TANÚSÍTVÁNY

A **HUNGUARD** Számítástechnikai-, informatikai kutató-fejlesztő és általános szolgáltató Kft. a 9/2005. (VII.21.) IHM rendelet alapján, mint a Magyar Köztársaság Gazdasági és Közlekedési Miniszterének 113/2007 számú kijelölési okiratával kijelölt tanúsító szervezet

tanúsítja,

hogy az **ST Incard S.r.l.** által előállított és forgalmazott

Touch&Sign2048 V1.00

intelligens kártya termék

tanúsítás tárgyát képező verziója:
A Touch&Sign2048 V1.00 SSCD alkalmazás
Touch&Sign2048 V1.00 eszköz meghajtók
Integrált áramkör és annak könyvtárai ST19WR66I az alábbi azonosítási adatokkal:
0x496E5472: MASK ID - (“InTr” ASCII-kódja)
0x00010002: ROM Code Version - (ver.01.02)
0x0180: EEPROM package CNS – (Version 1.80)

elektronikus aláírási termék
az 1. számú mellékletben részletezett feltételrendszer teljesülése esetén

megfelel

a 2001. évi XXXV. törvényben szereplő
minősített elektronikus aláírások létrehozására alkalmazható

„3-as típusú biztonságos aláírás-létrehozó eszköz”-nek.

Jelen tanúsítvány a HUNG-TJ-045-2009 számú értékelési jelentés alapján került kiadásra.
Készült a Microsec Számítástechnikai Fejlesztő Kft. megbízásából.
A tanúsítvány regisztrációs száma: **HUNG-T-045-2009.**
A tanúsítás kelte: 2009. február 23.
A tanúsítvány érvényességi ideje évenkénti felülvizsgálati eljárás mellett: 2012. február 23.
Mellékletek: feltételrendszer, követelmények, dokumentumok, összesen: 7 oldalon.

PH.

Endrődi Zsolt
Tanúsítási igazgató:

dr. Szabó István
Ügyvezető igazgató

1. számú melléklet

A tanúsítvány érvényességi feltételei

I. 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 Touch&Sign2048 V1.00 intelligens kártya szolgáltatásait igénybe vevő adminisztrátorok és felhasználók (aláírók) jól képzettek és megbízhatóak.
2. A Touch&Sign2048 V1.00 intelligens kártya szolgáltatásait igénybe vevő adminisztrátorok és felhasználók betartják a felhasználói dokumentáció (Touch&Sign2048 V1.00 – User and Administrator Guidance, Version A-2, Date: 2007-12-07, ST Incard) által a biztonságos használatra vonatkozó ajánlásokat

II. Az CC tanúsítás érvényességi feltételei

3. A CGA megvédi az aláíró nevének és az SVD-nek a hitelességét a minősített tanúsítványban a CSP fokozott biztonságú aláírása által (A.CGA).
4. Az aláíró csak megbízható SCA-t használ. Az SCA generálja és továbbítja az aláíró által aláírni kívánt adat DTBS-reprezentációját a TOE által aláírásra alkalmas formátumban (A.SCA).
5. A TOE perszonalizációja olyan fizikai és eljárásrendi intézkedések betartásával történik, amelyek biztosítják a TOE perszonalizációs adatok sértetlenségét, bizalmasságát és rendelkezésre állását. A biztonságos üzenetváltás megteremtéséhez szükséges megbízható csatornák és útvonal kialakítás szimmetrikus kulcsait biztonságos módon importálják és tárolják az SCA és CGA alkalmazások (A.PERSONALIZATION).
6. A TOE-t az Adminisztrátori útmutatóban leírtak szerint perszonalizálják és adminisztrálják, amit hozzáértő egyén végez, aki a TOE értékeinek a biztonságáért felelős és megbízható a tekintetben, hogy a jogosultságaival nem él vissza. A TOE adminisztrátor követi a TOE Adminisztrátori útmutatóban foglaltakat a TOE biztonságos megsemmisítése tekintetében, miután a TOE az SC használat vége állapotba került (A.MANAGE).
7. A TOE által igényelt pozitív azonosításhoz és hitelesítéshez szükséges információk a TOE felhasználókhoz biztonságos módon kerülnek (A.VAD).
8. A CSP csak megbízható CGA-t használ az SSCD által generált SVD számára készítendő minősített tanúsítvány generálásához (P.CSP_Qcert).

9. Az aláíró olyan aláírás létrehozó rendszert használ az adatok minősített elektronikus aláírással való ellátására, amely SSCD-vel előállított minősített tanúsítványon alapul (P.Qsign).
10. A TOE az aláírás létrehozásához használt SCD-t az aláíró kizárólagos felügyelete alatt tartja (P.Sigy_SSCD).
11. A támadásokkal szembeni nagy fokú ellenálláshoz csak a Triple DES és AES-128 algoritmusok használhatóak a hitelesítési folyamatokban. A Triple DES esetén a titkos kulcs hosszának 128-bitnek kell lennie (2 kulcs) vagy 192 bitnek (3 kulcs).
12. A generált SCD/SVD kulcspár hosszának 2048 bitnek kell lennie.
13. Bármilyen hosszú RSA kulcs generáláshoz legalább 5 bit hosszú nyilvános exponens használata szükséges, azaz értéke>=17.
14. A támadásokkal szembeni nagy fokú ellenálláshoz csak a Triple DES és AES-128 algoritmusok javasoltak szimmetrikus kriptográfiai algoritmusként. A Triple DES esetén a titkos kulcs hosszának 128-bitnek kell lennie (2 kulcs) vagy 192 bitnek (3 kulcs).
15. Az SCA által végrehajtott lenyomatkészítés használhatja az SHA-1 vagy SHA-256 algoritmust, de ez utóbbi használata javasolt.
16. A PIN kód értéke nem lehet kevesebb hat jegynél.
17. Az aláírási művelet előtt az aláírónak és az SCA-nak azonosítania és hitelesítenie kell magát.

III. A biztonságos aláírás-létrehozó eszközként történő használhatóság kiegészítő feltételei

Egy minősített aláírásokat létrehozó aláírónak a Touch&Sign2048 V1.00 intelligens kártya felhasználása során az alábbi kiegészítő feltételeket is be kell tartania:

18. A BALE-ként használt Touch&Sign2048 V1.00 intelligens kártyának csak egy felhasználója lehet, az aláíró.
19. Az aláírónak meg kell győződnie arról, hogy a kártyát még nem használták. (Ehhez a kibocsátónak megfelelő útmutatót kell biztosítani.)
20. Az aláírónak a Touch&Sign2048 V1.00 intelligens kártyát biztonságos helyen kell őriznie és a felhasználói hitelesítő adatot titokban kell tartania.
21. A Touch&Sign2048 V1.00 intelligens kártyának használatának lezárulását követően a kártyát meg kell semmisíteni, vagy vissza kell juttatni a kibocsátóhoz.
22. A minősített aláírások létrehozására használt magánkulccsal csak minősített aláírást szabad létrehozni. (Így nem szabad fokozott biztonságú aláírás-létrehozására felhasználni.)

2. számú melléklet
TERMÉKMEGFELELŐSÉGI KÖVETELMÉNYEK
A követelményeket tartalmazó dokumentumok

Az elektronikus aláírásról szóló 2001. évi XXXV. törvény

CEN/ISSS ESign Workshop – Expert Group F: Protection Profile – Secure Signature-Creation Device Type 3, version: 1.05, EAL4+

3. számú melléklet
A tanúsításhoz figyelembe vett egyéb dokumentumok

Common Criteria for Information Technology Security Evaluation, Version 2.3, August 2005

Common Methodology for Information Technology Security Evaluation (CEM), Evaluation Methodology, Version 2.3, August 2005

BSI certification: Procedural Description (BSI 7125)

Application Notes and Interpretations of the Scheme (AIS) as relevant for the TOE, specifically:

- AIS 25, Version 3, 6 August 2007 for: CC Supporting Document, - The Application of CC to Integrated Circuits, Version 2.0, CCDB-2006-04-003, April 2006
- AIS 26, Version 3, 6 August 2007 for: CC Supporting Document, -Application of Attack Potential to Smartcards, Version 2.3, CCDB-2007-04-001, April 2007
- AIS 31, Version 1, 25 Sept. 2001 for: Functionality classes and evaluation methodology of physical random number generators
- AIS 32, Version 1, 02 July 2001, Übernahme international abgestimmter CC-Interpretationen ins deutsche Zertifizierungs-schema.
- AIS 34, Version 1.00, 1 June 2004, Evaluation Methodology for CC Assurance Classes for EAL5+
- AIS 35 ST-lite
- AIS 36, Version 1, 29 July 2002 for: CC Supporting Document, ETR-lite for Composition, Version 1.1, July 2002 and CC Supporting Document, ETR-lite for Composition: Annex A Composite smartcard evaluation, Version 1.2 March 2002
- AIS 38, Version 2.0, 28 September 2007, Reuse of evaluation results

German IT Security Certificates (BSI 7148, BSI 7149), periodically updated list published also on the BSI Web-site

Security Target BSI-DSZ-0422-2008, Touch&Sign2048 V1.00 - Security Target, Version A-3, Date 2007-03-29, ST Incard (confidential document)

Security Target BSI-DSZ-0422-2008, Touch&Sign2048 V1.00 - Security Target, Version A-3, Date 2007-03-29, ST Incard (sanitised public document)

Evaluation Technical Report for Touch&Sign2048 V1.00, Version 3, Date 2008-03-05, Evaluation Body for IT-Security of TÜV Informationstechnik GmbH (confidential document)

Schutzprofil Secure Signature-Creation Device Type 3, Version 1.05, BSI-PP-0006-2002

ETR-lite for composition ST19WR66D / ST19WR66I (EAL 5+), ITSEF of SERMA Technologies, 12.10.2006 and Surveillance Technical Report ST19WR66I, (EAL 5+), ITSEF of SERMA Technologies 25.02.2008 (confidential document)

Touch&Sign2048 V1.00 –Configuration List, Version A-1, Date: 2008-01-18, ST Incard (confidential document)

Touch&Sign2048 V1.00 – User and Administrator Guidance, Version A-2, Date: 2007-12-07, ST Incard

Bekanntmachung zur elektronischen Signatur nach dem Signaturgesetz und der Signaturverordnung (Übersicht über geeignete Algorithmen), 17. Dezember 2007, Bundesnetzagentur für Elektrizität, Gas, Telekommunikation, Post und Eisenbahnen

Protection Profile PP9806 -Smartcard - Integrated Circuit, version: 2.0, EAL4+, September 1998

ST Microelectronics, Security Target, SMD_ST19WR66_ST_05_001_V01.02

Certification Report 2006/18, ST19WR66I microcontroller, November, 7th 2006, Direction centrale de la sécurité des systèmes d'information

Security Requirements for Cryptographic Modules (FIPS PUB 140-2), NIST, 1999

Certification Report BSI-DSZ-CC-0422-2008 for Touch&Sign2048 Version 1.00 from ST Incard S.r.l.

Kérelem /a tanúsítás elvégzésére/

4. számú melléklet

Rövidítések

AES Advanced Encryption Standard (Továbbfejlesztett rejtjelezési szabvány)

CGA Certification generation application (Tanúsítvány generáló alkalmazás)

CSP Certification-Service provider (Hitelesítés szolgáltató)

DES Data Encryption Standard (Adattitkosítási szabvány)

PIN Personal Identification Number (személyi azonosító szám)

RSA Rivest-Shamir-Adleman Algorithm (RSA algoritmus)

SC Smart Card (intelligens kártya)

SCA Signature creation application (aláírás létrehozó alkalmazás)

SCD Signature creation data (aláírás létrehozó adat)

SSCD Secure Signature Creation Device (**BALE** biztonságos aláírás létrehozó eszköz)

SVD Signature verification data (aláírás ellenőrző adat)

TOE Target of Evaluation (értékelés tárgya)

VAD Verification authentication data (ellenőrző hitelesítési adat)