förmver frissítés betöltéskor	Hiba – a modul a létező förmverrel folytatja a működést

A bekapcsolási tesztek futtatása során a modul összes interfésze le van tiltva egészen az önteszt sikeres befejezéséig.

2.9. Förmver biztonság

A Förmver Biztonsági Szabályzat szerint minden förmver imaget, melyet a szabályzatnak megfelelően töltöttek be, a SafeNet ellenőrzött annak biztosítása céljából, hogy a förmver helyesen működik. A szabályzat vonatkozik a kezdeti förmver betöltésre és a későbbi förmver frissítésekre is.

A modulnak nem szabad megengednie, hogy külső szoftvert[10] töltsenek a hatókörén belülre. Csak megfelelően kialakított förmver tölthető be. A kezdeti vagy későbbi förmver célmodulba juttatását egy erre a funkcióra dedikált SafeNet modulnak kell kezdeményeznie. A SafeNet gyártási aláíró kulccsal a förmvert alá kell írni, és rejtjelezni kell egy titkos kulccsal, melyet a fogadó modul a megoldáshoz származtatni képes (a belsőleg tárolt titkos kulcs alapján)). Az aláírás RSA (4096 bit) PKCS #1 V1.5 SHA-256 jóváhagyott aláírási algoritmusok felhasználásával történik. A titkosítatlan förmver nem lehet látható a modulon kívül sem a betöltési művelet előtt, sem alatta, sem pedig utána.

A Bootloader mechanizmusokat kell biztosítania a saját sértetlenségének védelme érdekében, és a kriptográfiai modulon belül tárolt mindennemű tartós biztonság-kritikus adat sértetlenségének garantálása céljából.

2.10. Fizikai biztonság

A Luna kriptográfiai modul egy többchipes beágyazott modul, a FIPS PUB 140-2 4.5 szakaszának megfelelően. Bontásvédelemi mechanizmust biztosító erős fém külső borítással rendelkezik. A modul biztonságát veszélyeztető fizikai manipuláció észlelhető a modul fizikai sértetlenségének vizuális vizsgálatával. A borítás a nyomtatott áramkör panelra van rákötve, és a borítás eltávolítási kísérlete a kártyán jelentős károkat okoz, aminek következtében a modul működésképtelenné válik.

A modul borítása átlátszatlan az eszköz elemei elrendezésének vizuális vizsgálata megakadályozása érdekében, valamint az eszköz fizikai vizsgálatának és az egyedi komponensein lévő érzékeny adatokhoz való hozzáférési kísérletekkel szembeni ellenállás biztosítása céljából.

A modulon belül tárolt nyílt szövegű kritikus biztonsági paraméterek (CSP) a Master Tamper Key (MTK), a Key Encryption Key (KEK) és az Token/Module Variable Key (TVK), amik az automatikus aktiválási tulajdonság megvalósításához szükséges. Az MTK, KEK és TVK az elemmel rendelkező RAM-ban tárolódnak.
Az MTK és TVK fizikai manipuláció érzékelése esetén felülíródik – akkor is, ha a külső fizikai manipulációt észlelő jel riaszt be, és akkor is, ha a PCI-e slotból távolítják el a kártyát. A KEK törlődik, ha visszavonási jel érkezik.
A modul érzékel és reagál a működési tartományon kívüli hőmérséklet és feszültség értékekre. Ezekben az esetekben a memória törlődik, és a működés leáll. Ha az értékek visszaállnak a normál tartományba a modul újraindítás után működésbe hozható.

[10] Külső szoftveren végrehajtható kódok bármely formája értendő, melyet a SafeNeten kívül más hozott létre, és nem legitim SafeNet förmver imageként lett kialakítva és aláírva.

2.10.1 Biztonságos visszaállítás

Az MTK létrehozásakor két szeletre kerül bontásra. Az egyik szelet az elemmel rendelkező RAM-ban tárolódik, a másik a modul förmverébe kerül. Ez utóbbi szelet kiírható a lila iKey-re akár M az N-ből módszerrel.
Tamper esemény esetén, miután a tamper állapot ellenőrzésre került, lehetséges visszaállítani a modul működőképességét, az MTK visszaállításával a belső szelet és a lila iKey-en tárolt szelet segítségével.
A biztonságos visszaállítás tulajdonság felhasználható a modul biztonságos szállítására is. Az MTK törölhető egy kriptográfiai modul paranccsal, így a modul biztonságos szállítás módba kerül. Így biztosítható, hogy az érzékeny objektumok kriptográfiailag védettek, és a modul nem használható rosszhiszeműen a szállítás alatt. Az eszköz működőképessége visszaállítható a biztonságos visszaállítás funkció segítségével.

2.11. EMI / EMC

A modul megfelel az FCC 15. rész B osztály követelményeinek.

2.12. Hibatűrés

Amennyiben bármilyen okból az áramellátás megszakad, a modulnak minimális követelményként olyan állapotban kell tartania magát, hogy vissza tudjon állni a működőképes állapotba az áramellátás helyreállása után, anélkül, hogy a funkcionalitás vagy a tartósan tárolt adatok kompromittálódnának.
A modulnak a biztonságos állapotot fenn kell tartania adat input/output hibák bekövetkezte esetén. Amikor az adat input/output képesség helyreáll, a modul visszatér a működés azon állapotába, amelyben az input/output hibát megelőzően volt.

2.13. Egyéb támadások csökkentése

Az időzítéses támadások kockázatát a modul mechanizmusai csökkentik közvetlenül a moduláris hatványozási műveletek esetén a hardver gyorsító chip használatával. A hardvergyorsító alkalmazása biztosítja, hogy minden RSA aláírási művelet majdnem ugyanazon idő alatt fejeződik be, így az időkülönbségek elemzése irrelevánssá válik. Az RSA blinding pedig szintén egy választható opció az ilyen típusú támadások kockázatának csökkentése érdekében.

A kriptográfiai modul csatlakozót biztosít, amivel lehetővé válik külső fizikai beavatkozási esemény jelének fogadása.

A jelre való reagálással a modul biztosíthatja, hogy nem marad érzékeny adat, még akkor sem, ha célzott támadással a külső fizikai védelmi mechanizmusokon áthatolnak.

Két forrása van a lehetséges tamper jelnek. az első esetben a kriptográfiai modul áramköre detektálja a modul eltávolítását a slotból. A külső jelre való reagálással a modul biztosítja, hogy minden nyílt érzékeny adat törlődik, ha a modult eltávolítják a slotból.
A második forrás csak appliance-ba történő telepítés során van alkalmazva. Ebben az esetben a jelzés akkor érkezik, ha a behatolást jelző áramkör az appliance fedelének nyitását érzékeli. A külső jelre való reagálással a modul biztosítja, hogy minden nyílt érzékeny adat törlődik az appliance fedelének nyitása esetén.

3. A FIPS Tanúsítvány eredményeinek összefoglalása

A Luna® PCI-e kriptográfiai modul egy kriptográfiai modulok tesztelésére az Egyesült Államokban és Kanadában akkreditált laboratórium megvizsgálta, értékelte és tesztelte az alábbi követelményrendszernek való megfelelőség szempontjából:

> *a FIPS 140-2-ből (Kriptográfiai modulokra vonatkozó biztonsági követelmények) származtatott teszt követelmények*
> */Derived Test Requirements for FIPS 140-2, Security Requirements for Cryptographic Modules/*

A (FIPS) értékelés eredményei az alábbiak voltak:

A kriptográfiai modul tervezése:	3-as szint
Modul portok és interfészek:	3-as szint
Szerepkörök, szolgáltatások és hitelesítés:	3-as szint
Véges állapotú automata modell:	3-as szint
Fizikai biztonság /több chipes, beágyazott/:	3-es szint
Kriptográfiai kulcsgondozás:	3-as szint
Elektromágneses interferencia és kompatibilitás:	3-as szint
Ön-tesztek:	3-es szint
Tervezési biztosíték:	3-as szint
Más támadások enyhítése:	3-as szint
A kriptográfiai modul biztonsági szabályzata	3-as szint
Működési környezet:	nincs értékelve

Az elért általános biztonsági szint:	**3-as**

4. A Luna® PCI-e kriptográfiai modul értékelési követelményei a FIPS 140-2 szerint

Az alábbiakban áttekintjük azokat a (FIPS 140-2 követelményrendszer 3-as szintjéből fakadó) biztonsági követelményeket, melyeknek való megfelelőséget a Luna® PCI-e kriptográfiai modul értékelését végző laboratórium vizsgálta és igazolta.

Az alábbi jelölést alkalmazzuk:

KÖV_x.y: a FIPS 140-2 x. fejezetének y. biztonsági követelménye.[11]

4.1. A kriptográfiai modul tervezése és dokumentálása

KÖV_01.01:
A kriptográfiai modulnak tartalmaznia kell hardverek, szoftverek, förmverek halmazát vagy ezek olyan kombinációját, mely kriptográfiai funkciókat vagy eljárásokat valósítanak meg, beleértve ebbe a kriptográfiai algoritmusokat és esetlegesen a kulcsgenerálást is, mindezt egy meghatározott kriptográfiai határon belül.

KÖV_01.02:
A kriptográfiai modulnak legalább egy FIPS által jóváhagyott biztonsági funkciót kell megvalósítania, melyet FIPS által Jóváhagyott működési módban kell használnia.

KÖV_01.03:
A kezelőnek értesülnie kell arról, hogy a Jóváhagyott működési mód lett kiválasztva.

KÖV_01.04:
A modulnak jeleznie kell, hogy a FIPS által Jóváhagyott működési mód lett kiválasztva.

KÖV_01.05:
A kriptográfiai határnak tartalmaznia kell egy pontosan meghatározott vonalat, ami a kriptográfiai modul fizikai határát jelenti.

KÖV_01.06:
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_01.07:
A következő dokumentálási követelményeknek meg kell felelnie minden hardvernek, szoftvernek és förmvernek, amiket a kriptográfiai modul tartalmaz.

KÖV_01.08:
A dokumentációnak teljes mértékben meg kell határoznia a kriptográfiai modul minden hardver, szoftver és förmver komponensét, meg kell határoznia a modulnak a kriptográfiai határát, amely a komponenseket körülzárja, valamint teljes mértékben ismertetnie kell a modul fizikai konfigurációját.

KÖV_01.09:
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_01.10:
A dokumentációnak tartalmaznia kell a kriptográfiai modul összes fizikai és logikai interfészét.

[11] Csak azokat a követelményeket adjuk meg, mely a Luna® PCI-e kriptográfiai modul ténylegesen vonatkoznak, ezért a követelmények sorszámozása nem mindig folyamatos.

KÖV_01.11:
A dokumentációnak tartalmaznia kell a kriptográfiai modul manuális és logikai kezelőit, a fizikai és logikai állapotjelzőit és a fizikai, logikai és elektromos karakterisztikáját.

KÖV_01.12:
A dokumentációnak fel kell sorolnia az összes biztonsági funkciót, mind a FIPS által Jóváhagyottakat, mind a nem Jóváhagyottakat, melyeket a kriptográfiai modulban felhasználnak, és meg kell határozni az összes működési módot, FIPS által Jóváhagyott és nem Jóváhagyott formában is.

KÖV_01.13:
A dokumentációnak tartalmaznia kell egy blokkdiagramot, amely leírja a modul minden fontos hardver komponensét és azok csatlakozásait, beleértve ebbe a mikroprocesszorokat, input/output puffereket, nyílt szöveg/rejtjelezett szöveg pufferek, vezérlési pufferek, kulcstárak, működési memória és program memória.

KÖV_01.14:
A dokumentációnak meg kell határoznia a hardver, szoftver és förmver komponensek tervezését. Magasszintű specifikációs nyelvet kell használni a szoftver/förmver vagy a hardver séma tervezésének leírására.

KÖV_01.15:
A dokumentációnak meg kell határoznia minden biztonsággal kapcsolatos információt, mint a titkos és magán kriptográfiai kulcsok (nyílt és titkosított formában), autentikációs adatok (pl. jelszavak, PIN kódok), és más védett információk (pl. naplózott események, naplóadatok), melyek közzététele vagy módosítása kompromittálja a modul biztonságát.

KÖV_01.16::
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[12] biztonsági követelményeiből illetve a gyártó által előírt járulékos biztonsági követelményekből származnak.

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.

KÖV_02.02:
A modul interfészeknek egymástól logikailag el kell különülniük, bár osztozhatnak egy fizikai porton (pl. a bejövő adat beléphet, a kimenő adat távozhat ugyanazon a porton) vagy el lehetnek osztva egy vagy több fizikai portra (pl. a bejövő adat érkezhet a soros vagy párhuzamos portról is).

KÖV_02.03:
A modulnak legalább a következő négy logikai interfészt tartalmaznia kell:
- adat input interfész,
- adat output interfész,
- vezérlési input interfész,
- státusz output interfész.

KÖV_02.04:
Minden adatot (kivéve a vezérlési adatot, mely a vezérlői input interfészen érkezik), mely bekerül a modulba, és az feldolgozza (ilyen a nyílt adat, a titkos adat, kriptográfiai kulcsok és CSP-k, autentikációs adatok és állapot információk más moduloktól), az adat input interfészen keresztül kell bevinni.

[12] FIPS 140-2

KÖV_02.05:
Minden adatot (kivéve a vezérlési adatot, mely a vezérlői output interfészen távozik), mely kikerül a modulból (ilyen a nyílt adat, a titkos adat, kriptográfiai kulcsok és CSP-k, autentikációs adatok és állapot információk más moduloknak), az adat output interfészen keresztül kell kiolvasni.

KÖV_02.06:
Az adat output interfészen keresztül történő minden adat outputot le kell tiltani hiba állapot vagy az öntesztek végrehajtása során.

KÖV_02.07:
Minden input parancs, jel, vezérlő adat (pl. a hívások és a manuális vezérlők, mint a kapcsolók, gombok és billentyűzetek), melyek a modul működését befolyásolják, a vezérlési input interfészen keresztül kell, hogy közlekedjen.

KÖV_02.08:
Minden output jel, jelző és állapotinformáció (pl. a visszatérő kódok, és a fizikai jelzők, mint a LED-ek és a kijelzők), melyek a modul állapotának jelzésére szolgál, a státusz output interfészen keresztül kell, hogy közlekedjen.

KÖV_02.09:
Minden külső elektromos áramforrásnak, mely a kriptográfiai modulba csatlakozik, az elektromos áram interfészen keresztül kell, hogy illeszkedjen.

KÖV_02.10:
A modulnak meg kell különböztetnie az input adatot és vezérlést valamint az output adatot és állapotot.

KÖV_02.11:
Minden input adat, mely bekerül a modulba az adat input interfészen keresztül, csak az input adat úton keresztül közlekedhet.

KÖV_02.12:
Minden output adat, ami az adat output interfészen keresztül hagyja el a modult, csak az output adat úton keresztül közlekedhet.

KÖV_02.13:
Az output adat utat logikailag le kell kapcsolni az áramkörről és a folyamatokról a kulcsgenerálás, a manuális kulcsbejegyzés és a kulcs törlése során.

KÖV_02.14:
Az érzékeny információk véletlen kiszivárgásának megakadályozása érdekében két független belső lépés szükséges az adat kiadásához bármely output interfészen, melyen nyílt szövegű kriptográfiai kulcsok vagy CSP-k, illetve érzékeny adatok távoznak (pl. két független szoftver flag beállítása, melyek egyikét a felhasználó állítja; két hardveres kapu, melyek sorosan hajtanak végre két intézkedést).

KÖV_02.15:
A dokumentációnak a modul minden fizikai portot, logikai interfészt, input és output adat utat ismertető, teljes specifikációt kell tartalmaznia.

KÖV_02.16:
Azon fizikai portoknak, melyeken nyílt szövegű kriptográfiai kulcsok, autentikációs adatok és CSP-k érkeznek vagy távoznak, fizikailag el kell különülniük az összes többi porttól a modulon belül, vagy eleget kell tenniük a KÖV_02.17-nek.

KÖV_02.17:
Azon logikai interfészeknek, melyeken nyílt szövegű kriptográfiai kulcsok, autentikációs adatok és CSP-k érkeznek vagy távoznak, fizikailag el kell különülniük az összes többi interfésztől megbízható adatút segítségével, vagy eleget kell tenniük a KÖV_02.16-nak.

KÖV_02.18:
Nyílt szövegű kriptográfiai kulcs komponenseket, autentikációs adatokat és más CSP-ket közvetlenül a kriptográfiai modulba kell bevinni (pl. megbízható adatúton vagy közvetlenül csatolt kábelen).

4.3 Szerepkörök és szolgáltatások

KÖV_03.01:
A kriptográfiai modulnak támogatnia kell az operátori szerepköröket és az ezekhez tartozó megfelelő szolgáltatásokat.

KÖV_03.02:
Ha a modul több egyidejű operátort támogat, akkor a modulnak belsőleg le kell kezelnie az egyes operátorok által végrehajtott jogosult szerepkörök és szolgáltatások szétválasztását.

4.3.1 Szerepkörök

KÖV_03.03:
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:
A dokumentációnak teljes specifikációt kell nyújtania mindazokról a jogosult szerepkörökről, amelyeket a modul támogat.

4.3.2 Szolgáltatások

KÖV_03.07:
A *szolgáltatások* fogalom minden olyan szolgáltatásra, műveletre és funkcióra vonatkozik, amit a modullal végre lehet hajtani.

KÖV_03.08:
A szolgáltatás bemenet tartalmaz minden olyan adatot és vezérlőműveletet, ami kezdeményez vagy elér bizonyos szolgáltatást, műveletet vagy funkciót.

KÖV_03.09:
A szolgáltatás kimenet tartalmaz minden olyan adatot és vezérlőműveletet, ami egy szolgáltatás, művelet vagy funkció eredménye, amit egy szolgáltatás bemenet kezdeményezett.

KÖV_03.10:
Minden szolgáltatás inputnak egy szolgáltatás outputot kell eredményeznie.

KÖV_03.11:
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.
- jóváhagyott biztonsági funkciók végrehajtása: legalább egy jóváhagyott biztonsági funkció végrehajtása Jóváhagyott működési módban.

KÖV03.14:
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.

KÖV03.15:
A dokumentációnak tartalmaznia kell minden olyan modul által nyújtott szolgáltatást, melynél nem szükséges az operátor bizonyos szerepköre, valamint annak a leírása, hogy ezek a szolgáltatások nem befolyásolják a kriptográfiai kulcsokat, CSP-ket, illetve a modul teljes biztonságát.

4.3.3 Operátori hitelesítés

KÖV_03.16:
A biztonság fokától függően a modulnak legalább a következők egyikét támogatnia kell: szerepkör alapú hitelesítés vagy azonosság alapú hitelesítés.

KÖV_03.19:
Azonosságon alapuló hitelesítés 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_03.20:
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_03.21:
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_03.22:
A hitelesítő adatokat a modulon belül védeni kell a nyilvánosságra kerüléstől, a módosítástól és a helyettesítéstől.

KÖV_03.23:
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_03.24:
A hitelesítési eljárások erősségének teljesítenie kell a következő követelményeket:

KÖV_03.25:
Minden hitelesítési próbálkozásnál a véletlen kitalálás vagy a hibás elfogadás valószínűsége legalább 1/1.000.000 kell, hogy legyen.

KÖV_03.26:
Egy perc alatti többszörös hitelesítési kérések véletlen kitalálásának vagy hibás elfogadásának a valószínűsége 1/100.000 kell, hogy legyen.

KÖV_03.27:
A hitelesítési adatot a hitelesítés során el kell takarni az operátor elől (pl. nem látszódnak a képernyőn a karakterek).
KÖV_03.28:
A hitelesítési próbálkozás visszajelzése az operátor felé nem gyengítheti a hitelesítési eljárást.

KÖV_03.29:
A dokumentációnak tartalmaznia kell a következőket:
- a modul által nyújtott hitelesítési eljárások,
- az autentikációs adatok típusa, ami a hitelesítési eljárások eléréshez szükségesek,
- azon hitelesítési eljárás, mely a modul első eléréséhez és inicializáláshoz szükséges, valamint
- a különböző hitelesítési eljárások erőssége.

KÖV_03.32:
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:
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_04.03:
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_04.05:
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.

4.5. Fizikai biztonság

KÖV_05.01:
A kriptográfiai modulnak fizikai biztonsági eljárásokat kell alkalmaznia annak érdekében, hogy letiltsák a modul tartalmához való nem engedélyezett hozzáférést és hogy felfedezzék a modul nem nem engedélyezett működtetését és módosítását az telepítés során.

KÖV_05.02:
A kriptográfiai határon belül levő összes hardver, szoftver és förmver egységet védeni kell.

4.5.1 Közös követelmények[13]

KÖV_05.03:
A következő követelményeknek minden fizikai biztonsági alkotóra érvényesnek kell lenniük:

KÖV_05.04:
A dokumentációnak tartalmaznia kell a fizikai megvalósítás teljes specifikációját, valamint azt a biztonsági szintet, melyen a modul fizikai biztonsági eljárásai meg lettek valósítva.

KÖV_05.05:
A dokumentációnak tartalmaznia kell azoknak az alkalmazható biztonsági mechanizmusoknak a teljes leírását, amelyeket a modul alkalmazhat.

KÖV_05.12:
A modulnak rendelkeznie kell olyan gyártás során beépített alkatrésszel, ami megvédi a modult (pl. védőburkolat, mely a modul áramköreit veszi körül, ezzel védve a fizikai károsodástól).

KÖV_05.16:
A modulnak rendelkeznie kell olyan megoldással, ami lehetővé teszi a modulhoz való illetéktelen fizikai hozzáférés felfedését.

KÖV_05.17:
A modulnak a 3. biztonsági szinten a következő követelmények is eleget kell tennie:

KÖV_05.18:
Ha a kriptográfiai modul tartalmaz valamilyen nyílást vagy fedőt, vagy van karbantartási felülete, rendelkeznie kell olyan alkatrésszel, ami illetéktelen hozzáférés esetén kitörli az érzékeny adatokat a modulból.

KÖV_05.19:
Az illetéktelen hozzáférésre adott válasz során a törlő áramkörnek minden nyílt szövegű titkos kulcsot és CSP-t törölnie kell a nyílás kinyitásakor, a fedél elmozdításakor vagy a karbantartási felülethez való hozzáféréskor.

KÖV_05.20:
Az illetéktelen hozzáférésre való válaszadásnak és a törlő áramkörnek mindig működnie kell, amikor nyílt szövegként titkos kulcs vagy CSP van a modulban.

[13] Vagyis a kriptográfiai modul mindhárom lehetséges fizikai konfigurációjára (egy chipből álló, több chipes, beágyazott, illetve több chipes, önmagában álló) vonatkozik.

4.5.2 Több chipes, beágyazott kriptográfiai modulra vonatkozó követelmények

KÖV_05.33:
Több chipes, beágyazott kriptográfiai modul esetén a modulban lévő chipeknek olyan termék minőségűeknek kell lenniük, amelyek magukban foglalnak standard passziválási technikát is.

KÖV_05.34:
Több chipes, beágyazott kriptográfiai modul esetében a modult egy nem átlátszó, beavatkozást kimutató anyaggal kell beburkolni.

KÖV_05.36:
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.

4.6 Az operációs rendszer biztonsága

Nincsenek követelmények[14].

4.7 Kriptográfiai kulcsgondozás

4.7.1 Általános követelmények

KÖV_07.01:
A titkos és magán kulcsokat védeni kell a jogosulatlan felfedéssel, módosítással és helyettesítéssel szemben.

KÖV_07.02:
A nyilvános kulcsokat védeni kell a jogosulatlan módosítással és kicseréléssel szemben.

KÖV_07.03:
Dokumentációnak kell specifikálnia a kriptográfiai modulra vonatkozó kulcsgondozás minden vonatkozását.

4.7.2 Véletlenszám generátorok (RNG)

KÖV_07.04:
Amennyiben a modul Jóváhagyott vagy Nem jóváhagyott RNG-t használ Jóváhagyott működési módban, az RNG-ből származó adatnak teljesíteni kell a folyamatos véletlenszám generálási tesztet.

KÖV_07.06:
A Jóváhagyott RNG-ket alá kell vetni a kriptográfiai algoritmus tesztnek.

KÖV_07.07:
A nem-determinisztikus RNG-knek meg kell felelnie az összes, szabványban foglalt, alkalmazható követelménynek.

KÖV_07.08:
Jóváhagyott RNG-t kell használni a Jóváhagyott biztonsági funkció kriptográfiai kulcsainak generáláshoz.

KÖV_07.09:
A mag (seed) és a kezdeti kulcs (seed key) soha nem lehet ugyanolyan értékű.

KÖV_07.10:

[14] Mivel Luna® PCI-e kriptográfiai modul működési környezete nem képezi az értékelés részét.

A dokumentációban fel kell sorolni a modul által használt összes véletlenszám generátort.

4.7.3 Kulcs generálásra vonatkozó követelmények

KÖV_07.11:
Egy kriptográfiai modul opcionálisan ki lehet egészítve egy belső kulcs generálási funkcióval[15]. A modulnak egy FIPS által jóváhagyott kulcs generálási algoritmust kell implementálni

KÖV_07.12:
Ha a kulcs generálási folyamatban egy véletlenszám generátor is alkalmazva van[16], minden értéket olyan módon kell véletlenszerűen vagy pszeudo-véletlenszerűen generálni, hogy a bitek minden lehetséges kombinációja és minden lehetséges érték egyenlő valószínűséggel generálódjon.

KÖV_07.13:
A kulcsgenerálási eljárás biztonságának veszélyeztetéséhez legalább annyi művelet szükséges, amennyiből a véletlen kulcs értékét ki lehet találni.

KÖV_07.14:
Ha egy kezdeti *(seed)* kulcs alkalmazva van[17], akkor azt ugyanolyan módon kell bevinni, mint a kriptográfiai kulcsokat.

KÖV_07.15:
Közbenső kulcs generálási állapotoknak és értékeknek nem szabad hozzáférhetőnek lenniük a modulon kívül nyílt vagy más nem védett formában.

KÖV_07.16:
A dokumentációnak tartalmaznia kell a modul által használt összes kulcsgenerálási eljárást.

4.7.4 Kulcs szétosztásra vonatkozó követelmények

KÖV_07.17:
Egy kriptográfiai modulnak FIPS által jóváhagyott kulcs szétosztási technikát kell implementálnia.

KÖV_07.19:
A kulcs szétosztási eljárás veszélyeztetéséhez legalább annyi művelet szükséges, amennyiből a továbbított kriptográfiai kulcs értékét ki lehet számolni.

KÖV_07.20:
Amennyiben létezik kulcstovábbítási eljárás, a teljesíteni kell a kulcs be- és kivitelre vonatkozó követelményeket

KÖV_07.21:
A dokumentációnak specifikálnia kell a modul által alkalmazott kulcs szétosztási technikát.

4.7.5 Kulcs bevitelére és kivitelére vonatkozó követelmények

KÖV_07.22:
Kézi úton szétosztott kriptográfiai kulcsok bevihetők a kriptográfiai modulba, illetve outputként kinyerhetők abból, tisztán kézi módszerekkel vagy elektronikus módszerekkel.

KÖV_07.23:
Amennyiben egy kezdeti (seed) kulcs kerül a modulba a kulcsgenerálás során, azt a kriptográfiai kulcsokkal azonos feltételek mellett kell bevinni.

KÖV_07.24:

[15] A Luna® PCI-e kriptográfiai modul megvalósít belső kulcs generálási funkciót.
[16] A Luna® PCI-e kriptográfiai modul alkalmaz véletlenszám generátort.
[17] A Luna® PCI-e kriptográfiai modul véletlenszám generátora alkalmaz kezdeti *(seed)* kulcsot.

Minden titkosított titkos és nyilvános kulcsot, melyet a kriptográfiai modulba bevisznek vagy kivesznek, a FIPS által jóváhagyott módban egy FIPS által jóváhagyott algoritmussal kell titkosítani.

KÖV_07.25:
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_07.26:
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_07.27:
Ha kódolt kulcsok vagy kulcs komponensek kerülnek beírásra, az ebből származó nyílt formájú titkos vagy magán kulcsok nem jeleníthetők meg.

KÖV_07.28:
A dokumentációnak tartalmaznia kell minden olyan kulcs be- és kiviteli eljárást, melyet a kriptográfiai modul használ.

KÖV_07.30:
Az elektronikus úton szétosztott titkos és magán kulcsokat kódolt formában kell bevinni és kinyerni.

KÖV_07.31:
A kézi úton szétosztott titkos vagy magán kulcsokat nem szabad bevinni vagy outputként kinyerni a kriptográfiai modulból nyílt formában. Ha kézi úton szétosztott titkos vagy magán kulcsokat kell bevinni a kriptográfiai modulba vagy outputként kinyerni onnan, akkor ezeket a következő módszerek valamelyikével kell elvégezni:

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

KÖV_07.32:
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.

KÖV_07.33:
Osztott tudáson alapuló hitelesítés esetén 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.

KÖV_07.34:
Osztott tudáson alapuló eljárásoknál legalább két kulcs komponens szükséges az eredeti kriptográfiai kulcs újragenerálásához.

KÖV_07.35:
Osztott tudáson alapuló eljárások esetén a dokumentációban meg kell jelennie, hogy ha egy kulcs újragenerálásához n kulcs komponens kell, akkor n-1 kulcs komponens jelenléte nem elegendő az eredeti kulcshoz kapcsolódó bármilyen információ kinyeréséhez, kivéve a hosszát.

KÖV_07.36:
Osztott tudáson alapuló eljárások esetén a dokumentációnak tartalmaznia kell a modul által használt összes ilyen eljárást.

4.7.6 Kulcs tárolásra vonatkozó követelmények

KÖV_07.37:
Ha a titkos vagy magán kulcsokat a kriptográfiai modul tartalmazza, akkor azok tárolhatók nyílt formában.

KÖV_07.38:
A nyílt formájú kulcsok a modulon kívülről nem lehetnek hozzáférhetők.

KÖV_07.39:
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.

KÖV_07.40:
A dokumentációnak tartalmaznia kell minden kulcstárolás eljárást.

4.7.7 Kulcs megsemmisítésre vonatkozó követelmények

KÖV_07.41:
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.

KÖV_07.42:
A dokumentációnak tartalmaznia kell minden kulcstörlési eljárást.

4.8 Elektromágneses interferencia, elektromágneses kompatibilitás

KÖV_08.01:
A kriptográfiai modulnak eleget kell tennie az alábbi követelményeknek:

KÖV_08.02:
A kriptográfiai modulok jeladó részének (rádiónak) minden alkalmazható FCC követelménynek eleget kell tenniük.

KÖV_08.03:
A dokumentációban nyilatkozatot kell tenni az EMI/EMC követelményeknek való megfelelőségről.

KÖV_08.05:
Egy kriptográfiai modulnak alkalmazkodnia kell az EMI/EMC követelményekhez, amelyek a 47 Code of Federal Regulations 15. részében, a B alfejezetben, B osztályában (azaz a házi alkalmazásra vonatkozó részben) vannak megadva.

4.9 Ön-tesztek

4.9.1 Általános követelmények

KÖV_09.01:
A modulnak végre kell tudnia hajtani bekapcsolási öntéseket és feltételes öntéseket, ami a helyes működést biztosítja.

KÖV_09.02:
Bizonyos ön-teszteket akkor kell végrehajtani, amikor a modul áram alá kerül (áram alá helyezéskor végrehajtandó tesztek).

KÖV_09.03:
Egyéb ön-teszteket különböző feltételek esetén kell végrehajtani, általában akkor, ha egy meghatározott funkció vagy művelet kerül végrehajtásra (feltételhez kötött tesztek).

KÖV_09.04:
Amennyiben a kriptográfiai modul valamelyik ön-tesztje sikertelen, a modulnak hiba állapotba kell kerülnie, és hiba jelet kell kiadnia a státusz interfészen keresztül.

KÖV_09.05:
A modul semmilyen kriptográfiai funkciót nem végezhet addig, amíg hiba állapotban van.

KÖV_09.06:
A modul semmilyen adatot nem adhat ki outputként az adat output interfészen keresztül, amíg a hiba feltétel fennáll.

KÖV_09.07:
Minden lehetséges bekapcsolási és feltételes öntesztnek, 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).

4.9.2 Áram alá helyezési tesztek

4.9.2.1 Általános tesztek

KÖV_09.08:
Miután egy kriptográfiai modult áram alá helyeztek, a modulnak ön-teszt állapotba kell kerülnie.

KÖV_09.09:
Az áram alá helyezés utáni ön-tesztek nem igényelhetnek operátori közreműködést a futtatáshoz.

KÖV_09.10:
Amennyiben minden áram alá helyezés utáni teszt sikeres, akkor egy jelzést kell kiadni a "státusz output" interfészen keresztül.

KÖV_09.11:
Minden adat outputot le kell tiltani, amíg ezek a tesztek végrehajtás alatt állna.

KÖV_09.12:
A modulnak eszközöket kell biztosítania arra, hogy az áram alá helyezési teszteket igény esetén a modul periodikus tesztelésére is kezdeményezni lehessen.

KÖV_09.13:
A modulnak legalább a következő (áram alá helyezési) teszteket végre kell hajtania:

- kriptográfiai algoritmus teszt,
- szoftver/förmver teszt,
- a kritikus műveletek tesztje és

4.9.2.2 Kriptográfiai algoritmus tesztek

KÖV_09.16:
A kriptográfiai algoritmusokat tesztelni kell oly módon, hogy az algoritmust olyan adatokon kell végrehajtani, amelyekre vonatkozóan a helyes output már ismert ("ismert eredmény teszt"). Az ismert eredmény tesztet minden egyes kriptográfiai funkcióra vonatkozóan (pl. kódolás, dekódolás, hitelesítés) végre kell hajtani.

KÖV_09.17:
A teszt sikertelen, ha a kiszámított output nem egyezik meg a korábban generált outputtal.

KÖV_09.18:
Azon kriptográfiai algoritmusokat, melyek kimenete a bemenettől függ (pl. a DSA algoritmus), vagy az ismert eredmény teszttel vagy a pár konzisztencia teszttel kell ellenőrizni.

KÖV_09.19:
Az üzenet lenyomat készítő algoritmusok tesztelésére egy független ismert eredmény teszt vagy egy, a lenyomatoló algoritmushoz kapcsolódó kriptográfiai algoritmust tesztelő ismert eredmény teszt szükséges.

KÖV_09.20:
Ha a kriptográfiai modulnak két független megoldása van ugyanannak a kriptográfiai algoritmusnak a tesztelésére, akkor a két megvalósítás kimenetét folyamatosan össze kell hasonlítani.

KÖV_09.21:
Ha a kriptográfiai modulnak két független megoldása van ugyanannak a kriptográfiai algoritmusnak a tesztelésére, és a két megvalósítás kimenete nem egyezik, akkor a kriptográfiai algoritmus tesztnek nem felelt meg.

4.9.2.3 Szoftver/förmver teszt

KÖV_09.22:
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.

KÖV_09.23:
Amennyiben a kiszámolt eredmény nem egyenlő a korábban készített eredménnyel, a szoftver/förmver teszt nem felelt meg.

4.9.2.4 Kritikus funkciók tesztjei

KÖV_09.25:
Minden más, a modul biztonságos működése szempontjából kritikus funkció tesztelhető azon ön-tesztek részeiként, amelyeket az áram alá helyezéskor kell végrehajtani.

KÖV_09.26:
A meghatározott feltételek esetén végrehajtandó egyéb kritikus funkciókat a feltételhez kötött tesztek részeként kell végrehajtani.

KÖV_09.27:
A dokumentációnak teljes specifikációt kell szolgáltatnia a kritikus funkciókról és azon áram alá helyezési ön-tesztek természetéről, amelyek ezen funkciók számára ki vannak jelölve.

4.9.3 Feltételhez kötött tesztek

KÖV_09.29:
A feltételhez kötött teszteket a modulnak akkor kell végrehajtania, amikor a következő tesztek feltételei teljesülnek:

- páronkénti konzisztencia teszt,
- szoftver/förmver betöltési teszt,
- kézi kulcs bevitel teszt,
- folyamatos véletlenszám generátor teszt
- megkerülés teszt

4.9.3.1 Páronkénti konzisztencia teszt

KÖV_09.30:
Azon kriptográfiai modulok, amelyek nyilvános és magán kulcsokat generálnak, tesztelniük kell a kulcsokat a páronkénti konzisztencia szempontjából.

KÖV_09.31:
Ha a kulcsokat FIPS által jóváhagyott kulcstovábbításra használják, a nyilvános kulccsal kell titkosítani a nyílt szövegű értéket. Az eredményként kapott titkos szöveget kell összehasonlítani a nyílt szövegű értékkel. Ha a két érték egyezik, akkor a teszt sikertelen. Ha a két érték különbözik, akkor a titkos kulccsal dekódolni kell a titkos szöveget, majd a kapott értéket össze kell hasonlítani az eredeti nyílt szöveggel. Ha a két érték nem egyezik, akkor a teszt sikertelen.

KÖV_09.33:
Ha a kulcsokat csak digitális aláírás létrehozására és ellenőrzésére használják, akkor a kulcsok konzisztenciája tesztelhető egy aláírás létrehozásával és ellenőrzésével is.

4.9.3.2 Szoftver/förmver betöltési tesztek

KÖV_09.34:
Ha a modulba kívülről szoftver vagy förmver komponenst lehet betölteni, a következő szoftver/förmver teszteket kell végrehajtani.

KÖV_09.35:
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.

KÖV_09.36:
A kiszámolt eredményt össze kell hasonlítani a korábban generált eredménnyel. Ha a két kiszámolt eredmény nem egyezik, akkor a szoftver/förmver integritás teszt nem felelt meg.

4.9.3.3 Kézi kulcs bevitel tesztje

KÖV_09.37:
Amennyiben egy kriptográfiai modulba kézi úton visznek be kriptográfiai kulcsokat vagy kulcs elemeket, a következő teszteket kell végrehajtani.

KÖV_09.38:
A kulcsoknak rendelkezniük kell egy hiba detektáló kóddal (pl. paritás ellenőrzési érték), vagy pedig kétszeres beírást kell alkalmazni a beírt kulcsok helyességének ellenőrzésére.

KÖV_09.39:
EDC használata esetén az EDC-nek legalább 16 bit hosszúnak kell lennie.

KÖV_09.40:
Ha az EDC-t nem lehet ellenőrizni, vagy a kétszeres beírás nem egyezik, a teszt nem felelt meg.

4.9.3.4 Folyamatos véletlenszám generátor teszt

KÖV_09.41:
Azon kriptográfiai moduloknak, amelyek egy véletlenszám vagy pszeudó véletlenszám generátort implementálnak, tesztelniük kell a generátort a sikertelenség szempontjából egy konstans értékig.

KÖV_09.42:
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.

KÖV_09.43:
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.

4.10 Tervezési biztosíték

4.10.1 Konfiguráció kezelés

KÖV_10.01:
A modul kriptográfiai határán belül meg kell valósítani egy konfiguráció kezelő rendszert a kriptográfiai modul és a modul komponensek részére, és ezt a dokumentációban meg kell jeleníteni.

KÖV_10.02:
Minden, a konfigurációt érintő elemet, mely érinti a rendszer biztonságát és a dokumentációt, egy egyedi azonosítóval kell ellátni.

4.10.2 Továbbítás és működtetés

KÖV_10.03:
A dokumentációnak tartalmaznia kell a biztonságos telepítés, inicializálás és indítás műveleteit.

KÖV_10.04:
A dokumentációnak tartalmaznia kell a biztonság fenntartásának körülményeit a modul szétosztása és továbbítása során.

4.10.3 Fejlesztés

KÖV_10.06:
A dokumentációnak meg kell mutatnia a hardver, a szoftver és a förmver komponensek tervezése és a kriptográfiai modul biztonsági szabályzata közötti összhangot.

KÖV_10.07:
Amennyiben a modul tartalmaz szoftver vagy förmver komponenst, a dokumentációban meg kell jelennie ezek forráskódjának, világosan jelezve a tervezésnek való megfelelőségüket.

KÖV_10.08:
Ha a kriptográfiai modul tartalmaz hardver komponenseket, a dokumentációban meg kell határozni ezek sémáját és/vagy Hardver Leíró Nyelv (HDL) segítségével a komponensek listáját.

KÖV_10.10:
A dokumentációnak tartalmaznia kell olyan funkcionális specifikációt, mely informális módon leírja a modult, a külső portokat és az interfészeket, és az interfészek célját.

KÖV_10.12:
Minden szoftver és förmver komponenst magas-szintű nyelven kell megvalósítani, kivéve akkor, amikor teljesítmény vagy kivitelezési problémák miatt csak alacsony-szintű nyelv (assembly vagy mikrokód) használható.

KÖV_10.13:
Minden hardver komponenst magas-szintű specifikációs nyelvvel kell megtervezni.

4.10.4 Támogató dokumentáció

KÖV_10.21:
A kriptográfiai tisztviselő dokumentációjában le kell írni az adminisztratív funkciókat, biztonsági eseményeket, biztonsági paramétereket (és paraméter értékeket), fizikai portokat, és logikai interfészeket, amik a kriptográfiai tisztviselő számára elérhetők.

KÖV_10.22:
A kriptográfiai tisztviselő dokumentációjában le kell legyen írva, hogy hogyan lehet a kriptográfiai modult biztonságosan üzemeltetni.

KÖV_10.23:
A kriptográfiai tisztviselő dokumentációjának olyan, a felhasználók viselkedésével kapcsolatos elvárásokat is tartalmaznia kell, amik a biztonságos működéshez szükségesek.

KÖV_10.24:
A felhasználói dokumentációban meg kell határozni a Jóváhagyott biztonsági funkciókat, fizikai portokat, logikai interfészeket, melyek a felhasználó számára elérhetők.

KÖV_10.25:
A felhasználói dokumentációnak meg kell határoznia a felhasználó azon kötelességeit, melyek szükségesek a biztonságos működéshez.

5. A Luna® PCI-e modul 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® PCI-e kriptográfiai modul értékelését végző laboratórium számára.

Az alábbi jelölést alkalmazzuk:

FB_x.y.z: a FIPS 140-2 x. fejezetének y. biztonsági követelményére vonatkozó z. fejlesztői bizonyítékot meghatározó elvárása.

5.1. A kriptográfiai modul tervezése és dokumentálása

FB_01.03.01:
A fejlesztő által nyújtott biztonsági szabályzatnak tartalmaznia kell a FIPS által jóváhagyott működési mód leírását.

FB_01.03.02:
A fejlesztő által nyújtott biztonsági szabályzatnak tartalmaznia kell azokat az utasításokat, melyekkel a FIPS által jóváhagyott működési módot el lehet indítani.

FB_01.04.01:
A fejlesztő által nyújtott biztonsági szabályzatnak tartalmaznia kell annak a megoldásnak a leírását, ahogy a modul jelzi, ha FIPS által Jóváhagyott működési módban van.

FB_01.04.02:
A fejlesztő által nyújtott biztonsági szabályzatnak tartalmaznia kell, hogy a FIPS által Jóváhagyott működési mód jelzése hogyan érhető el.

FB_01.06.01:
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_01.06.02:
Minden processzor esetén a fejlesztőnek meg kell határoznia minden olyan hardvert, amelyhez a szóban forgó processzor kapcsolódik.

FB_01.08.01:
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_01.08.02:
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_01.08.03:
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_01.08.04:
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_01.08.05:
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_01.08.06:
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_01.08.07:
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_01.09.01:
Minden olyan komponenst, amely nem tartozik a biztonsági követelmények alá, tételesen fel kell sorolni a fejlesztői dokumentációban.

FB_01.09.02:
A FB_01.09.01 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_01.12.01:
A fejlesztőnek be kell mutatnia a FIPS által jóváhagyott kriptográfiai algoritmusokkal kapcsolatos tanúsítványait.

FB_01.12.02:
A fejlesztői dokumentációnak tartalmaznia kell minden FIPS által nem jóváhagyott biztonsági funkció listáját.

FB_01.13.01:
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_01.13.02:
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.

FB_01.13.03:
A blokkdiagramnak be kell mutatnia a modul fő komponensei közötti, valamint a modul és a külső berendezés közötti kapcsolatokat.

FB_01.13.04:
A blokkdiagramnak be kell mutatnia a modul kriptográfiai határát.

FB_01.14.01:
A fejlesztői dokumentációnak tartalmaznia kell a hardver, szoftver és/vagy förmver komponensek részletes specifikációját. A dokumentációban meg kell jelennie egy véges állapot modellnek a 4.4 fejezetben meghatározott feltételeknek megfelelően. Amennyiben a kapcsolat a véges állapot modell és a tervezési specifikáció között nem világos, további dokumentációt kell benyújtani, ami tisztázza a kapcsolatot.

FB_01.15.01:
A fejlesztőnek dokumentálnia kell minden biztonsággal kapcsolatos információt, mint a titkos és nyilvános kulcsok, hitelesítő adatok, és más védett információk védelme, amik kiszivárgása vagy módosítása befolyásolja a modul biztonságát.

FB_01.16.01:
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 meg kell határoznia minden fizikai portot és logikai interfészt , például:

- Fizikai portok és ezek tűkiosztásai
- Fizikai fedők, nyílások
- Logikai interfészek (pl. az API-k és más adat/vezérlő/állapot jelzések) és a jelzések nevei és funkciói
- Kézi vezérlők (gombok és kapcsolók), melyek a fizikai vezérlő bemenetre hatnak
- Fizikai állapotjelzők (pl. fényjelzések vagy kijelzők), melyek a fizikai állapot kimenetre érvényesek
- A logikai interfészek és a fizikai portok, kézi vezérlők, fizikai állapot jelzők közötti kapcsolatok
- Fizikai, logikai és elektromos karakterisztikák a fenti portokra és interfészekre

FB_02.01.02:
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.

FB_02.01.03:
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) követelményei kielégítésére készültek, valamint a logikai portokra vonatkozó 2. fejezetbeli követelményekkel.

FB_02.02.01:
A fejlesztői tervnek a modul interfészeket logikailag elkülönített kategóriákra kell szétválasztani minimálisan azon kategóriák alkalmazásával, amelyek a KÖV_02.03 és a KÖV_02.09 követelményekben definiálva vannak. Az információknak konzisztensnek kell lennie a logikai interfészek és a fizikai portok KÖV_02.01-ben foglalt specifikációjával.

FB_02.02.02:
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_02.03.02:
A fejlesztői dokumentációnak tartalmaznia kell annak bizonyítékát, hogy a következő négy logikai interfész megtalálható a modulban:

- adat input interfész (meghatározva a KÖV_02.04-ben),
- adat output interfész (meghatározva a KÖV_02.05-ben),
- vezérlési input interfész (meghatározva a KÖV_02.07-ben),
- státusz output interfész (meghatározva a KÖV_02.08-ban).

FB_02.04.01:
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_02.04.02:
A fejlesztői dokumentációban meg kell határozni minden olyan külső beviteli eszközt, mely valamilyen adat bevitelére alkalmas az adat input interfészen keresztül. Ez lehet intelligens kártya, token, biometrikus eszköz, stb.

FB_02.05.01:
A kriptográfiai modulnak rendelkeznie kell adat output interfésszel. Minden adatot (kivéve az állapotadat, mely az állapot output interfészen jelenik meg), mely feldolgozás után kikerül a modulból, az adat output interfészen keresztül kell kiadni. Ilyen adatok:

- Nyíltszövegű adat
- Titkosított adat és elektronikus aláírás
- Kriptográfiai kulcsok és más kulcskezelési adatok (nyíltan vagy kódolva)
- Vezérlőinformációk külső eszközöknek
- Bármilyen más kimenő adat

FB_02.05.02:
A fejlesztői dokumentációban meg kell határozni minden olyan külső kimeneti eszközt, mely valamilyen adat fogadására alkalmas az adat output interfészen keresztül. Ez lehet intelligens kártya, token, biometrikus eszköz, stb.

FB_02.06.01:
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_02.06.02:
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 9. fejezet (Ön-tesztek) dokumentálja, és a fejlesztői dokumentációnak tartalmaznia kell, hogy ez hogyan valósul meg.

FB_02.07.01:
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_02.07.02:
A fejlesztői dokumentációban meg kell határozni minden olyan külső beviteli eszközt, mely valamilyen parancs, jel vagy vezérlő adat bevitelére alkalmas a vezérlő input interfészen keresztül. Ez lehet intelligens kártya, token, stb.

FB_02.08.01:
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_02.08.02:
A fejlesztői dokumentációban meg kell határozni minden olyan külső kimeneti eszközt, mely valamilyen állapotinformáció, jel, logikai jelző vagy fizikai jelző fogadására alkalmas az állapot output interfészen keresztül. Ez lehet intelligens kártya, token, kijelző és/vagy tároló eszköz.

FB_02.09.01:
Ha a modul felvesz vagy szolgáltat külső áramot, rendelkeznie kell egy elektromos áram interfésszel, amely a fejlesztői dokumentációban megfelelő módon definiálva van, és amely tartalmazza az elektromos áram valamennyi belépési vagy kilépési pontját.

FB_02.10.01:
A fejlesztői dokumentációnak tartalmaznia kell annak leírását, hogy a modul hogyan tesz különbséget adat és vezérlés között az input, adat és állapot között az output interfészen, valamint hogy a bemenő adat és vezérlés útját meghatározó fizikai és logikai adatutak hogyan válnak szét a kimenő adat és állapot útját meghatározó fizikai és logikai adatutaktól.

FB_02.11.01:
A fejlesztői dokumentációnak minden fizikai és logikai input adat útvonalat megfelelő részletességgel ismertetnie kell abból a célból, hogy a modul input 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.

FB_02.12.01:
A fejlesztői dokumentációnak minden fizikai és logikai output adat útvonalat megfelelő részletességgel ismertetnie kell abból a célból, hogy a modul output információinak minden fő kategóriája specifikálva legyen. Minden output adat, amely az adat output interfészen keresztül lép ki modulból, csak az output adat útvonalon keresztül juthat ki.

FB_02.13.01:
A fejlesztői dokumentációban meg kell határozni, hogy a fizikai és logikai utak, melyeket a kimenő adatok fő kategóriái használnak, hogyan válnak le logikailag vagy fizikailag azokról a folyamatokról, melyek a kulcsgenerálást, a kézi kulcsbevitelt és a kriptográfiai kulcsok törlését végzik. A modul nem engedheti meg, hogy ezen folyamatok kulcs vagy CSP információkat adjanak ki, valamint a kimenő adatok ne zavarják meg a folyamatokat.

FB_02.14.01:
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_02.16.01:
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_02.17.01:
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 logikai interfészeknek logikailag el kell különülniük a modul összes logikai interfészétől. A fejlesztői dokumentációnak be kell mutatnia, hogy ez hogyan valósul meg.

FB_02.18.01:
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

FB_03.02.01:
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).

5.3.1 Szerepkörök

FB_03.03.01:
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 minden megkülönböztethető jogosult szerepkört, beleértve annak megnevezését, célját és azokat a szolgáltatásokat, amelyek az adott szerepkörben végrehajthatók.

FB_03.11.01:
A dokumentációnak tartalmaznia kell a modul állapotának lekérdezési módját, valamint a felhasználó által meghívható ön-tesztek inicializációját és futtatását, az FB_03.14.01 és az FB_03.15.01-ben meghatározott szolgáltatásokkal együtt.

FB_03.14.01:
A dokumentációnak tartalmaznia kell minden szolgáltatás célját és funkcióját.

FB_03.14.02:
A fejlesztői dokumentációnak meg kell határoznia minden szolgáltatáshoz kapcsolódóan az inputokat, outputokat és azon felhatalmazott szerepet vagy szerepeket, amivel végre lehet hajtani. A szolgáltatás inputoknak tartalmaznia kell a modul összes adat vagy vezérlő inputját, amin keresztül inicializálni vagy működtetni lehet azt. A szolgáltatás outputoknak tartalmaznia kell minden olyan adat és állapot

outputot, melyen keresztül az inputon keresztül kezdeményezett szolgáltatások, eredményét le lehet kérni.

FB_03.15.01:
A dokumentációnak tartalmaznia kell minden szolgáltatás célját és funkcióját.

FB_03.15.02:
A fejlesztői dokumentációnak meg kell határoznia minden szolgáltatásra az inputokat és a hozzájuk tartozó outputokat. A szolgáltatás inputoknak tartalmaznia kell minden adat vagy vezérlő inputot, melyen keresztül a szolgáltatások inicializálhatók vagy működtethetőek. A szolgáltatás outputoknak tartalmaznia kell minden olyan adat és állapot outputot, melyen keresztül az input által kezdeményezett szolgáltatás eredménye lekérdezhető.

5.3.3 Operátori hitelesítés

FB_03.19.01:
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_03.20.01:
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_03.21.01:
A fejlesztői dokumentációnak ismertetnie kell, hogy egy áramellátás megszűnését követően a megelőző hitelesítések eredményei hogyan lesznek törölve.

FB_03.22.01:
A dokumentációnak tartalmaznia kell minden olyan védelmi eljárást, amit a modul a hitelesítő adatok védelmére felhasznál. A védelemnek olyan eljárásokat kell tartalmaznia, melyek védenek az illetéktelen hozzáféréstől, módosítástól és helyettesítéstől.

FB_03.23.01:
A fejlesztői dokumentációnak tartalmaznia kell azon eljárásokat, melyek a modulhoz való hozzáférést szabályozzák az inicializálás előtt.

FB_03.25.01:
A dokumentációban meg kell jelennie minden egyes hitelesítési módnak, valamint az elfogadható hibás engedélyezés és a véletlen kitalálás arányoknak.

FB_03.26.01:
A fejlesztői dokumentációban megtalálható minden hitelesítési mód, valamint ezek megfejtésének valószínűsége egy perc alatt.

FB_03.27.01:
A dokumentáció leírja, hogy hogyan lehet megakadályozni a hitelesítő adatok operátor általi kifigyelését.

FB_03.28.01:
A dokumentációban meg kell jelennie egy olyan eljárásnak, mely biztosítja az operátor által bevitt hitelesítő adatok visszajelzését.

5.4 Véges állapotú automata modell

FB_04.05.01:
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.

5.5 Fizikai biztonság

5.5.1 Közös követelmények

FB_05.04.01:
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[18]. A specifikált fizikai megvalósításnak konzisztensnek kell lennie az aktuális modul fizikai tervével.

FB_05.05.01:
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.

FB_05.12.01:
A több chipes, beágyazott modul chipjeinek szabványos termék minőségű IC-knek kell lenniük, amelyeket úgy terveztek, hogy legalább a tipikus kereskedelmi minőségi specifikációknak feleljenek meg az áramellátás, hőmérséklet, megbízhatóság, ütés/rázkódás stb. tekintetében. Különösen fontos, hogy a modul standard passziválási technikát alkalmazzon minden egyes chipre vonatkozóan. A fejlesztői dokumentációnak ismertetnie kell az IC-k minőségét. Ha valamelyik alkalmazott IC nem szabványos, annak passziválási szerkezetét szintén ismertetni kell.

5.5.2 Több chipes, beágyazott kriptográfiai modulra vonatkozó követelmények

FB_05.34.01:
A modult tipikus termék szintű foglalatba vagy tokba kell beépíteni. A fejlesztői dokumentációnak ismertetnie kell a modulnak foglalat vagy tok leírását.

FB_05.36.01:
A modult egy nem átlátszó, beavatkozást kimutató burkolattal kell befedni, mint pl. egy, az alakot követő burkolat, vagy folyékony festék. Az anyagnak átlátszatlannak kell lennie a látható tartományon belül. A fejlesztői dokumentációnak meg kell adnia a beavatkozást kimutató, nem átlátszó burkolat fajtáját és annak karakterisztikáját.

5.6. Az operációs rendszer biztonsága

Nincsenek követelmények[19].

[18] A Luna® PCI-e kriptográfiai modul esetében ez: több chipes, beágyazott modul.
[19] Mivel a Luna® PCI-e kriptográfiai modul működési környezete nem képezi az értékelés részét.

5.7. Kriptográfiai kulcsgondozás

5.7.1 Általános követelmények

FB_07.01.01:
A fejlesztői dokumentációnak ismertetnie kell minden, a modul számára belső titkos és/vagy magán kulcs védelmét. A védelemnek tartalmaznia kell olyan mechanizmusok implementálását, amelyek védelmet nyújtanak a jogosulatlan felfedéssel, módosítással és helyettesítéssel szemben.

FB_07.02.01:
Ha a modul támogat nyilvános kulcsokat, a fejlesztői dokumentációnak ismertetnie kell minden nyilvános kulcs védelmét. A védelemnek tartalmaznia kell olyan mechanizmusok implementálását, amelyek védelmet nyújtanak a jogosulatlan módosítással és helyettesítéssel szemben.

FB_07.03.01:
A dokumentációnak ismertetnie kell a kriptográfiai kulcsok, kulcs komponensek és CSP-k listáját.

5.7.2 Véletlenszám generátorok (RNG)

FB_07.08.01:
A fejlesztői dokumentációban szerepelnie kell egy állításnak, miszerint a kulcsgenerálás során FIPS által jóváhagyott véletlenszám generálás történik. Az erre vonatkozó követelmények a FIPS PUB 140-2 C mellékletében találhatók.

FB_07.09.01:
A fejlesztői dokumentációnak tartalmaznia kell egy olyan eljárást, ami biztosítja, hogy a mag és a kezdeti kulcs sosem egyezik meg.

FB_07.10.01:
A fejlesztői dokumentációban le kell írni az összes felhasznált RNG-t (akár FIPS által jóváhagyott, akár nem), ezek típusát és felhasználását a modulban.

5.7.3 Kulcs generálásra vonatkozó követelmények

FB_07.11.01:
A fejlesztőnek bizonyítékot is kell nyújtania arra vonatkozóan, hogy a kulcs generálási algoritmus FIPS által jóváhagyott.

FB_07.13.01:
A fejlesztőnek olyan dokumentumot kell benyújtania, ami megmutatja, legalább hány művelet szükséges ahhoz, hogy a generált kulcs értékét ki lehessen találni a kulcsgeneráló algoritmust kihasználva (pl. a kezdeti kulcsot kitalálva determinisztikussá tenni az RNG-t).

FB_07.15.01:
A dokumentációnak jeleznie kell, hogy a kulcsgenerálás során valamilyen átmeneti érték elhagyja-e a modult.

FB_07.15.02:
A kulcs generálási eljárások nem tehetnek lehetővé semmilyen outputot a kulcs generálási folyamat során, kivéve azokat az értékeket, amelyek kódolva vannak.

FB_07.16.01:
A dokumentációnak bizonyítékot kell szolgáltatnia arról, hogy a kulcsgenerálási eljárást a modul használja.

5.7.4 Kulcs szétosztásra vonatkozó követelmények

FB_07.17.01:
A dokumentációban a fejlesztőnek nyilvánosságra kell hoznia, hogy FIPS által jóváhagyott kulcsgondozási eljárást használ. A jóváhagyott kulcsgondozási eljárások a FIPS PUB 140-2 D mellékletében találhatók.

FB_07.19.01:
A fejlesztőnek olyan dokumentumot kell benyújtania, ami megmutatja, legalább hány művelet szükséges ahhoz, hogy a kriptográfiai kulcs értékét ki lehessen találni a kulcs továbbítása során.

FB_07.21.01:
A dokumentációnak tartalmaznia kell a modul által felhasznált kulcsszétosztási eljárásokat.

5.7.5 Kulcs bevitelére és kivitelére vonatkozó követelmények

FB_07.23.01:
A kulcsmenedzsment dokumentációnak tartalmaznia kell a kezdeti kulcs bevitelének módját.

FB_07.24.01:
A dokumentációban meg kell jelennie, hogy a magán és titkos kulcsokat, melyeket a modulba betöltenek vagy kivesznek, milyen FIPS által jóváhagyott algoritmusokkal titkosítják.

FB_07.25.01:
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_07.27.01:
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_07.28.01:
A fejlesztői dokumentációnak meg kell határoznia a modul által használt kulcsbeviteli és kivételi eljárásokat.

FB_07.32.01:
A fejlesztői dokumentációban meg kell határozni azt a modul által használt eljárást, amivel a kulcsbevitelért illetve kivételért felelős operátorokat külön-külön lehet azonosítani.

FB_07.34.01:
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 hány kulcs komponens szükséges a kulcs újragenerálásához.

FB_07.35.01:
A dokumentációnak le kell írnia, hogy n-1 kulcs komponens ismerete nem elegendő semmilyen, a kulccsal kapcsolatos információ felfedésére, kivéve a kulcs hosszát.

FB_07.36.01:
A fejlesztő által kiadott dokumentációban szerepelnie kell annak az állításnak, hogy a modul osztott tudáson alapuló eljárásokat használ.

5.7.6 Kulcs tárolásra vonatkozó követelmények

FB_07.39.01:
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.

FB_07.40.01:
A fejlesztői dokumentációnak tartalmaznia kell a következő információt minden tárolt kulcsról:

- Típus és azonosító
- Tárolás helye
- A formátum, ahogy a kulcsot tárolják (nyílt szöveg, titkosított forma, osztott tudáson alapuló védelem). Amennyiben a kulcsot titkosított formában tárolják, meg kell határozni, hogy milyen FIPS által jóváhagyott algoritmus védi azt.

5.7.7 Kulcs megsemmisítésre vonatkozó követelmények

FB_07.41.01:
A fejlesztői dokumentációnak meg kell határozni a nyílt szövegű titkos és magán kulcsok valamint a CSP-k megsemmisítésével kapcsolatos információkat:

- Megsemmisítési technika
- Megkötések a nyílt szövegű titkos és magán kulcsok és a CSP-k megsemmisítésénél
- Nyílt szövegű titkos és magán kulcsok és a CSP-k, melyek megsemmisülnek
- Nyílt szövegű titkos és magán kulcsok és a CSP-k, melyek nem semmisülnek meg és ennek magyarázata
- Annak magyarázata, hogy a megsemmisítési eljárás annyi idő alatt megy végbe, amennyi nem elég a nyílt szövegű titkos és magán kulcsok és a CSP-k felfedésére

5.8 Elektromágneses interferencia, elektromágneses kompatibilitás

FB_08.02.01:
A fejlesztőnek meg kell neveznie azon FCC által akkreditált laboratóriumot, mely a tanúsítványát kiállította.

FB_08.02.02:
A fejlesztőnek be kell nyújtani a kriptográfiai modul FCC tanúsítványának számát.

FB_08.05.01:
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 B alrészben és B osztályban vannak megadva.

5.9 Ön-tesztek

5.9.1 Általános követelmények

FB_09.04.01:
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_09.05.01:
Lásd az FB_02.06.01-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_09.06.01:
Lásd az FB_02.06.01-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_09.07.01:
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_09.07.02:
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.

5.9.2 Az áram alá helyezési tesztek

5.9.2.1 Általános tesztek

FB_09.09.01:
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_09.10.01:
A fejlesztőnek dokumentálnia kell azt a jelzést, amelyet a modul kiad az áram alá helyezés után végrehajtandó tesztek sikeres végrehajtása esetén.

FB_09.12.01:
A fejlesztőnek ismertetnie kell azokat az eljárásokat, amelyek segítségével egy operátor elindíthatja az áram alá helyezéskor elvégzendő ön-teszteket.

FB_09.13.01:
Lásd az FB_09.07.01-t a fejlesztői dokumentációra vonatkozó követelményeket illetően.

5.9.2.2 Kriptográfiai algoritmus tesztek

FB_09.16.01:
Lásd az FB_09.07.01-t a fejlesztői dokumentációra vonatkozó követelményeket illetően.

FB_09.17.01:
A fejlesztőnek dokumentálnia kell az "ismert eredmény" tesztet, amelyet a kriptográfiai algoritmus tesztelésére végre kell hajtani.

FB_09.17.02:
A dokumentációban be kell mutatni azt, hogy amennyiben a két kimenet nem azonos, a modul hogyan megy át hibaállapotba, illetve milyen hibajelzés jelenik meg a kimenetén.

FB_09.18.01:
Lásd az FB_09.07.01-t a fejlesztői dokumentációra vonatkozó követelményeket illetően.

FB_09.18.02:
A fejlesztői dokumentációban meg kell határozni azokat a teszteket, amiket a modul felhasznál.

FB_09.19.01:
Lásd az FB_09.07.01-t a fejlesztői dokumentációra vonatkozó követelményeket illetően.

FB_09.19.02:
A fejlesztői dokumentációban meg kell határozni azokat a teszteket, amiket a modul felhasznál.

FB_09.20.01:
Lásd az FB_09.07.01-t a fejlesztői dokumentációra vonatkozó követelményeket illetően.

FB_09.20.02:
A fejlesztőnek meg kell határoznia, hogy ismert eredmény tesztet vagy két független kriptográfiai algoritmus megvalósítás kimenetének összehasonlító tesztjét alkalmazta a modul algoritmusainak tesztelésére. Amennyiben az összehasonlító tesztelést használja, ezt ki kell emelni a dokumentációban.

5.9.2.3 Szoftver/förmver teszt

FB_09.22.01:
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.

FB_09.22.02:
A dokumentációnak ismertetnie kell az implementált sértetlenséget vizsgáló mechanizmust.

FB_09.22.03:
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. Egy ilyen bizonylat hiányában a fejlesztő cégnek írásos nyilatkozatot kell szolgáltatnia, amely kijelenti, hogy a modulban implementált hitelesítési technika FIPS által jóváhagyott.

5.9.2.4 Kritikus funkciók tesztjei

FB_09.27.01:
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.

5.9.3 Feltételhez kötött tesztek

5.9.3.1 Páronkénti konzisztencia teszt

FB_09.31.01:
Ha a modul nyilvános és magán kulcsokat használ FIPS által jóváhagyott kulcstovábbítási eljárásokra, a fejlesztői dokumentációnak ismertetnie kell egy páronkénti konzisztencia tesztet, amely a nyilvános kulcsot használja fel egy nyílt szöveg titkosítására. Az eredményül kapott kódolt szöveget össze kell hasonlítani az eredeti nyílt szöveggel, hogy különböznek-e.

- Ha a két érték egyenlő, a modult hibaállapotba kell rakni, az állapot interfészen egy hibajelzésnek kell megjelennie.
- Ha a két érték különbözik, a titkos kulcsot használva vissza kell fejteni a kódolt szöveget, majd az eredményt össze kell hasonlítani az eredeti nyílt szöveggel.
- Ha a két érték nem azonos, a teszt nem felelt meg.

FB_09.33.01:
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.

*5.9.3.2 Szoftver/förmver betöltési teszte*k

FB_09.35.01:
A fejlesztői dokumentációnak ismertetnie kell a FIPS által jóváhagyott hitelesítési technikát, amelyet a kívülről betöltött szoftver és förmver sértetlenségének védelmére alkalmaznak.

FB_09.35.02:
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.

5.9.3.3 Kézi kulcs bevitel tesztje

FB_09.40.01:
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

FB_09.40.02:
Ha a hiba detektáló kódot alkalmazzák, a fejlesztői dokumentáció azon részének, amely a kriptográfiai kulcsok formátumát ismerteti (lásd KÖV_07.03), tartalmaznia kell a hiba detektáló kódra vonatkozó részt is.

5.9.3.4 Folyamatos véletlenszám generátor teszt

FB_09.42.01:
Ha a modul hardver véletlenszám generátort implementál, a fejlesztőnek dokumentálnia kell a folyamatos véletlenszám generátor tesztet.

FB_09.43.01:
Ha a modul hardver véletlenszám generátort implementál, a fejlesztőnek dokumentálnia kell a folyamatos véletlenszám generátor tesztet.

5.10 Tervezési biztosíték

5.10.1 Konfiguráció kezelés

FB_10.01.01:
A fejlesztői dokumentációnak tartalmaznia kell a kriptográfiai modul, a modul komponensek és a modul dokumentáció által használt konfiguráció kezelési rendszer leírását.

FB_10.02.01:
A fejlesztő konfiguráció kezelési dokumentációjának tartalmaznia kell a konfigurációs elemek listáját, és azokat az eljárásokat, amik ezek egyedi megkülönböztetésére szolgálnak.

FB_10.02.02:
A fejlesztői dokumentációnak tartalmaznia kell azon eljárást, mely minden hitelesített konfigurációs elem verzióját egyedileg azonosítja.

5.10.2 Továbbítás és működtetés

FB_10.03.01:
A fejlesztői dokumentációnak tartalmaznia kell azokat a lépéseket, melyek a modul biztonságos telepítéséhez, inicializációjához és indításához szükségesek

FB_10.04.01:
A szállítási dokumentációnak tartalmaznia kell azon eljárásokat, melyek a kriptográfiai modul felhatalmazott operátornak való átadása közbeni biztonságának fenntartásához szükségesek.

5.10.3 Fejlesztés

FB_10.06.01:
A fejlesztői dokumentációnak tartalmaznia kell annak leírását, hogy a hardver, szoftver és förmver tervezése során hogyan tartották be a modul biztonsági szabályzatának előírásait.

FB_10.07.01:
A fejlesztőnek be kell nyújtania egy listát a modulban felhasznált összes szoftver és förmver komponensről.

FB_10.07.02:
A fejlesztőnek egy megjegyzésekkel ellátott forrás listát kell beadnia a listában felhasznált összes szoftver és förmver és komponensről.

FB_10.08.01:
A fejlesztőnek a modulban található összes hardver elemről készített listát kell készítenie.

FB_10.10.01:
A fejlesztő funkcionális specifikációjának le kell írnia a kriptográfiai modult annak minden külső interfészével és portjával.

FB_10.10.02:
A fejlesztő funkcionális specifikációjának meg kell határoznia minden külső interfész célját.

FB_10.12.01:
A fejlesztőnek azonosítania kell minden szoftver és szoftver komponenst, ami nem magas-szintű nyelven lett írva, és magyarázatot vagy indoklást kell szolgáltatni arról, hogy miért alacsony-szintű nyelven készültek. A magyarázat hivatkozhat a magas-szintű nyelv hiányára vagy a szoftver/förmver teljesítménynövelésének igényére.

FB_10.13.01:
A fejlesztőnek olyan dokumentációt kell készítenie, mely a felhasznált hardver komponenseket magas-szintű nyelven írja le.

5.10.4 Támogató dokumentáció

FB_10.23.01:
A fejlesztői dokumentációnak minden olyan információt tartalmaznia kell, mely a KÖV_10.21-ben, a KÖV_10.22-ben és a KÖV_10.23-ban megjelennek.

FB_10.23.02:
A kriptográfiai tisztviselő dokumentációjának rendelkezésre kell állnia a kriptográfiai tisztviselő számára.

FB_10.25.01:
A fejlesztői dokumentációnak minden olyan információt tartalmaznia kell, mely a KÖV_10.24-ben és a KÖV_10.25-ban megjelennek.

FB_10.25.02:
A felhasználói dokumentációnak rendelkezésre kell állnia a felhasználó számára.

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 a 3-as biztonsági szintű FIPS 140-2 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:

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

[KM1.2]
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][20].

[KM1.3]
A kriptográfiai modul a minősített tanúsítvány aláíró kulcsokat csak kettős ellenőrzés alatt állíthatja elő[21].

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

[KM1.5]
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 [22].

[20] 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.
[21] Megjegyzés: A kettős ellenőrzési követelmény teljesíthető akár közvetlenül a kriptográfiai modul által, akár úgy, hogy a hitelesítés-szolgáltató kettős személyi ellenőrzést alkalmaz.
[22] Lásd [KM1.2] alatti megjegyzést.

[KM1.6]

A rendszervezérlési kulcsokat biztonságos kriptográfiai modulban kell előállítani.

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

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

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

[KM6.4]
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]
Egy minősített tanúsítvány aláírásához használt kulcsot csak minősített tanúsítványok és opcionálisan a kapcsolódó visszavonási státusz adatok aláírására szabad használni.

[CG1.6]
A megbízható rendszer által kibocsátott minősített tanúsítványnak meg kell felelnie a Törvény 2. mellékletében meghatározott követelményeknek.

6.2 Időbélyegzés szolgáltatásra vonatkozó követelmények

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

[TS4.2]
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[23]

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

[23] Lásd a [KM1.2] alatti megjegyzést.

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

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

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

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

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

[SP1.4]
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][24].

[SP1.5]
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.

[24] Lásd a [KM1.2] alatti megjegyzést.

7 A Luna® PCI-e kriptográfiai modul sebezhetőség vizsgálata

A Luna® PCI-e kriptográfiai modul vizsgálata kiterjedt a nyilvános adatbázisokban fellelhető sebezhetőségek ellenőrzésére.

A vizsgálat az alábbi nyilvános sebezhetőség adatbázisokra tért ki:

- National Vulnerability Database http://nvd.nist.gov/
- Security Focus http://www.securityfocus.com

Az ellenőrzés eredménye, hogy a Luna® PCI-e *Hardware verzió: VBD-05-0100, VBD-05-0101 és VBD-05-0103; Firmware verzió: 6.2.1* kriptográfiai modulról nyilvános adatbázisban fellelhető sebezhetőség jelen tanúsítás időpontjában nem található.

8. A Tanúsítási jelentés eredménye, érvényességi feltételei

8.1 A Tanúsítási jelentés eredménye

Luna® PCI-e

Hardware verzió: VBD-05-0100, VBD-05-0101 és VBD-05-0103;

Firmware verzió: 6.2.1

a Tanúsítás érvényességi feltételeinek[25] 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[26] aláírására történő felhasználására.

Aláírás-létrehozó eszközön az aláírás-létrehozó adat elhelyezése szolgáltatás keretén belül:

Az előfizetői (aláírói) kulcspár generálására[27].

[25] Lásd a 8.2 "Az eredmények érvényességi feltételei" fejezet feltételeit.
[26] Mely időbélyegzőt a 2001 évi XXXV. törvény az elektronikus aláírásról minősített időbélyegzőként említi.
[27] Amennyiben a kulcspár előállítása az aláírás-létrehozó eszközön kívül történik.

8.2 Az eredmények érvényességi feltételei

A Luna® PCI-e kriptográfiai 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.

A FIPS 140-2-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® PCI-e kriptográfiai 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.

8.2.1 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® PCI-e kriptográfiai modul szolgáltatásait igénybe vevő különböző munkaköröket (Security Officer, Crypto Officer, Crypto User) betöltő személyek:

- kompetensek, jól képzettek és megbízhatóak, valamint
- betartják a különböző útmutatók által leírt, kötelező tevékenységeket.

2. A modult csak megfelelően biztonságos operációs rendszerrel és alkalmazói programokkal üzemeltetett, és megfelelő interfésszel ellátott számítógépbe helyezhető.

3. A kriptográfiai modulhoz való fizikai hozzáférést és a kommunikációs kapcsolatokat felügyelet alatt kell tartani.

8.2.2 A FIPS 140-2 megfelelőségből fakadó érvényességi feltételek

Az alábbi feltételek ahhoz elengedhetetlenek, hogy a Luna® PCI-e kriptográfiai modul megfeleljen a FIPS 140-2 3-as biztonsági szintjének.

4. A FIPS-jóváhagyott módban történő működéshez az alábbi szabálybeállítások szükségesek:

- „Nem FIPS algoritmusok rendelkezésre állnak” lehetőséget le kell tiltani.
- „Hitelesítés megbízható útvonallal” lehetőséget be kell kapcsolni és modult a PED használatával kell inicializálni az SO hitelesítési adatainak megadásához.
- „Kérdés (challenge) nélküli megbízható útvonal művelet” lehetőséget le kell tiltani, ha az aktiválás vagy automatikus aktiválás be van kapcsolva.
- A „Sikertelen kérdés-válasz (challenge-response) validálások számlálása” lehetőséget engedélyezni kell, ha az aktiválás vagy automatikus aktiválás be van kapcsolva.
- Raw RSA műveleteket csak kulcs átvitelre szabad használni FIPS üzemmódban.

8.2.3 A minősített hitelesítés-szolgáltatáshoz történő használhatóság kiegészítő feltételei

Egy minősített hitelesítés-szolgáltatónak a Luna® PCI-e kriptográfiai modul felhasználása során az alábbi kiegészítő feltételeket is be kell tartania:

5. RSA aláírási algoritmus használata esetén a minimális modulus hosszúság (`MinModLen`): 2048 bit legyen.

6. DSA aláírási algoritmus használata esetén a minimális p prímhosszúság (`pMinLen`) 2048 bit, a minimális q prímhosszúság (`qMinLen`) 224 bit legyen.

7. Az ECDSA aláírási algoritmus használata esetén a következő paraméter feltételek teljesítése szükséges: `qMinLEN=256` SHA256 használata mellett, továbbá `r0Min` nagyobb mint 10^4 és `MinClass` legalább `200`, ahol a paraméterek jelölése megfelel az ETSI TS 102 176-1 v 2.1.1 –ben leírtaknak.

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

9. Csak az ETSI TS 102 167-1 érvényes verziójában használhatónak minősített lenyomatoló algoritmust szabad használni.

10. A minősített tanúsítvány (QC) aláírásához használt kulcsot csak minősített tanúsítványok és opcionálisan a kapcsolódó visszavonási státusz adatok (beleértve az azok ellenőrzésére szolgáló tanúsítványt) aláírására szabad használni.

11. 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, 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 vagy AES 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.

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

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

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

15. A Tanúsítvány csak a 8.1 fejezetben megadott hardver és förmver verzióra érvényes. Új förmver verzióra való frissítés 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 NMHH biztonságos elektronikus aláírási termék nyilvántartásába.

8.2.4 Egyéb, az érvényességet befolyásoló megjegyzések

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

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

9. A tanúsításhoz figyelembe vett dokumentumok

9.1 Termék megfelelőségi követelményeket tartalmazó dokumentumok

Az Európai Parlament és a Tanács 910/2014/EU rendelete (2014. július 23.) a belső piacon történő elektronikus tranzakciókhoz kapcsolódó elektronikus azonosításról és bizalmi szolgáltatásokról

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

FIPS 140-2: Security Requirements for Cryptographic Modules

Derived Test Requirements for FIPS 140-2

ETSI TS 102 176-1 V2.1.1 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

9.2 A tanúsítási jelentéshez figyelembe vett egyéb dokumentumok

Kérelem /a tanúsítás elvégzésére/

FIPS 140-2 Consolidated Validation Certificate No. 0015, Certificate number:1694

LEVEL 3 NON-PROPRIETARY SECURITY POLICY FOR Luna® PCI-e Cryptographic Module /DOCUMENT NUMBER: CR-3397 Revision 8 April 27, 2012/

10. Rövidítések

AES	Advenced Encryption Standard
ANSI	American National Standards Institute
API	Application Programming Interface
CA	Certification Authority
CC	Common Criteria
CEN	European Comittee for Standardization
CMCKG	Cryptographic Module for CSP Key Generation Services
CMCSO	Cryptographic Module for CSP Signing Operations
CRC	Cyclic Redundancy Check
CRT	Chinese Remainder Theorem
CSP	Critical Security Parameter
DAC	Data Authentication Code
DES	Data Encryption Standard /FIPS PUB 46-3, FIPS PUB 74, FIPS PUB 81/
DSA	Digital Signature Algorithm /FIPS PUB 186-2/
ECC	Elliptic Curve Cryptography
EDC	Error Detecting Code
EMI	Electromagnetic Interference
EMC	Electromagnetic Compability
ETSI	European Telecommunication Standards Institute
FCC	Federal Communications Commission
FIPS	Federal Information Processing Standards Publications
FIPS 140-2	Security Requirements for Cryptographic Modules
HA	High Availability
HMAC	Hashed (Keyed) Message Authentication Code
HSM	Hardware Security Module
ITSEC	Information Technology Security Evaluation Criteria
KAT	Known Answer Test
MAC	Message Authentication Code
MD2	Message Digest Algorithm 2
MD5	Message Digest Algorithm 5
NIST	National Institute of Standards and Technology
PCI	Peripheral Component Interconnection
PCI-e	Peripheral Component Interconnection-express
PED	PIN Entry Device
PIN	Personal Identification Number
PKCS	Public Key Cryptographic Standards
PKCS #11	Cryptographic Token Interface Standard
PP	Protection Profile
PRNG	Pseudo Random Number Generator
RA	Registration Authority
RC2	Rivest’s Code 2
RC4	Rivest’s Code 4
RNG	Random Number Generator
RSA	Rivest-Shamir-Adleman (public key cryptosystem) /ANSI X9.31/
SFF	Short-Form Factor
SHA-1	Secure Hash Algorithm /FIPS PUB 180-1/
SO	Security Officer
SSCD-PP	Secure Signature Creation Device – Protection Profile
Triple DES	/FIPS PUB 46-3, ANSI X9.52/
TS	Technical Specification
TVK	Token or Module Variable Key