CERTIFICATE

HUNGUARD Informatics and IT R&D and General Service Provider Ltd. as a certification authority assigned by the assignment document No. 113/2007 of the Minister of the Ministry of Economy and Transport of the Republic of Hungary
based on the Ministry of Informatics and Communication Decree 9/2005. (VII.21)

certifies that the

Touch&Sign2048 V1.00

manufactured and sold by
ST Incard S.r.l.

electronic signature smartcard product

with the following certified components and versions:

The SSCD Application Touch&Sign2048 V1.00
The device drivers Touch&Sign2048 V1.00
The Integrated Circuit and its libraries ST19WR66I and has following identification data:
0x496E5472: MASK ID - (ASCII code for “InTr”)
0x00010002: ROM Code Version - (ver.01.02)
0x0180: EEPROM package CNS – (Version 1.80)

is suitable for

the application of creating qualified electronic signatures
according to the Act XXXV of 2001
as a Type-3 secure signature creation device

This certificate has been issued on the basis of the evaluation report HUNG-TJ-045-2009.
Produced on commission of Microsec Informatics and Development Ltd.
Registration number: **HUNG-T-45-2009.**
Date of the certification: February 23, 2009
Validity of this certificate in case of yearly revision: February 23, 2012
Annexes: conditions, requirements, documents in seven pages.

LS

Endrődi Zsolt
Certification director

dr. Szabó István
Managing director

Annex 1

Validity conditions of the certificate

I. General validity conditions

The following conditions are necessary for every usage modes (the whole general utilization scope designed by the manufacturer) for reliable and secure operation.

1. Administrators and users (signers) using Touch&Sign2048 V1.00 smartcard product's services are well-trained and reliable.
2. Administrators and users using the services of Touch&Sign2048 V1.00 smartcard observe the secure usage recommendations by ST Incard found in User and Administrator Guidance (Touch&Sign2048 V1.00 – User and Administrator Guidance, Version A-2, Date: 2007-12-07, ST Incard).

II. Validity conditions due to CC certification

3. The CGA protects the authenticity of the signatory's name and the SVD in the qualified certificate by an advanced signature of the CSP (A.CGA).
4. The signatory uses only a trustworthy SCA. The SCA generates and sends the DTBS-representation of data the signatory wishes to sign in a form appropriate for signing by the TOE (A.SCA).
5. The TOE personalization takes place with the observance of physical and procedural measures granting the integrity, confidentiality and availability of the TOE personalization data. The symmetric keys that are used to implement the trusted channels and path by the secure messaging mechanism are securely imported and stored by the SCA and the CGA applications (A.PERSONALIZATION).
6. The TOE is personalized and administered according to the Administration documentation by a competent individual who is responsible for the security of TOE assets and who is trusted not to abuse his privileges. The TOE Administrator follows the TOE Administration documentation for TOE secure disposal after it entered the SC end of use state (A.MANAGE).
7. Information needed for positive identification and authentication by the TOE is delivered to TOE users in a secure manner (A.VAD).
8. The CSP uses a trustworthy CGA to generate the qualified certificate for the SVD generated by the SSCD (P.CSP_Qcert).
9. The signatory uses a signature creation system to sign data with a qualified electronic signature that is based on a qualified certificate and that is created by an SSCD (P.Qsign).
10. The TOE implements the SCD used for signature creation under sole control of the signatory (P.Sigy_SSCD).

11. For high resistance to attacks only Triple DES and AES-128 algorithms are recommended in authentication processes. For Triple DES the secret key length must be 128-bit (2 keys) or 192-bit (3 keys).
12. The length of generated SCD/SVD key pair must be 2048 bits.
13. For the generation of RSA keys of whatever length it is recommended to use a public exponent with length at least 5 bits i.e. with value >= 17.
14. For high resistance to attacks only Triple DES and AES-128 algorithms are recommended as symmetric crypto algorithm. For Triple the secret key length must be 128-bit (2 keys) or 192-bit (3 keys)
15. The hashing performed by the SCA can use the SHA-1 or the SHA-256 algorithm,but SHA-256 is recommended.
16. The PIN code value shall not be less than six digits.
17. Before a signature operation is processed the Signatory and the SCA must be identified and authenticated in advance.

III. Supplementary conditions for qualified certification service provision

During the usage of Touch&Sign2048 V1.00 a signatory creating qualified electronic signatures must keep the following supplementary rules:

18. Touch&Sign2048 V1.00 used as an SSCD has a sole user, the signatory.
19. The signatory must confirm that the card has not been used before (for this the issuer should provide a guidance).
20. The signatory must keep the Touch&Sign2048 V1.00 smart card in a secure place and the user authentication data must be kept secret.
21. After the end of usage of Touch&Sign2048 V1.00 smart card the card must be disposed or must be returned o the issuer.
22. Private key used for creating qualified signatures must be used only for creating qualified signatures (therefore it should not be used for advanced electronic signatures).

Annex 2
PRODUCT CONFORMANCE REQUIREMENTS
Requirements document

Act XXXV of 2001 of the Republic of Hungary on electronic signature

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

Annex 3
Further documents considered during certification

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.

Request for certification

Annex 4

Acronyms

AES Advanced Encryption Standard

CGA Certification generation application

CSP Certification-Service provider

DES Data Encryption Standard

PIN Personal Identification Number

RSA Rivest-Shamir-Adleman Algorithm

SC Smart Card

SCA Signature creation application

SCD Signature creation data

SSCD Secure Signature Creation Device

SVD Signature verification data

TOE Target of Evaluation

VAD Verification authentication data