T-Systems ...

Tanúsítási jelentés

T-Systems-DSZ-ITSEC-04084-2002

nem hivatalos magyar fordítása

CardOS/M4.01A
Digitális Aláírás
Előállító Alkalmazással
Siemens AG

T-Systems ISS GmbH

Tanúsítási jelentés: T-Systems-DSZ-ITSEC-04084-2002, version 1.0, September 24, 2002

A jelentéssel kapcsolatos további információkért vagy példányokért kérem lépjen kapcsolatba a tanúsító szervezettel:

Levél: T-Systems ISS GmbH, - Zertifizierungsstelle -, Rabinstr.8, D-53111 Bonn, Germany
Telefon: +49-228-9841-0, Fax: +49-228-9841-60
WEB: www.t-systems-zert.com

Embléma: Deutsches IT-Sicherheitszertificat
Annerkant: Bundesamt für Sicherheit in der Informationstechnik
(Információtechnikai Biztonsági Hivatal által elismert
Német IT - Biztonsági Tanúsítvány)

T-Systems ...

A T-Systems ISS GmbH

Tanúsító Szervezete

ezennel tanúsítja, hogy a

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

CardOS/M4.01A Digtális Aláírás Létrehozó Alkalmazással

eszközét megvizsgálta az ITSEC-nek és ITSEM-nek megfelelő specifikus Biztonsági Előirányzat alapján; a következő eredmények születtek:

Biztonsági funkciók:	Azonosítás és autentikáció, Hozzáférés szabályozás, Auditálás, Objektumok újrahasznosítása, Adatcsere
A kiértékelés bizonyossági szintje:	**E4**
A mechanizmusok minimális erőssége:	**Magasszintű**

Ez a tanúsítvány megfelel az 1998.03.03-án aláírt SOGIS-MRA követelményeinek (aláíró országok: Finnország, Franciaország, Németország, Nagy-Britannia, Görögország, Olaszország, Hollandia, Norvégia, Portugália, Spanyolország, Svédország, Svájc).
A tanúsítvány csak a tanúsítási jelentésben leírt konfigurációra és környezetre érvényes, a lenti regisztrációs kódú teljes tanúsítási jelentéssel összefüggésben. A tanúsítási jelentés megkötéseit és javaslatait be kell tartani. A tanúsítási jelentés tartalmazza a Biztonsági Előirányzatot, amely a vizsgálat alapját képezte. A tikosításra és visszakódolásra alkalmas kriptográfiai algoritmusok erősségének meghatározása a BSI meghatározásából származik. A tanúsítás és tanúsítási jelentés másolataiért lépjen kapcsolatba a tanúsító szervezettel vagy a megbízójával!

Regisztráció:
T-Systems-
DSZ-ITSEC-04084-2002

Bonn: Sept. 24, 2002

Dr. Heinrich Kersten
tanúsító szervezet vezetője

Certification Body of T-Systems ISS GmbH, Rabinstr.8, D-53111 Bonn, Germany
_ +49-228-9841-0, Fax: +49-228-9841-60, Internet: www.t-systems-zert.com
accredited against EN 45011 unter DAR registration DIT-ZE-005/98 by DATech e.V.

Tartalom

Függelék

Biztonsági előirányzatok a
„CardOS/M4.01A Digitális Aláírás Létrehozó Alkalmazással”
elektronikus aláíró eszközhöz
(nincs lefordítva: elérhető angol nyelven:
http://www.t-systems-zert.de/pdf/ein_01_zer_itsec_cc/zr_04084_e.pdf;
német nyelven: CardOS/M4.01A mit Applikation für digitale Signatur
http://www.t-systems-zert.de/pdf/ein_01_zer_itsec_cc/zr_04084_d.pdf)

Rövidítések

AIS	Anwendungshinweise und Interpretationen zum Schema [Felhasználási útmutató és értelmezés a sémához]
BGBl	Bundesgesetzblatt [Német Szövetségi Közlöny]
BS	British Standard [Brit szabvány]
BSI	Bundesamt für Sicherheit in der Informationstechnik [Információtechnikai Biztonsági Hivatal]
CC	Common Criteria for Information Technology Security Evaluation [Információtechnológiai Biztonsági Fejlesztések Egységes Követelményrendszere]
CEM	Common Methodology for Information Technology Security Evaluation [Információtechnológiai Biztonsági Fejlesztések Egységes Módszertana]
DAR	Deutscher Akkreditierungsrat [Német Akkreditációs Tanács]
DATech	Deutsche Akkreditierungsstelle Technik e.V. [Német Műszaki Akkreditációs Hatóság]
DIN	Deutsches Institut für Normung e.V. [Német Szabványügyi Intézet]
ETR	Evaluation Technical Report [műszaki vizsgálati jelentés]
ISO	International Organization for Standardization [Nemzetközi Szabványosítási Szervezet]
IT	Information Technology [információtechnológia]
ITSEC	Information Technology Security Evaluation Criteria [Információtechnológiai Biztonsági Értékelési Követelmény]
ITSEF	IT Security Evaluation Facility [IT Biztonsági Értékelési Szervezet]
ITSEM	IT Security Evaluation Manual [IT Biztonsági Értékelési Kézikönyv]
JIL	Joint Interpretation Library [egységes értelmező könyvtár]
RegTP	Regulierungsbehörde für Telekommunikation und Post [(német) Távközlési és Postaügyi Szabályozó Hatóság]
SigG	Signaturgesetz [Német Elektronikus Aláírási Törvény]
SigV	Signaturverordnung [Német Elektronikus Aláírási Rendelet]
TOE	Target of Evaluation [a vizsgálat tárgya, VT]

Referenciák

AIS	Anwendungshinweise und Interpretationen zum Schema [Felhasználási útmutató és értelmezés a sémához], BSI, jóvágyagyott verzió
ALG	Geeignete Kryptoalgorithmen [jóváhagyott kriptográfiai algoritmusok], a RegTP által közzétéve a Német Szövetségi Közlönyben, hivatalos verzió
BS7799	BS 7799-1:2000 Information technology - Code of practice for information security management [az informatikai biztonsági menedzsment gyakorlati kódolása] BS7799-2:1999 Specification for information security management systems [az informatikai biztonsági menedzsment rendszerek specifikációja]
CC	Common Criteria for Information Technology Security Evaluation (ISO 15408), August 1999 Part 1: Introduction and general model [bevezetés és általános modell] Part 2: Security functional requirements [biztonsági funkcionális követelmények] Part 3: Security assurance requirements [biztonsági garanciák követelményei]
CEM	Common Methodology for Information Technology Security Evaluation Part 1: Introduction and general model, [bevezetés és általános modell] version 0.6, January 1997 Part 2: Evaluation Methodology [vizsgálati módszertan], version 1.0, August 1999
EU-DIR	Directive 1999/93/EC of the European Parliament and of the Council of 13 December 1999 on a Community framework for electronic signatures [az Európai Parlament és Tanács direktívája az elektronikus aláíró rendszerek közösségi keretrendszere]
ITSEC	Information Technology Security Evaluation Criteria (ITSEC), version 1.2 (1991), ISBN 92-826-3004-8
ITSEM	Information Technology Security Evaluation Manual (ITSEM), version 1.0 (1993), ISBN 92-826-7087-2
JIL	Joint Interpretation Library, version 2.0, November 1998
SigG	Gesetz über Rahmenbedingungen für elektronische Signaturen und zur Änderung weiterer Vorschriften (Signaturgesetz . SigG) as of May 16, 2001 (BGBl. I, S. 876 ff.)
SigV	Verordnung zur elektronischen Signatur (Signaturverordnung . SigV) 16.11.2001 (BGBl. I., S. 3074 ff.)

Szószedet

Ez a szószedet értelmezi a T-Systems ISS GmbH tanúsításában használt kifejezéseket, de nem törekszik teljességre vagy általános érvényességre.

Accreditation	Akkreditáció. Egy akkreditációs szervezet által végzett folyamat annak igazolására, hogy egy vizsgáló, értékelő testület [pld. egy tanúsító szervezet] megfelel a vonatkozó szabványok – ISO 17025 [resp. EN 45011] – által támasztott követelményeknek.
Audit	Auditálás: Egy eljárás, melynek során igazolást nyer, hogy egy folyamat az elvárásoknak megfelelően működik.
Availability	Elérhetőség, rendelkezésre állás: Klasszikus biztonsági cél. Az arra feljogosított személyeknek mindig hozzá kell férniük az adatokhoz, vagyis az adat elérését nem akadályozhatják meg arra jogosulatlan személyek, vagy műszaki hibák.
Certificate	Tanúsítvány: A tanúsító szervezet által kiállított összefoglaló megállapítás a tanúsítás eredményéről.
Certification	Tanúsítás: Független értékelés a fejlesztés korrektségéről. Ezt a kifejezést használjuk a teljes folyamat megnevezésére is, amely a kiértékelésből, monitorozásból, majd ezt követően a tanúsítványok és tanúsítási jelentések kibocsátásából áll.
Certification Body	Tanúsító szervezet: Egy szervezet, amely tanúsítványokat állít elő.
Certification Report	Tanúsítási jelentés: A tanúsító szervezet által kiadott jelentés a tanúsítás tárgyáról, folyamatairól és eredményeiről.
Certification Scheme	Tanúsítási séma: A tanúsító szervezet által alkalmazott elvek, szabályzatok és folyamatok összessége.
Certification Service Provider	Hitelesítés szolgáltató: Egy intézmény, amely igazolja az egyének és aláíró kulcsok összerendelését a elektronikus tanúsítványok vonatkozásában.
Certifier	Tanúsító: A tanúsító szervezet alkalmazottja, aki felhatalmazással bír a kiértékelés felügyeletére és a tanúsítás végrehajtására.
Confidentiality	Bizalmasság: Klasszikus biztonsági cél. Az adatokat csak az arra feljogosított személyek érhetik el.
Evaluation	Kiértékelés: Egy IT termék, rendszer vagy szolgáltatás kiértékelése egy publikált IT biztonsági feltételrendszer szerint.
Evaluation (Assurance) Level	A kiértékelés bizonyossági szintje: A kiértékelés során elért bizonyossági szint. Az ITSEC/CC biztonsági kritériumok besorolási rendszerének része, annak

	garancia szintje, hogy a vizsgálat tárgya eléri a kitűzött Biztonsági előirányzatokat.
Evaluation Facility	Kiértékelő szervezet: A kiértékelést végző szervezeti egység (ITSEF).
Evaluation Technical Report	Kiértékelés műszaki jelentése.: A kiértékelő szervezet által írt végső jelentés a kiértékelés folyamatáról és eredményeiről.
Evaluator	Kiértékelő: A kiértékelésben részt vevő személy a kiértékelő szervezetnél.
Integrity	Integritás: Klasszikus biztonsági cél. Csak feljogosított személy lehet képes az adatok megváltoztatására.
IT Product	IT termék: A szállítótól (gyártótól, forgalmazótól) beszerezhető szoftver és/vagy hardver.
IT Security Management	IT biztonsági rend (szabályzat): Egy szervezet IT biztonságának létrehozása és fenntartása érdekében alkalmazott eljárásrend.
IT Service	IT szolgáltatás: Egy IT rendszer által nyújtott szolgáltatás.
IT System	IT rendszer: IT termékek egy egységként funkcionáló kombinációja. (ITSEC:) IT termékek valódi installációja egy ismert működési környezetben.
License Agreement	Licensz megállapodás: A tanúsító hatóság és a kiértékelő szervezet közötti megállapodás, amely a közös kiértékelő és tanúsító project eljárási és felelősségi kérdéseit szabályozza.
Milestone Plan	Mérföldkő terv: A kiértékelő és tanúsító folyamat ütemezésének terve.
Monitoring	Monitorozás, felügyelet: A tanúsító szervezet által alkalmazott eljárás a kiértékelési folyamat helyes menetének ellenőrzésére (megfelelés a követelményeknek, szabványos folyamatok és osztályozások használata, stb.).
Problem Report	Probléma jelentés: A kiértékelés alatt a kiértékelő szervezet által a tanúsító hatóságnak küldött jelentés valamilyen speciális kérdésben, pld. egy IT biztonsági követelmény értelmezésének vonatkozásában.
Process	Folyamat: Láncolt események (részfolyamatok, folyamat elemek) sora, amelyet egy bizonyos szolgáltatás nyújtása érdekében hajt végre egy adott környezet.
Product Certification	Termék tanúsítás: IT termékek tanúsítása.
Re-Certification	Újra tanúsítás, tanúsítás megújítása: Egy korábban már tanúsított termék módosított verziójának újra tanúsítása; az új tanúsítás szükséges lehet egy eszköz, gyártási/szállítási folyamat vagy biztonsági követelmény változása miatt is.

Security Certificate	Biztonsági tanúsítvány: lásd Certificate
Security Confirmation SigG:	SigG biztonsági igazolás: Egy hivatalosan előírt dokumentáció, amely igazolja a német aláírási törvénynek való megfelelőséget..
Security Criteria	Biztonsági előírás: Szabályozó jellegű dokumentum, amely tartalmazhat a termékre, rendszerre, szolgáltatásra vonatkozó műszaki adatokat, de legalább ezen követelmények kiértékelését leírja.
Security Function	Biztonsági funkció: Bizonyos fenyegetettségeket közömbösítő funkció.
Security Target	Biztonsági előirányzat: Egy adott TOE fejlesztésénél kiinduló alapként felhasznált biztonsági követelményeket és előírásokat leíró dokumentum.
Service	Szolgáltatás: Itt egy vállalat által felajánlott tevékenység, melyet az üzleti folyamatai szolgáltatnak és az ügyfél által felhasználható.
System Certification	Rendszer tanúsítás: Egy telepített IT rendszer tanúsítása.
Target of Evaluation	Kiértékelés tárgya (TOE): A kiértékelési folyamat tárgyát képező IT termék vagy rendszer a hozzá kapcsolódó adminisztrátori és felhasználói dokumentációval.
Trust Centre	Bizalmi központ: lásd Certification Service Provider

Biztonsági követelmények alapjai

Ez a fejezet röviden áttekinti a kiértékelés során használt feltételeket és azok osztályozási rendszerét. Az eredeti ITSEC és ITSEM szöveget zárójelekbe írjuk.

- Alapok

Az ITSEC vizsgálati módszere alapján a biztonság akkor megfelelő, ha elegendő bizonyosság van arra vonatkozóan, hogy a vizsgálat tárgya (TOE: target of evaluation) megfelel a biztonsági céloknak.

Általánosságban, egy termék vagy rendszer biztonsági céljai bizonyos adatok bizalmasságára, elérhetőségére és integritására vonatkozó követelményekből állnak. Ezeket a biztonsági célokat a kiértékelés szponzora fogalmazza meg. Normál esetben egy IT termék vizsgálatának szponzora a fejlesztő vagy forgalmazó, egy IT rendszer vizsgálatánál a rendszer tulajdonosa.

A megfogalmazott biztonsági célokat fenyegetettségeknek teszik ki, mint pld. az adatok bizalmasságának, elérhetőségének, integritásának elvesztése.

Az alapvető fenyegetettségek támadásokká válnak, amikor illetéktelenek megpróbálják olvasni, módosítani az adatokat, vagy meggátolni a jogosult felhasználókat az adatok elérésében.

A TOE által biztosított biztonsági funkciók hivatottak elhárítani ezeket a fenyegetettségeket.

Két alapkérdés van:

- Megfelelően működnek a biztonsági funkciók?
- Hatékonyak a biztonsági funkciók?

Ennek megfelelően a biztonsági céloknak való megfelelés a korrektség és hatásosság értékelése révén állapítható meg kielégítő biztonsággal.

- Bizonyossági szint

A kiértékeléshez csak korlátozott források állnak rendelkezésre, különösen korlátozott a rendelkezésre álló idő.

Ennek következtében a kiértékelés mélysége mindig korlátozott. Másrészt értelmetlen lenne nagyon sok erőforrást áldozni egy olyan kiértékelésre, amikor csak alacsony biztonsági szintre van szükség, ugyanilyen helytelen volna kis erőforrást használni, amikor magas szintű biztonságra van szükség.

Ennek megfelelően célszerű különböző megfelelőségi szinteket meghatározni. Az ITSEC 6 megfelelőségi szintet használ a korrektség és hatásosság értékeléséhez. E1 a legalacsonyabb, E6 a legmagasabb szint.

Ennek megfelelően a TOE megbízhatósága ezeken a megfelelőségi szinteken mérhető.

Az ITSEC-ből származó alábbi kivonatok megmutatják, hogy a kiértékelési folyamat mely szempontokat fedi le, és milyen mélységű elemzés tartozik az egyes megfelelőségi szintekhez.

(A TOE az értékelendő termék vagy rendszer)

E1 Ezen a szinten kell lenni egy Biztonsági előirányzatnak és egy kötetlen leírásnak a TOE rendszerszintű tervezéséről. Működési tesztekkel kell igazolni, hogy a TOE kielégíti a Biztonsági előirányzatokat.

E2 Az E1 szint követelményein túlmenően lenni kell egy kötetlen leírásnak a TOE részletes tervezéséről. Egyértelműen meg kell bizonyosodni a helyes működésről. Léteznie kell egy konfigurációs vezérlő rendszernek egy elfogadott terjesztési eljárásnak.

E3 Az E2 követelményein túlmenően ki kell értékelni a biztonsági rendszerek forráskódját vagy hardver kapcsolási rajzait. Ezen funkciók helyes működéséről meg kell győződni.

E4 Az E3 követelményein túlmenően szükséges egy alap hivatalos biztonsági politika a Biztonsági előirányzatok szolgálatában. A biztonsági védelmi funkciókat, az architektúrális és részletes tervet specifikálni kell tetszőleges formátumban.

E5 Az E4 követelményein túlmenően szoros megfelelőségnek kell lennie a részletes biztonsági terv és a forráskód vagy hardver terv között.

E6 Az E5 követelményein túlmenően a biztonsági védelmi funkciókat és a rendszertervet megadott formában kell előállítani, ami összhangban van a specifikált alap formális modellel és biztonsági politikával.

Ezen túlmenően valamennyi szinten ki kell értékelni a hatékonysági szempontokat az alábbi követelményeknek megfelelően:

A hatékonyság értékelése magába foglalja a TOE alábbi szempontok szerinti megvizsgálását.

a) a TOE biztonsági védelmi funkcióinak alkalmassága a Biztonsági előirányzatokban megfogalmazott fenyegetettségek kivédésére

b) a TOE biztonsági védelmi funkcióinak és mechanizmusainak alkalmassága az együttműködésre oly módon, hogy kölcsönösen támogatják egymást és egy egységes, hatékony egészet alkotnak.

c) a TOE védelmi mechanizmusainak képessége a közvetlen támadások kivédésére

d) vajon a TOE megalkotásakor ismert biztonsági hiányok veszélyeztethetik-e a gyakorlatban a TOE biztonságát

e) hogy a TOE nem konfigurálható vagy használható nem biztonságos módon, miközben az adminisztrátor vagy felhasználó azt indokoltan biztonságosnak hiszi

f) vajon a TOE ismert működési biztonsági hiányosságai veszélyeztethetik-e a gyakorlatban a TOE biztonságát

- Biztonsági funkciók és védelmi mehanizmusok

A TOE biztonsági funkcióinak feladata a fenyegetettségek elhárítása.

A biztonsági funkciók megfelelő csoportosításával funkcionális osztályokat hoztak létre:

Példa: Az F-C2 funkcionalitási osztály lefedi az ’Azonosítás és hitelesítés’, ’Hozzáférés szabályozás’, ’Könyvelés és auditálás’ ’Objektum újra felhasználása’ általános fejezeteket. Ez egy tipikus osztály számos operációs rendszerre.

Egy speciális biztonsági funkció általában több módon is megvalósítható.

Példa: Az ’Azonosítás és hitelesítés’ funkció megvalósítható egy jelszavas eljárással, intelligens kártyával egy ’challenge response’ eljárással vagy biometrikus módszerekkel. Az ’Azonosítás és hitelesítés’ biztonsági funkció különféle megvalósításait biztonsági mechanizmusoknak nevezzük. Más biztonsági függvényeknél a mechanizmus fogalmát hasonlóan használjuk.

A biztonsági mechanizmus erőssége a mechanizmus osztályozott képessége a potenciális közvetlen támadások elhárítására.

Az ITSEM kétféle mechanizmus típust vesz figyelembe: B és A típusút.

B típus A B típusú biztonsági mechanizmusnak megfelelő tervezés és megvalósítás esetén nincs gyengesége. A B típusú mechanizmust ellenállónak tekinthetjük a közvetlen támadásokkal szemben függetlenül a felhasznált források, szakismeret és lehetőségek mennyiségétől. Azonban ezek a B típusú mechanizmusok gyengíthetők indirekt támadásokkal, amelyek más hatékonyságvizsgálat tárgyát képezik.

A típus Az A típusú védelmi mechanizmusok potenciális sebezhetőséget tartalmaznak az algoritmusukban, elvükben vagy tulajdonságaikban, így megfelelő erőforrás, szakértelem és lehetőség esetén egy közvetlen támadás során feltörhetők. Az A típusú mechanizmusok gyakran valamilyen 'titok' használatát tételezik fel, mint például egy jelszó vagy kriptográfiai kulcs.

Az A típusú mechanizmusok erőssége megfelel a közvetlen támadással való feltörésükhöz szükséges erőforrások, szakértelem és lehetőség szintjének.

Hogyan definiálható az A típusú mechanizmusok erőssége?

Valamennyi biztonsági mechanizmust felbecsülik (pontosabban, amelyek hibája biztonsági gyengeséget okoz) a közvetlen támadásokkal szembeni ellenálló képesség alapján. Valamennyi védelmi mechanizmus minimális (garantált) védelmi erőssége három csoportba sorolandó: alapszintű, közepes és magasszintű.

alapszintű Az alapszintű kritikus védelmi mechanizmusnak biztonságosan védelmet kell nyújtania legalább a véletlenszerű, téves támadások ellen, de megfelelő ismerettel rendelkező támadók hatástalaníthatják a működését.

közepes A közepes szintű kritikus védelmi mechanizmus védelmet nyújt legalább a korlátozott erőforrással és lehetőséggel rendelkező támadók ellen.

magasszintű A magasszintű kritikus védelmi mechanizmusnál egyértelműnek kell lennie, hogy csak a magasszintű gyakorlattal, lehetőséggel és forrásokkal rendelkező támadók gyengíthetik, a sikeres támadást normál körülmények között gyakorlatilag megvalósíthatatlannak tartjuk.

1 A vizsgálat tárgya és szponzora

1 **Szponzor** Siemens AG, ICN EN TNA, Charles-de-Gaulle Strasse 2-4, D-81737 Munich, Germany.

2 A kért tanúsítvány típusa .**Deutsches IT Sicherheitszertifikat [német IT biztonsági tanúsítvány]**..

3 A vizsgálat tárgya **„**CardOS/M4.01A elektronikus aláírás alkalmazással (az IC beágyazott szoftvere megfelel a német SigG, SigV és DIN V 66291-1 normáknak).**biztonságos elektronikus aláíró termék**.

4 A TOE egy Infineon SLE66CX322P chipen megvalósított intelligens kártya operációs rendszer elektronikus aláírás alkalmazással.

5 A szponzor a TOE Biztonsági előirányzatait tartalmazó dokumentumot biztosította a vizsgálathoz angol nyelven. A Biztonsági előirányzatok 2002.09.11-i dátumú 2.2-es verziója megtalálható a jegyzőkönyv függelékei között.

6 A Biztonsági előirányzat az **ITSEC** kritériumok teljesítése **E4** bizonyossági szinten, a védelmi mechanizmusok minimális erőssége **magasszintű**.

7 A tanúsítvány regisztrációs kódja T-Systems-DSZ-ITSEC-04084-2002

2 A vizsgálat főbb dokumentumai

8 A szponzor kérésének megfelelően a TOE vizsgálata az ITSEC alapján történt

9 Ezentúl a vizsgálat és tanúsítás során az alábbi dokumentumok voltak fontosak:

- Information Technology Security Evaluation Manual (ITSEM) /ITSEM/,
- Joint Interpretation Library /JIL/,
- Anwendungshinweise und Interpretationen zum Schema, Bundesamt für Sicherheit in der Informationstechnik /AIS/,
- Work instruction .Deutsches IT-Sicherheitszertifikat by T-Systems ISS GmbH (endorsed version).

3 A vizsgálat

10 A TOE értékelését a ’Prüfstelle für IT-Sicherheit of T-Systems ISS GmbH’ végezte a Siemes AG megbízásából.

11 Az ISO 1705 akkreditációval rendelkező értékelő szervezet a vizsgálat tárgyában rendelkezik a BSI tanúsító hatóságának érvényes **engedélyével**.

12 A kiértékelés a T-Systems ISS GmbH tanúsítási sémájának megfelelő feltételekkel történt.

13 A kritériumoknak való megfelelés vonatkozásában a kiértékelést folyamatosan figyelemmel kísérte a tanúsító hatóság.

14 A vizsgáló szervezet által előállított 2.03 verziószámú, 2002.09.23-i dátumú tanúsítási jelentés (**Evaluation Technical Report** (ETR)) tartalmazza a tanúsítás eredményeit.

15 A tanúsítás 2002. 09.24-én fejeződött be.

4 Tanúsítás

16 A T-Systems ISS GmbH **tanúsítási sémája (eljárása)** a tanúsító hatóság honlapján megtalálható (www.t-systems-zert.com).

17 A T-Systems ISS GmbH **tanúsító szervezete** az EN 45011-nek megfelelően működik és a DATech e.V. által kiadott megfelelő felhatalmazással rendelkezik ITSEC és Common Criteria (DAR regisztrációs szám DIT-ZE-005/98). szerinti vizsgálatok végzésére.

18 A TOE **tanúsítása** a megbízó kérésének megfelelően a 4-es típusú német IT-biztonsági tanúsításnak megfelelően történt (type 04: .Deutsches IT-Sicherheitszertifikat)

19 A TOE tanúsítása megszorítások és javaslatok tárgyát képezheti az 5. fejezetben részletezett módon.

20 Jelen tanúsítási jelentés 3. oldalán található az eredményeket összegző 2002.09.24-i T-Systems-DSZ-ITSEC-04084-2002 biztonsági tanúsítás.

21 A tanúsítványon a BSI (Bundesamt für Sicherheit in der Informationstechnik) hivatalos engedélyével szerepel a német IT Biztonsági tanúsítás logója (Deutsches IT-Sicherheitszertifikat), amely szerint a BSI a tanúsítványt a saját tanúsítványaival egyenrangúnak ismeri el. Szerződéses megállapodás alapján a BSI nemzetközi viszonylatban is megerősíti ezt a megfelelést.

22 A tanúsítás és a tanúsítási jelentés publikálásra került a tanúsító szervezet Internetes lapján (www.t-systems-zert.com) és a BSI BSI 7148 / 7149 kiadványokban.

23 Ezennel igazoljuk, hogy

- az eljárásban résztvevő értékelők és tanúsítók nem vettek részt a TOE fejlesztésében, értékesítésében és alkalmazásában.
- Az egyedi típusú eljárás tanúsítási sémájának valamennyi szabálya és a vonatkozó kritériumok betartásra kerültek.

Klaus-Werner Schröder	Dr. Heinrich Kersten
(tanúsító)	(tanúsító szervezet vezetője)

5 Az eredmények összefoglalása

24 Az értékelést a TOE alábbi konfigurációján végeztük:

A TOE a C804-es ROM maszk verzión (CardOS/M4.01A) alapul, amely a TOE minden konfigurációjára egyedi. Az alap aláíró alkalmazás szintén egyedi a TOE valamennyi konfigurációjára. A megszemélyesítés során a TOE-re töltött szolgáltatás csomag szintén egyedi a TOE összes konfigurációjára.

a TOE konfigurációi az alábbi szempontok vonatkozásában különböznek:

A megszemélyesítés folyamata centralizált vagy decentralizált lehet

Centralizált megszemélyesítés esetén az egész folyamatot a bizalmi központban (tanúsító hatóság) végzik az ennek megfelelő megszemélyesítő program használatával (personalisation script for centralised personalisation).

Decentralizált megszemélyesítés esetén a bizalmi központban (hitelesítő szervezet) elő-megszemélyesítést végzünk a megfelelő programmal (personalisation script for pre-personalisation), majd a megszemélyesítés folyamatát egy helyi regisztrációs hatóságnál (LRA: local registration authority) folytatjuk illetve fejezzük be a megfelelő program (personalisation script for post-personalisation) felhasználásával.

A TOE személyes konfigurációját (röviden **n = 1**) egyéneknek (kártyabirtokos) tervezték. A PIN kóddal (Personal Identification Number) történő azonosítás után a kártyabirtokos egyetlen elektronikus aláírást hozhat létre. A TOE aláíró modul konfigurációját (röviden **n ≠ 1**) speciálisan biztosított környezetben való felhasználásra tervezték (mint pld a minősített tanúsítási szolgáltató). A PIN alapú azonosítás után egynél több, vagy korlátlan számú elektronikus aláírás hozható létre.

Az n paraméter határozza meg a fent leírt működési módokat. n=0 és n=255 esetén korlátlan számú elektronikus aláírás hozható létre egyetlen azonosítás után. Minden más esetben (1 ≤ n ≤ 255) pontosan n számú elektronikus aláírás generálható egy azonosítás után. Aláíró modul létrehozásához a megszemélyesítő folyamatot e szerint kell alkalmazni. A megszemélyesítésért felelős szervezetet tájékoztatni kell az igénylési eljárásról és különös figyelemmel kísérnie a kézbesítési folyamatot, nehogy tévedésből egy egyéni felhasználóhoz kerüljön az aláíró modul.

25 A kiértékelés eredménye csak a fentebb leírt TOE konfigurációra vonatkozik.

26 A biztonsági előirányzatokon és a kiértékelés eredményére alapozva a TOE az alábbi biztonsági funkcionalitásokkal rendelkezik:

Azonosítás és hitelesítés, Hozzáférés szabályozás, Auditálás, Elem újrafelhasználás, Adatcsere

27 A vizsgáló szervezet arra a megállapításra jutott, hogy a TOE megfelel az ITSEC E4 biztonsági szint által támasztott korrektségi és hatásossági követelményeknek

Az **ITSEC E4.1 – E4.37** pontoknak a korrektség szempontjából

Tervezési, fejlesztési folyamat:

Követelmények, Blokkszintű tervezés, részletes tervezés, megvalósítás

Tervező – fejlesztő környezet:

A kialakítás szabályozása, programnyelvek és fordítók,

fejlesztők biztonsága ...

Üzemeltetés – Felhasználói dokumentáció

Felhasználói dokumentáció, Adminisztrátori dokumentáció

Üzemeltetés

Szállítás és beállítás, Beindulás és üzemelés

ITSEC 3.12 - 3.37 a hatékonyság szempontjából

Hatékonysági követelmény – Tervezés:

A funkcionalitás megfelelősége, a funkcionalitások összeköttetése, a mechanizmusok erőssége, a konstrukció sebezhetőségének értékelése

Hatásossági kritérium - Működés

Könnyű használhatóság, Üzemelési sebezhetőség értékelése

28 A védelmi mechanizmusok vonatkozásában az értékelés a következő eredménnyel zárult:

A TOE védelmi mechanizmusai közül kritikusak: valamennyi

A minimálisan **magasszintű** védelemmel rendelkező **A** típusú védelmi mechanizmusok: M1, M2, M4, M5, M10, M11 (lásd: Biztonsági előirányzatok)

B típusú biztonsági mechanizmusok: az összes többi

A B típusú biztonsági mechanizmusokra a követelményrendszernek megfelelően nem határozunk meg erősségi szintet. Ennek ellenére akkor sem észlelhető kihasználható, támadható gyengülés a feltételezett környezetben, ha egy magasszintű támadást tételeztünk fel a sebezhetőség vizsgálat során.

29 A TOE kézbesítési eljárását a megrendelő az alábbiak szerint írta le:

Kézbesítés futár által. Ez a kézbesítési folyamat megfelel a nemzeti tanúsítási hatóság által az ITSEC E4 szintre meghatározott követelményeknek.

30 A megrendelőnek az alábbi korlátozásokat kell betartania:

1. A T-Systems-DSZ-ITSEC-04084-2002 tanúsítvány és a hozzá tartozó tanúsítási jelentés csak a következő eszköz verzióra vonatkozik: ”SLE66CX322P mikrochipből, OS/M4.01A operációs rendszerből és elektronikus aláírás létrehozó alkalmazásból álló intelligens kártya”, ahol a chip típus azonosító 6C (hexadecimális), és a chip az Infineon 2-s számú gyártósorán, Drezdában készült.
2. A SigG előírásainak megfelelő kriptográfiai eljárásokat a SigV 1. melléklet 2. fejezetének megfelelően publikálták a Szövetségi Újságban. A jelenleg érvényes publikálás (Geeignete Kryptoalgorithmen, 05.07.2001, Federal Gazette No. 158, p. 18562, as of August 24th, 2001) szerint a TOE algoritmusai (hash algorithm SHA-1 and RSA algorithm) 2006 végéig engedélyezettek. Ennek megfelelően az SO6 *A kulcsgenerálás minősége* és az SO7 *Biztonságos digitális aláírás előállítása* vonatkozásában kapott

értékelési eredmények 2006 végéig érvényesek, ez után a vizsgálat megismétlése szükséges.

3. A TOE ismételt vizsgálata szükségessé válik, amint olyan új fejlesztések, vagy felfedezések látnak napvilágot, amelyek potenciális veszélyt jelentenek a TOE kriptográfiai vagy más védelmi mechanizmusaira, és kérdésessé teszik a mechanizmusok magasszintű védelmi képességét.

4. Az SLE66CX322P hardver kézbesítésére az alábbi folyamatot kell használni: A gyártónak (Siemens AG, ICN EN TNA) személyesen kell átvennie a félvezető szeleteket és modulokat az Infineon regensburgi raktárában.

5. Különösen figyelni kell a teljes felhasználói dokumentáció kézbesítésére (lásd Biztonsági előirányzatok).

31 A TOE biztonságos használatához az alábbi feltételeknek kell teljesülniük:

1. Amennyiben az ”SLE66CX322P mikrochipből, OS/M4.01A operációs rendszerből és elektronikus aláírás létrehozó alkalmazásból álló intelligens kártya” aláíró eszközt a hatályos jogszabályoknak megfelelő minősített elektronikus aláírás létrehozására használják, a hitelesítés szolgáltató biztonsági szabályzatában a biztonságos megszemélyesítéshez szükséges valamennyi feltételt/körülményt szabályozni kell.

2. A speciálisan biztonságos környezetben való felhasználásra tervezett, aláíró modulként konfigurált TOE-t (n ≠ 1) **TILOS** kiadni magánszemélyeknek személyes aláíró eszközként. A követelmény betartása a kártya kibocsátó (hitelesítés szolgáltató) felelőssége.

3. A kártya gyártása, inicializálása, megszemélyesítése során szigorúan be kell tartani a „CardOS/M4.01 Delivery, Generation and Configuration” és a „CardOS/M4.01 Documentation for Trust Center” dokumentumokban leírt folyamatokat, azoktól eltérni tilos. Ezek a folyamatok megakadályozzák a hibákat, és a hitelesítés szolgáltató biztonsági koncepciójának részét kell képezniük. A megszemélyesítő program módosítása csak a megjegyzésekben meghatározott helyen és értelemben engedélyezett.

4. A kulcsgenerálás csak biztonságos környezetben engedélyezett, mint például a hitelesítés szolgáltató telephelye.

5. A TOE nem felel meg a DIN V 66291-1 szabványnak abból a szempontból, hogy PIN azonosítás nélkül is korlátozás nélkül lehetővé teszi a kártyabirtokos tanúsítványának (C.CH.DS) kiolvasását az EF_C_CH_DS fájlból.

6 Az eredmények alkalmazása

32 A kiértékelés és tanúsítás kiemelkedő szakértelemmel készült, ennek ellenére teljes biztonsággal nem garantálható, hogy a TOE mentes minden gyengeségtől/sebezhetőségtől. Mindazonáltal a kiértékelési/vizsgálati szint növelésével a felfedetlen kihasználható sebezhetőségek létének valószínűsége jelentősen csökken.

33 A tanúsítási jelentés a megbízó számára egy formális igazolás az elvégzett értékelésről, a felhasználó számára pedig a TOE biztonságos használatának alapja.

34 A TOE biztonságos használatára vonatkozóan a tanúsítási jelentés alábbi pontjai tartalmaznak fontos információt.

1. fejezet:	a termék pontos megnevezése és verziója A tanúsítás és a tanúsítási jelentés csak a TOE itt leírt verziójára vonatkozik.
5. fejezet	a TOE kézbesítési eljárásának meghatározása. Más kézbesítési eljárás nem nyújt az E4 bizonyossági szintnek megfelelő biztonságot.
5. fejezet	a TOE vizsgált konfigurációjának specifikálása. A TOE tanúsítása csak a leírt konfigurációkra érvényes.
5. fejezet	a TOE felhasználójára vonatkozó feltételek/megszorítások. A TOE csak ezen feltételek betartása esetén használható biztonságosan.
Függelék	a TOE Biztonsági előirányzata különösen figyelmesen kell elolvasni a TOE tervezett felhasználására, a TOE elemek felsorolására, a fenyegetettségek kivédését célzó biztonsági elemekre és az üzemeltetési környezetre vonatkozó információkat.

35 Ha a jelentésben leírt bármely feltétel nem teljesül, a kiértékelés eredménye nem teljes mértékben alkalmazható. Ez esetben további vizsgálat elvégzése szükséges annak megállapítására, hogy a megváltozott feltételek szerint a TOE milyen szinten nyújt biztonságot. A vizsgáló szervezet és a tanúsító hatóság támogatást tud nyújtani ehhez a vizsgálathoz.

36 Amennyiben a TOE, a kézbesítési eljárás vagy a működési környezet módosításra kerül, a tanúsító hatóság szabályzatában meghatározott módon újratanúsítás végezhető. Az újratanúsítás eredményei jelen tanúsítási jelentés függelékeként kerülnek dokumentálásra..

37 Amennyiben a TOE biztonságát befolyásoló új IT biztonsági felfedezések jelennek meg, a tanúsítási jelentéshez műszaki mellékletként csatolhatók.

38 A tanúsító hatóság honlapja (www.t-systems-zert.com) információt nyújt a tanúsítási jelentéshez csatolandó függelékek kibocsátásáról. A függelékek számozása folyamatos (/1, /2,...)

- Tanúsítással rendelkező, vagy kiértékelés alatt álló Új TOE verziók

Tanúsítási jelentés vége