FELÜLVIZSGÁLATI JEGYZŐKÖNYV
(E-SI04F1-TANF) MELLÉKLETE

Dokumentumazonosító:	**TANF.ME-01**	
Projektazonosító:	**E-SI04F1**	**Siemens Rt 2004**
MATRIX tanúsítási igazgató:	**Dr. Szőke Sándor**	
Kelt:	Budapest, 2004. október 12.	
	……. MATRIX tanúsítási igazgató	

1. A FELÜLVIZSGÁLAT KÖRÜLMÉNYEI

Az elvégzett felülvizsgálat, illetve az ez alapján kiállított Felülvizsgálati Jegyzőkönyv a T-Systems ISS GmbH (Németország)

T-Systems.02085.TE.09.2002 sorszámú tanúsításán és
T-Systems-DSZ-ITSEC-04084-2002 sorszámú vizsgálati jegyzőkönyvén

valamint a MátrixATRIX Kft. (Magyarország)

E-SI03T-TAN sorszámú tanúsításán,
E-SI03T-TAN.ME-01 sorszámú tanúsítási mellékletén
és a tanúsítás során létrehozott nem publikus vizsgálati anyagain

alapul.

A német vizsgálat a német vizsgálati eljárás alapján igazolta a termék megfelelését az alábbi normatív dokumentumokban foglalt követelményeknek:

SigG Gesetz über Rahmenbedingungen für elektronische Signaturen und zur Änderung weiterer Vorschriften (Signaturgesetz – SigG) [Német elektronikus aláírás törvény] vom 16. May, 2001
SigV Verordnung zur elektronischen Signatur (Signaturverordnung – SigV) [Elektronikus aláírás törvény végrehajtási utasítás] vom 16. November 2001.
DIN V 66291-1 Chipcards with digital signatur application/function according to SigG and SigV - Part 1: Application interface

A német tanúsítás során felhasználták az SLE66CX322P mikrochip alábbi tanúsítását:

BSI-DSZ-CC-0169-2002 Smart Card IC (Security Controller) SLE66CX322P with RSA 2048 / m1484a23 7 May 2002

A német tanúsítás honosítása során tételesen megvizsgáltuk, hogy a magyar

előírások mennyiben felelnek meg a vizsgálat alapját képező fenti normatíváknak, illetve általánosan elfogadott európai biztonsági követelményeknek és ajánlásoknak. A vizsgálat során megállapítottuk, hogy a német és a magyar szabályozás lényegi előírásai megfelelnek egymásnak, az eltéréseknél a rendelkezésre álló dokumentáció alapján megvizsgáltuk a magyar jog által előírt feltételek teljesülését. A honosításhoz rendelkezésünkre állt az eredeti vizsgálat során felhasznált valamennyi dokumentum illetve eszköz.

A felülvizsgálat során megvizsgáltuk, hogy az eredeti tanúsítás érvényességét illetve feltételeit megváltoztatták-e a tanúsítás kiadása óta eltelt időszakban megjelent

- magyar normatívák,
- a német tanúsítás kiegészítései,
- a felhasznált algoritmusokat érintő felfedezések, szabályozások.

A felülvizsgálat mellékletét az eredeti tanúsítás mellékletével egységes formába foglalva jelentetjük meg. A Felülvizsgálati Jegyzőkönyv kiadásával az eredeti Tanúsítvány Melléklete (**E-SI03T-TAN.ME-01**) hatályát veszti.

2. A VIZSGÁLAT TÁRGYA

2.1. A tanúsításhoz a megrendelő által átadott eszközök és dokumentációk

Az eszköz megnevezése: “SLE66CX322P mikrochipből, OS/M4.01A operációs rendszerből és elektronikus aláírás létrehozó alkalmazásból álló intelligens kártya”.

Típus	Tárgy	Verzió	Dátum	Adat-hordozó
Hardver	Controller Infineon SLE66CX322P (Chip Identifier 6C, Produktion Line Number 2)	-	-	Chip-kártya
Szoftver (Operációs rendszer)	CardOS M4.01A	C804	2003.11.25.	ROM/ EEPROM
Megszemélyesítő programok: Applikáció/Adatstruktúra	PersAppsigG.csf VorPersAppsigG.csf NachPersAppsigG.csf	2.10 2.10 2.10	2002.07.29.	Papír
Megszemélyesítő program	StartKey_0 to StartKey_1.csf	A kártyát kibocsátó Hitelesítés Szolgáltatóval egyeztetendő egyedi programok		Papír
Megszemélyesítő program	M401a_Service Pack_SigG.csf	5.0	2002.07.26.	Papír
Dokumentáció	CardOS/M4.01 Application SigG	1.0	2001.10.04.	Papír
Dokumentáció	CardOS/M4.01A Application SigG	2.0	2002.06.19.	Papír
Dokumentáció	CardOS/M4.0 User’s Manual	1.0	2001.10. hó	Papír
Dokumentáció	CardOS/M4 User’s Manual - correction	2.0	2002.06. hó	Papír

	sheet			
Dokumentáció	CardOS/M4.01 Card Holder Manual	1.02	2002.02.27.	Papír
Dokumentáció	CardOS/M4.01A Card Holder Manual	2.1	2002.07.08.	Papír
Dokumentáció	CardOS/M4.01 Terminal Developer Manual	1.12	2002.02.27.	Papír
Dokumentáció	CardOS/M4.01A Terminal Developer Manual	2.0	2002.06.17.	Papír
Dokumentáció	CardOS/M4.01 Documentation for theTrust Center	1.02	2002.02.27.	Papír
Dokumentáció	CardOS/M4.01A Documentation for theTrust Center	2.0	2002.06.17.	Papír
Dokumentáció	CardOS/M4.01 Delivery Generation Configuration	1.1	2001.12.18.	Papír
Dokumentáció	CardOS/M4.01A Delivery Generation Configuration	2.0	2002.06.17.	Papír
Dokumentáció	T-Systems.02085.TE.09.2002 Tanúsítvány		2002.10.01.	CD
Dokumentáció	T-Systems-DSZ-ITSEC-04084-2002 Vizsgálati jegyzőkönyv		2002.09.24.	CD
Dokumentáció	BSI-DSZ-CC-0169-2002. Smart Card IC (Security Controller) SLE66CX322P with RSA 2048 / m1484a23 Tanúsítvány és tanúsítási jelentés		2002.05.07.	CD
Dokumentáció	Security Target, SLE66CX322P with RSA2048 /m1484		2002.05.06.	CD
Dokumentáció	Anhang Nr. 1 vom 30.04.2004 zum Zertifizierungsreport T-Systems-DSZ-ITSEC-04084-2002 vom 24.09.2002		2004.04.30	CD

Szállító:

Siemens AG
ICN EN TNA
Charles de Gaulle-Straße 2-4
D-81737 Munich, Germany

Tanúsítás megrendelője:

Siemens Rt.
1143 Budapest
Gizella út 51-57.

3. FUNKCIONÁLIS LEÍRÁS

A tanúsított intelligens kártya egy elektronikus aláírást létrehozó eszköz, melynek fő komponensei:

- Infineon SLE66CX322P vezérlő mikrochip,
- CardOS/M4.01A operációs rendszer elektronikus aláírás alkalmazással.

A **CardOS/M4.01A** egy aktív és passzív adatvédelmet egyaránt támogató multifunkcionális intelligens kártya operációs rendszer, melynek kifejlesztése a legmagasabb biztonsági követelményeknek megfelelően történt.

A CardOS/M4.01A az Infineon SLE66CX322P mikrochipre épül, amely az asszimetrikus kriptográfiához és a valódi véletlenszám-generátorhoz biztosít beépített biztonsági vezérlőt.

Bármely arra feljogosított hitelesítés szolgáltatónál (HSZ) végzett **megszemélyesítés** során az elektronikus aláíráshoz szükséges kulcspár az intelligens kártyán generálódik és a DF SigG[1]-ben tárolódik. A **nyilvános** kulcsot a HSZ kiolvassa és felhasználja a kártyabirtokos tanúsítványának létrehozásához.. A **magánkulcs nem** olvasható ki. Az aláírás PIN-jével történő hitelesítést követően a kártyabirtokos a **magánkulcs** segítségével **egyetlen minősített elektronikus aláírást** hozhat létre.

Az elektronikus aláírás alkalmazást kizárólag elektronikus aláírások létrehozására fejlesztették ki.

A kártyán lévő elektronikus aláírás létrehozó alkalmazás mellé tetszőleges további alkalmazást lehet telepíteni a kártyán, amelyek kihasználhatják az operációs rendszer tulajdonságait.

A CardOS/M4.01A az alábbi fő tulajdonságokkal bír:

- védelem az eddig ismert valamennyi biztonsági támadás ellen,
- az összes parancs megfelel az ISO 7816-4, -8 és -9 szabványoknak
- PC/SC és CT-API megfelelőség,
- letisztult struktúrájú biztonsági felépítés és bevizsgált kulcs menedzselés.
- A kártya szolgáltatások és parancsok felhasználó- és alkalmazásfüggő konfigurálhatósága
- Az operációs rendszer kibővíthetősége utólag feltölthető program komponensekkel.

A fájl rendszer:

A CardOS/M4.01A chip-specifikus kriptográfiai mechanizmusok által védett dinamikus és rugalmas fájl rendszert kínál:

- tetszőleges számú fájl (EF: Elementary File, DF: Dedicated File),
- a könyvtár fájlok (DF) egymásba ágyazását csak a tárolási kapacitás korlátozza,
- dinamikus tárolásvezérlés a rendelkezésre álló EEPROM optimális kihasználása érdekében,
- EEPROM működési hiba és áramkimaradás elleni védelem.

[1] A DIN V66291-1 C függelékében definiált tárolási struktúra egyetlen kulcstanúsítvány és a hozzá tartozó adatok számára.

Hozzáférés kontroll:

- 126 eltérő hozzáférési jogosultságot állíthat be a programozó,
- a hozzáférési jogosultságok tetszés szerint kombinálhatók Bool-algebrai kifejezésekkel,
- minden parancs- vagy adat-objektum egyéni hozzáférési profillal védhető,
- az összes úgynevezett "kulcsobjektum" a megfelelő DF-ben kerül tárolásra,
- a biztonsági struktúra a fájlok létrehozását követően is adatvesztés nélkül finomítható tovább.

Kriptográfiai szolgáltatások:

- algoritmusok: RSA 1024 Bit (PKCS#1), SHA-1, Triple-DES (CBC), DES (ECB, CBC), MAC, Retail-MAC,
- Differenciális hibaelemzés elleni védelem ("Bellcore-Attack"),
- A DES és RSA védelme egyszerű teljesítmény elemzés (Simple Power Analysis) és differenciális teljesítmény elemzés (Differential Power Analysis) ellen,
- Parancs láncolás ("Command Chaining") támogatása ISO 7816-8 szabvány szerint,
- aszimmetrikus kulcsok generálása valódi "onboard" véletlenszám-generátor használatával,
- digitális aláírás funkciók megvalósítása a mikrochipen,
- külső nyilvános kulcsú tanúsítási szolgáltatásokhoz való kapcsolódási képesség.

Biztonságos üzenetküldés (Secure Messaging):

- ISO 7816-4 szabványnak megfelelő,
- külön meghatározható valamennyi parancs- illetve adat-objektumra.

4. MEGFELELŐSÉG AZ ALÁÍRÁSRÓL SZÓLÓ TÖRVÉNYNEK ÉS VONATKOZÓ RENDELETEKNEK

4.1. Megfelelőség

Az "SLE66CX322P mikrochipből, OS/M4.01A operációs rendszerből és elektronikus aláírás létrehozó alkalmazásból álló intelligens kártya" elektronikus aláírás létrehozó termék megfelel az alábbi követelményeknek:

- 2004. évi LV. törvénnyel módosított 2001. évi XXXV. törvény az elektronikus aláírásról
- 2/2002. (IV.26.) MeHVM irányelv a minősített elektronikus aláírással kapcsolatos szolgáltatásokra és ezek szolgáltatóira vonatkozó biztonsági követelményekről
- MSZ EN ISO/IEC 7816-4:2001 Információtechnika. Azonosító kártyák. Érintkezős, integrált áramkörös kártyák. 4. rész: Iparágak közötti parancsok információcseréhez
- MSZ ISO/IEC 7816-8:2001 Információtechnika. Azonosító kártyák. Érintkezős, integrált áramkörös kártyák. 8. rész: Biztonsággal kapcsolatos, iparágak közötti parancsok.

- ISO/IEC 7816-9: CD2 1998: Information technology – Identification cards Integrated Circuit(s) cards with contacts – Part 9: Additional interindustry commands and security attributes
- PKCS#1: RSA Encription Standard Version 1.5. Nov. 1993

Az aláírás generáló eszköz megfelel a fenti követelményeknek a 4.2. pontban leírt működési környezetben az alábbi feltételek teljesülése mellett:

1. A termék ismételt vizsgálata és a tanúsítás megújítása nélkül nem engedélyezett
   - az elektronikus aláírás alkalmazás jelen eljárásban tanúsított verziójának módosítása illetve kibővítése, vagy
   - további alkalmazások feltöltése a kártyára, amelyek a CardOS/M4.01. módosítását vagy kibővítését eredményezik.
2. A 3. fejezetben hivatkozott Triple-DES (CBC), DES (ECB, CBC), MAC, Retail-MAC algoritmusok alkalmazására nem kerül sor az elektronikus aláírások során, ezért nem képezik jelen biztonsági hitelesítés tárgyát.

4.2. Működési környezet

A fenti megfelelőség feltétele az alábbi működési környezetre vonatkozó követelményrendszer teljesülése:

4.2.1. Megszemélyesítés és technikai környezet

Jelen biztonsági hitelesítés az Infineon SLE66CX322P mikrochipen megvalósított, elektronikus aláírás alkalmazással kiegészített CardOS/M4.01A értékelésén alapul. Az értékelés **kizárólag azokra a processzorokra** vonatkozik, amelyek azonosítója (Chip Type ID) ’6C’ (hexadecimális), a ROM fejlesztési szint azonosítója „b14” (Designstand b14) és az Infineon drezdai 2-s számú gyártósorán készültek. Az érvényesség kiterjesztése más gyártósorra csak azzal a feltétellel lehetséges, ha a másik gyártósoron előállított SLE66CX322P hardver bizonyíthatóan ugyanazt a biztonságot mutatja fel.

Az elektronikus aláírás létrehozó eszköz alapja a ROM maszk C804 verziója (CardOS/ M4.01A), amely azonos minden konfigurációnál (lásd 4.2.2. fejezet)). Az elektronikus aláírás létrehozó alkalmazás alapstruktúrája szintén azonos minden konfigurációnál. Ezen túl a megszemélyesítés során egy – az összes konfigurációnál azonos – szolgáltatáscsomag kerül feltöltésre az elektronikus aláírás létrehozó eszközre.

A hitelesítés szolgáltatónak (HSZ) a biztonságos megszemélyesítéshez szükséges valamennyi biztonsági intézkedést dokumentálnia kell a saját biztonsági előírásában foglaltak szerint.

A CardOS/M4.01A szállítási, létrehozási és konfigurációs illetve a CardOS/M4.01 Trust Center dokumentációkban leírt komplettírozási-, inicializálási- és megszemélyesítési folyamatoktól nem szabad eltérni. Ezen folyamatok garantálják a működési hibák kiküszöbölését és ezért a HSZ biztonsági koncepciójának részét kell képezniük.

A megszemélyesítés centralizáltan és decentralizáltan egyaránt történhet:

- Centralizált (központi) eljárás esetén a megszemélyesítést teljes egészében a HSZ végzi; a folyamat során a központi megszemélyesítő script-et alkalmazzák.

- Decentralizált eljárás során egy úgynevezett előzetes megszemélyesítést (pre-personalisation) végez a HSZ a 'pre-personalisation script' alkalmazásával. Ez követően egy decentralizált regisztrációs hivatal (a HSZ kihelyezett egysége) fejezi be a megszemélyesítési folyamatot egy úgynevezett 'post-personalisation script' felhasználásával.

A megszemélyesítő script-ek csak a vonatkozó megjegyzéseknek megfelelő helyen és értelemben módosíthatók.

4.2.2. Az aláírás generáló eszköz leszállítása és konfigurálása

Az "SLE66CX322P mikrochipből, OS/M4.01A operációs rendszerből és elektronikus aláírás létrehozó alkalmazásból álló intelligens kártya" elektronikus aláírás létrehozó eszközt forgalmazó a 2. fejezetben leírt specifikációk szerint szállítja a hitelesítés szolgáltatónak. A specifikációnak teljes mértékben meg kell felelni.

Az aláírás létrehozó eszköz két különböző konfigurációval rendelkezik:

- A PIN által történő hitelesítést követően a felhasználó (kártyabirtokos) használatába kerülő személyes aláírás létrehozó eszköz kizárólag egyetlen elektronikus aláírás létrehozását teszi lehetővé. Ezen konfiguráció jelölése: "**n = 1**".
- Jelen hitelesítés tárgyát képezik azok az „aláírás létrehozó modulok" is, amelyek egynél több illetve végtelen számú aláírás létrehozását teszik lehetővé a PIN egyszeri hitelesítését követően. Ezen aláíró eszközök használata különlegesen védett környezetekre korlátozódik (pl. HSZ). Ezen konfigurációk jelölése: "**n ≠ 1**".

A jelölésnél az "**n**" arra a műszaki paraméterre utal, amely ezen viselkedésmódot meghatározza. A PIN segítségével történő egyszeri hitelesítést követően végtelen számú elektronikus aláírást lehet előállítani abban az esetben, ha n = 0 vagy n = 255, míg minden más lehetséges esetben ($1 \leq n \leq 254$) pontosan **n** elektronikus aláírás létrehozására van lehetőség. Aláírás létrehozó modul létrehozása esetén a megszemélyesítő folyamat illesztése is szükséges. A megszemélyesítést végző szervezeteknek szigorúan be kell tartaniuk az előírt folyamatokat. Jelen biztonsági hitelesítés mindkét konfigurációra ("**n=1**" és "**n ≠ 1**") kiterjed.

Az "SLE66CX322P mikrochipből, OS/M4.01A operációs rendszerből és elektronikus aláírás létrehozó alkalmazásból álló intelligens kártya" elektronikus aláírás létrehozó eszköz rendelkezik egy PUK (Personal Unblocking Key) kóddal a következő funkcionalitással:

- A PUK helyes bevitele esetén a PIN értéket újra lehet állítani.
- A PUK helyes bevitele nem tesz lehetővé semmiféle aláírás létrehozást.

A PUK kódot csak akkor szabad alkalmazni, amikor a hitelesítés szolgáltató biztosítja, hogy a 4.2.3. fejezetben megnevezett feltételek teljesülnek.

Az "SLE66CX322P mikrochipből, OS/M4.01A operációs rendszerből és elektronikus aláírás létrehozó alkalmazásból álló intelligens kártya" elektronikus aláírás létrehozó eszközt használó egyéb alkalmazások **nem** képezik jelen hitelesítés tárgyát.

4.2.3. A termék használata

Működés közben a megfelelő termék használat érdekében az alábbi előírásoknak kell megfelelni:

A minősített hitelesítés szolgáltatóra vonatkozó előírások:

- A személyes aláírás létrehozó eszközön (**"n=1"**) az elektronikus aláírás alkalmazáshoz szükséges kulcspár előállítása kizárólag különlegesen

biztonságos környezetben történhet.

- Az aláírás létrehozó modulon (**"n≠1"**) történő elektronikus aláírás alkalmazáshoz szükséges kulcspár előállítása kizárólag különleges biztonsági előírások teljesítése mellett történhet.
- Az **"n≠1"** konfiguráció csak különleges biztonsági környezetben használható, ahol az aláírás létrehozó modullal való visszaélés lehetősége megbízható módon kiküszöbölhető. Ilyen jellegű működési környezet általában a minősített hitelesítés szolgáltatóknál biztosított.
- Az egyszeri hitelesítést követően korlátlan számú elektronikus aláírás létrehozását lehetővé tevő aláírás létrehozó modulok (**"n≠1"** konfiguráció, n=0 vagy n=255) esetében a korlátozás egy megfelelő aláírás alkalmazás komponenssel biztosítható, amely az "idő" és "szám" paramétereket vezérli, feltéve, ha garantált, hogy az új hitelesítést minden esetben az aláíró kulcs tulajdonosa kezdeményezi (és nem az alkalmazás automatikus üzemmódban). Egyértelműen megállapítható kell legyen az aláíró kulcs tulajdonosának deklarált igénye az elektronikus aláírás létrehozására.
- A hitelesítés szolgáltató köteles garantálni, hogy a csak különleges biztonsági környezetben használható aláírás létrehozó modulokat (**"n≠1"** konfiguráció) a végfelhasználók (kártyabirtokosok) nem kaphatják meg személyes aláírás létrehozó eszközként.
- i). Az azonosító adatok (PIN és PUK) bevitele az aláírás létrehozó eszközbe a megszemélyesítési folyamat alatt úgy kell történjen, hogy a művelet végén az azonosító adatok ne legyenek tárolva az aláírást létrehozó eszközön kívül.
- ii). A kulcshitelesítés szolgáltató a biztonsági szabályzatában az azonosító adatok az aláíró kulcs tulajdonos részére való átadására illetve az általa történő felhasználására olyan eljárásokat kell előírjon, amelyek semmilyen azonosító adat az aláírást létrehozó eszközön kívüli tárolásával nem számolnak.
- - Az i) és ii) pontoknak megfelelő, a kulcshitelesítés szolgáltató által előírt eljárásokat biztonsági vizsgálatnak kell alávetni, és meg kell róla győződni, hogy azok eleget tesznek a törvényes követelményeknek. Ezen eljárásokat a szolgáltató megfelelő szabályzatában szerepeltetni kell.

Az "SLE66CX322P mikrochipből, OS/M4.01A operációs rendszerből és elektronikus aláírás létrehozó alkalmazásból álló intelligens kártya" elektronikus aláírás létrehozó eszköz leszállításakor a hitelesítés szolgáltatót megfelelő utasításokkal kell ellátni, hogy megfelelelhessen a fenti működési követelményeknek.

A végfelhasználókra vonatkozó általános követelmények:

- Az aláíró kulcs birtokosa az aláírás létrehozó eszközt úgy használja és tárolja, hogy a visszaélés és manipulálás megakadályozható legyen.
- Az aláíró kulcs birtokosa az aláírás létrehozó funkciót kizárólag olyan adatok vonatkozásában alkalmazhatja, amelyek integritását és hitelességét garantálni akarja.
- Az aláíró kulcs birtokosa az aláírás létrehozó eszközre vonatkozó aktivizáló adatait (pl. PIN) bizalmasan kezelje.
- Az aláíró kulcs birtokosa rendszeres időközönként módosítsa az aláírás létrehozó eszközre vonatkozó aktivizáló adatait.
- Az aláíró kulcs birtokosa az aláírás létrehozó eszközt kizárólag az elektronikus aláírásról szóló törvény előírásainak megfelelő aláírás

alkalmazás komponenssel együtt alkalmazhatja.

- Az aláírás létrehozó eszköz kizárólag olyan – a felhasználó által jól ismert – informatikai környezetben (“office IFD“) használható elektronikus aláírás létrehozására, amely
  - megfelel az elektronikus aláírásról szóló törvény előírásainak,
  - biztosítja a kártyabirtokos azonosító adatainak (PIN, PUK) bizalmasságát,
  - biztosítja az aláírás létrehozó eszközbe továbbított adatok integritását és bizalmasságát,
  - megfelelően továbbítja a felhasználói felület felé az aláírás létrehozó eszköz aktuális azonosítási állapotát, biztosítva ezzel a kártyabirtokos azonosító adatok (PIN, PUK) helyes felhasználását.
- Az aláírás létrehozó eszköz felhasználása ismeretlen informatikai környezetben (“public IFD“) nem engedélyezett.

4.3. Algoritmusok és kapcsolódó paraméterek

Az aláírás létrehozó eszköz biztosítja az SHA-1 lenyomatfüggvényt (hash-function) és az RSA algoritmust.

A 2/2002 MeHVM irányelv 1. melléklete szerint az SHA-1 lenyomatfüggvény és a minimum 1020 bit hosszú modulust használó RSA algoritmus használata legalább az alábbi időpontokig engedélyezett:

- 2005.12.31. digitális aláírásra,
- 2006.12.31-ig a digitális aláírás ellenőrzésére.

Az algoritmusok használati engedélye meghosszabbítható, ha az adott határidőig a műszaki komponensek vagy azok algoritmusai vonatkozásában nem látnak napvilágot olyan felfedezések, fejlesztések, amelyek a jelenlegi jogszabályi megfelelést érvényteleníténék.

4.4. Biztonsági szint és a védelmi mechanizmus erőssége

Az SLE66CX322P mikrochipen megvalósított “OS/M4.01A operációs rendszer elektronikus aláírás létrehozó alkalmazással” szoftver értékelése sikeresen megtörtént az **ITSEC E4** biztonsági szinten. Az alkalmazott védelmi mechanizmusok erőssége **magasszintű** besorolást kapott.

Az SLE66CX322P mikrochip értékelése sikeresen megtörtént a **Common Criteria EAL5+** biztonsági szinten (ALC_DVS.2, AVA_MSU.3 és AVA_VLA.4 teljesítésével).

Az “OS/M4.01A operációs rendszer elektronikus aláírás létrehozó alkalmazással” szoftver és az SLE66CX322P mikrochip informatikai biztonsági szempontoknak megfelelő korrekt integrálásának értékelése megtörtént.

Ez alapján az eszköz továbbra is megfelel a minősített elektronikus aláírás létrehozására alkalmas biztonságos aláíró eszközökkel (BALE) szemben támasztott követelményeknek, amelyek minimálisan az **ITSEC E3** vagy **CC EAL4** biztonsági szintet, illetve a védelmi mechanizmusok erősségére a **magasszintű** besorolást írják elő.

Dokumentum vége