Federal Office
for Information Security

Certification Report

BSI-DSZ-CC-0422-2008

for

Touch&Sign2048
Version 1.00

from

ST Incard S.r.l.

BSI - Bundesamt für Sicherheit in der Informationstechnik, Postfach 20 03 63, D-53133 Bonn
Phone +49 (0)228 9582-0, Fax +49 (0)228 9582-5477, Infoline +49 (0)228 9582-111

Bundesamt
für Sicherheit in der
Informationstechnik

Deutsches IT-Sicherheitszertifikat

erteilt vom Bundesamt für Sicherheit in der Informationstechnik

BSI-DSZ-CC-0422-2008

Smart Card with Digital Signature Application

Touch&Sign2048
Version 1.00

from	ST Incard S.r.l.
PP Conformance:	Protection Profile Secure Signature-Creation Device Type 3, Version 1.05, BSI-PP-0006-2002
Functionality:	PP conformant plus product specific extensions Common Criteria Part 2 extended
Assurance:	Common Criteria Part 3 conformant EAL 4 augmented by AVA_MSU.3 and AVA_VLA.4

Common Criteria Arrangement for components up to EAL 4

Common Criteria

The IT product identified in this certificate has been evaluated at an accredited and licensed / approved evaluation facility using *the Common Methodology for IT Security Evaluation, Version 2.3 extended by advice of the Certification Body* for components beyond EAL 4 and guidance specific for the technology of the product for conformance to the *Common Criteria for IT Security Evaluation (CC), Version 2.3 (ISO/IEC 15408:2005)* .

This certificate applies only to the specific version and release of the product in its evaluated configuration and in conjunction with the complete Certification Report.

The evaluation has been conducted in accordance with the provisions of the certification scheme of the German Federal Office for Information Security (BSI) and the conclusions of the evaluation facility in the evaluation technical report are consistent with the evidence adduced.

This certificate is not an endorsement of the IT product by the Federal Office for Information Security or any other organisation that recognises or gives effect to this certificate, and no warranty of the IT product by the Federal Office for Information Security or any other organisation that recognises or gives effect to this certificate, is either expressed or implied.

Bonn, 09. April 2008

For the Federal Office for Information Security

IT Security Certified

SOGIS - MRA

Bernd Kowalski L.S.
Head of Department

This page is intentionally left blank.

Preliminary Remarks

Under the BSIG[1] Act, the Federal Office for Information Security (BSI) has the task of issuing certificates for information technology products.

Certification of a product is carried out on the instigation of the vendor or a distributor, hereinafter called the sponsor.

A part of the procedure is the technical examination (evaluation) of the product according to the security criteria published by the BSI or generally recognised security criteria.

The evaluation is normally carried out by an evaluation facility recognised by the BSI or by BSI itself.

The result of the certification procedure is the present Certification Report. This report contains among others the certificate (summarised assessment) and the detailed Certification Results.

The Certification Results contain the technical description of the security functionality of the certified product, the details of the evaluation (strength and weaknesses) and instructions for the user.

[1] Act setting up the Federal Office for Information Security (BSI-Errichtungsgesetz, BSIG) of 17 December 1990, Bundesgesetzblatt I p. 2834

Contents

A Certification

1 Specifications of the Certification Procedure

The certification body conducts the procedure according to the criteria laid down in the following:

- BSIG[2]
- BSI Certification Ordinance[3]
- BSI Schedule of Costs[4]
- Special decrees issued by the Bundesministerium des Innern (Federal Ministry of the Interior)
- DIN EN 45011 standard
- BSI certification: Procedural Description (BSI 7125)
- Common Criteria for IT Security Evaluation (CC), Version 2.3 (ISO/IEC 15408:2005)[5]
- Common Methodology for IT Security Evaluation, Version 2.3
- BSI certification: Application Notes and Interpretation of the Scheme (AIS)
- Advice from the Certification Body on methodology for assurance components above EAL4 (AIS 34)

2 Recognition Agreements

In order to avoid multiple certification of the same product in different countries a mutual recognition of IT security certificates - as far as such certificates are based on ITSEC or CC - under certain conditions was agreed.

---

2 Act setting up the Federal Office for Information Security (BSI-Errichtungsgesetz, BSIG) of 17 December 1990, Bundesgesetzblatt I p. 2834

3 Ordinance on the Procedure for Issuance of a Certificate by the Federal Office for Information Security (BSI-Zertifizierungsverordnung, BSIZertV) of 07 July 1992, Bundesgesetzblatt I p. 1230

4 Schedule of Cost for Official Procedures of the Bundesamt für Sicherheit in der Informationstechnik (BSI-Kostenverordnung, BSI-KostV) of 03 March 2005, Bundesgesetzblatt I p. 519

5 Proclamation of the Bundesministerium des Innern of 10 May 2006 in the Bundesanzeiger dated 19 May 2006, p. 3730

2.1 European Recognition of ITSEC/CC - Certificates

The SOGIS-Agreement on the mutual recognition of certificates based on ITSEC became effective on 3 March 1998.

This agreement was signed by the national bodies of Finland, France, Germany, Greece, Italy, The Netherlands, Norway, Portugal, Spain, Sweden, Switzerland and the United Kingdom. This agreement on the mutual recognition of IT security certificates was extended to include certificates based on the CC for all evaluation levels (EAL 1 – EAL 7). The German Federal Office for Information Security (BSI) recognises certificates issued by the national certification bodies of France and the United Kingdom within the terms of this Agreement.

The SOGIS-MRA logo printed on the certificate indicates that it is recognised under the terms of this agreement.

2.2 International Recognition of CC - Certificates

An arrangement (Common Criteria Arrangement) on the mutual recognition of certificates based on the CC evaluation assurance levels up to and including EAL 4 has been signed in May 2000 (CC-MRA). It includes also the recognition of Protection Profiles based on the CC.

As of February 2007 the arrangement has been signed by the national bodies of: Australia, Austria, Canada, Czech Republic, Denmark, Finland, France, Germany, Greece, Hungary, India, Israel, Italy, Japan, Republic of Korea, The Netherlands, New Zealand, Norway, Republic of Singapore, Spain, Sweden, Turkey, United Kingdom, United States of America. The current list of signatory nations resp. approved certification schemes can be seen on the web site: http://www.commoncriteriaportal.org

The Common Criteria Arrangement logo printed on the certificate indicates that this certification is recognised under the terms of this agreement.

This evaluation contains the components AVA_MSU.3 and AVA_VLA.4 that are not mutually recognised in accordance with the provisions of the CCRA. For mutual recognition the EAL4 components of these assurance families are relevant.

3 Performance of Evaluation and Certification

The certification body monitors each individual evaluation to ensure a uniform procedure, a uniform interpretation of the criteria and uniform ratings.

The product Touch&Sign2048 V1.00 has undergone the certification procedure at BSI.

The evaluation of the product Touch&Sign2048 V1.00 was conducted by TÜV Informationstechnik GmbH. The evaluation was completed on 7 March 2008.

The TÜV Informationstechnik GmbH is an evaluation facility (ITSEF)[6] recognised by the certification body of BSI.

For this certification procedure the sponsor and applicant is: ST Incard S.r.l.

The product was developed by: ST Incard S.r.l.

The certification is concluded with the comparability check and the production of this Certification Report. This work was completed by the BSI.

4 Validity of the certification result

This Certification Report only applies to the version of the product as indicated. The confirmed assurance package is only valid on the condition that

- all stipulations regarding generation, configuration and operation, as given in the following report, are observed,
- the product is operated in the environment described, it is specified in the following report and in the Security Target.

For the meaning of the assurance levels and the confirmed strength of functions, please refer to the excerpts from the criteria at the end of the Certification Report.

The Certificate issued confirms the assurance of the product claimed in the Security Target at the date of certification. As attack methods may evolve over time, the resistance of the certified version of the product against new attack methods can be re-assessed if required and the sponsor applies for the certified product being monitored within the assurance continuity program of the BSI Certification Scheme. It is recommended to perform a re-assessment on a regular basis.

In case of changes to the certified version of the product, the validity can be extended to the new versions and releases, provided the sponsor applies for assurance continuity (i.e. re-certification or maintenance) of the modified product, in accordance with the procedural requirements, and the evaluation does not reveal any security deficiencies.

5 Publication

The following Certification Results contain pages B-1 to B-18 and D1 to D-2.

The product Touch&Sign2048 V1.00 has been included in the BSI list of the certified products, which is published regularly (see also Internet: http:// www.bsi.bund.de). Further information can be obtained from BSI-Infoline +49 228 9582-111.

[6] Information Technology Security Evaluation Facility

Further copies of this Certification Report can be requested from the developer[7] of the product. The Certification Report may also be obtained in electronic form at the internet address stated above.

[7] ST Incard S.r.l.
Z.I. Marcianise SUD
81025 Marcianise
ITALY

B Certification Results

The following results represent a summary of

- the security target of the sponsor for the target of evaluation,
- the relevant evaluation results from the evaluation facility and
- complementary notes and stipulations of the certification body.

Contents of the certification results

1 Executive Summary

The Target of evaluation (TOE) is called Touch&Sign2048 V1.00. It is a multifunctional smartcard product that is intended to provide all capabilities required to devices involved in creating qualified electronic signatures.

The TOE is able to generate its own signature key pair. The authorized Administrator uses the CGA to initiate SCD/SVD generation and to ask the SSCD to export the SVD for generation of the corresponding certificate. The TOE holds the SVD and, before exporting the SVD to a CGA for certification purposes, it provides a trusted channel in order to maintain its integrity.

The signatory must be authenticated before signature creation is allowed. For authentication he sends his authentication data (a PIN) to the TOE using a trusted path between the interfaces device used, i.e. between a smartcard reader and the TOE. The smartcard reader is also used by the Signatory or the Administrator to change his Reference Authentication Data (RAD) held by the TOE against which the TOE verifies a user PIN and it is used by the Administrator to unblock the Signatory's Reference Authentication Data, when needed.

The data to be signed (DTBS) or their representation (DTBSR) are transferred by the SCA to the TOE only over a trusted channel in order to maintain their integrity. The same channel is used to return the signed data object (SDO) from the TOE to the SCA (see the SSCD Protection Profile [9] chapter 2.1). The TOE, when requested by the SCA, is able to generate a to be signed representation (DTBSR) using a hash function agreed as suitable according to [13].

Main Touch&Sign2048 V1.00 functionality include

- Cryptographic key generation and secure management,
- Secure signature generation with secure management of data to be signed,
- Identification and Authentication of trusted users and applications,
- Data storage and protection from modification or disclosures, as needed,
- Secure exchange of sensitive data between the TOE and a trusted applications,
- Secure exchange of sensitive data between the TOE and a trusted human interface device.

The Security Target [6] is the basis for this certification. It is based on the certified Protection Profile Secure Signature-Creation Device Type 3, Version 1.05, BSI-PP-0006-2002 [9].

The TOE security assurance requirements are based entirely on the assurance components defined in part 3 of the Common Criteria (see part C or [1], part 3 for details). The TOE meets the assurance requirements of the Evaluation Assurance Level EAL 4 augmented by AVA_MSU.3 and AVA_VLA.4.

The TOE Security Functional Requirements (SFR) relevant for the TOE are outlined in the Security Target [6] resp. [7], chapter 12.1. They are selected from Common Criteria Part 2 and some of them are newly defined. Thus the TOE is CC part 2 extended.

The Security Functional Requirements (SFR) relevant for the IT-Environment of the TOE are outlined in the Security Target [6] resp. [7], chapter 12.3.

The TOE Security Functional Requirements are implemented by the following TOE Security Functions:

TOE Security Function	Addressed issue
SF.AUTH	Authentication functions
SF.RAD	RAD management
SF.AC	Access Control
SF.KEY_GEN	Key Generation
SF.HASH	Hash computation
SF.MAC	MAC computation
SF.SIGN	Crypto functions
SF.SM	Secure Messaging
SF.OBS_A	Un-observability
SF.INT_A	TOE logical integrity
SF.DATA_ERASE	Secure destruction of the data
SF.TRANSACTION	Anti-tearing function
SF.TEST	Self Test and Audit
SF.EXCEPTION	Error message and exception
SF.LIFE_CYCLE	TOE life state management
SF.HARDWARE	TRNG and physical protection, TOE Cryptographic support

Table 1: TOE Security Funktions

For more details please refer to the Security Target [6] resp. [7], chapter 13.

The claimed TOE's strength of functions 'high' (SOF-high) for specific functions as indicated in the Security Target [6] resp. [7], chapter 15.4 is confirmed. The rating of the strength of functions does not include the cryptoalgorithms suitable for encryption and decryption (see BSIG Section 4, Para. 3, Clause 2). For details see chapter 9 of this report.

The assets to be protected by the TOE are defined in the Security Target [6] resp. [7], chapter 10.1. Based on these assets the security environment is defined in terms of assumptions, threats and policies. This is outlined in the Security Target [6] resp. [7], chapter 10.

This certification covers the following configurations of the TOE: Touch&Sign2048 V1.00. For details refer to chapter. 8 of this report.

The Certification Results only apply to the version of the product indicated in the Certificate and on the condition that all the stipulations are kept as detailed in this Certification Report. This certificate is not an endorsement of the IT product by the Federal Office for Information Security (BSI) or any other organisation that recognises or gives effect to this certificate, and no warranty of the IT product by BSI or any other organisation that recognises or gives effect to this certificate, is either expressed or implied.

2 Identification of the TOE

The Target of Evaluation (TOE) is called:

Touch&Sign2048 V1.00

The following table outlines the TOE deliverables:

No	Type	Identifier	Release	Form of Delivery
1	HW/SW	The SSCD Application Touch&Sign2048 V1.00 The devices drivers Touch&Sign2048 V1.00 The Integrated Circuit and its libraries ST19WR66I	N/A	Physical delivery
2	DOC	Touch&Sign2048 V1.00 User and Administrator guidance [12]	A-2, 2007-12-07	Document in paper or electronic format
3	OTHER	Keys required for the Personalisation	N/A	electronic format via trusted channel

Table 2: Deliverables of the TOE

The TOE is in initialisation state when it is delivered from HW developer. The prepersonalisation state comprises of TOE patching and configuration. The Perso-A state is intended for the Card Manufacturer internal use. The state in which all the files required by the application are created by the Administrator is the Perso-B state. The TOE is finished after the end of Perso-A state. The delivery to the card holder is the Personalisation Agent's responsibility. For details and definitions of the lifecycle states of the TOE please read chapter 9.3 of the Security Target [6] resp. [7] and more specifically the Guidance [12].

The TOE is initialised and pre-personalised in ST Incard S.r.l. production area before delivering to personalisation centre. The personalisation centre can be either internal or external to ST Incard S.r.l.

In case of internal personalisation TOEs are delivered by internal delivery. The company internal secured areas and an authentication key stored in the TOE grant the security and the TOE integrity.

In case of external personalisation the TOEs are packed, sealed and delivered by trusted courier. Delivery documentation, manuals and authentication keys

are delivered in electronic format via trusted channel (e.g. e-mail signed and ciphered by PGP).

3 Security Policy

The TOE is the composition of an IC, IC Dedicated Software and Smart Card Embedded Software and is intended to be used as a secure signature creation device (SSCD) for the generation of signature creation data (SCD) and the creation of qualified electronic signatures. The security policy is expressed by the set of security functional requirements and implemented by the TOE. It covers the following issues:

- physical attacks through the TOE interfaces,
- storing, copying, releasing and deriving the signature creation data by an attacker,
- forgery of the electronic signature, of the signature-verification data, or of the DTBS-representation,
- repudiation of signatures,
- misuse of the signature creation function of the TOE.

4 Assumptions and Clarification of Scope

The assumptions defined in the Security Target and some aspects of threats and organisational security policies are not covered by the TOE itself. These aspects lead to specific security objectives to be fulfilled by the TOE-Environment. The following topics are of relevance:

- 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).
- 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).
- 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).
- 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).

- Information needed for positive identification and authentication by the TOE is delivered to TOE users in a secure manner (A.VAD).

Furthermore, the Security Target [6], chapter 10.5 refers to three Organisational Security Policies in the Protection Profile [9] that state that the CSP uses a trustworthy CGA to generate the qualified certificate for the SVD generated by the SSCD (P.CSP_Qcert), that 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), and that the TOE implements the SCD used for signature creation under sole control of the signatory (P.Sigy_SSCD). Please refer to the Security Target [6], chapter 10.5 and to the Protection Profile [9], chapter 3.3 for more details.

5 Architectural Information

The TOE Touch&Sign2048 V1.00 is a multifunctional smartcard product on a smartcard integrated circuit implementing a type 3 Secure Signature Creation Device (SSCD) according to the Protection Profile [9] and defined by:

- The SSCD Application Touch&Sign2048 V1.00
- The devices drivers Touch&Sign2048 V1.00
- The Integrated Circuit and its libraries ST19WR66I
- User and Administrator guidance

Touch&Sign2048 V1.00 was developed on a ST Microelectronics microcontroller: ST19WR66I ICC, a hardware platform offering 224Kb ROM, 6Kb RAM, 66Kb of EEPROM and cryptographic support, especially designed for secure application based on high performance Public and Secret key algorithms (i.e. RSA, DES, TripleDES, AES-128). The chip includes a Modular Arithmetic Processor (MAP), based on a 1088-bit processor architecture, and a DES accelerator, both designed to speed up cryptographic calculations.

The hardware also includes a true random number generator (TRNG) compliant to both FIPS 140-2 [17] and P2 class of AIS 31 [4].

The HW platform has been certified under the French Scheme (see [16], ST19WR66I Certification Report) and it is compliant with the PP9806 Protection Profile for smartcard integrated circuit [14].

The TOE consists of hardware and embedded software which is realised in several subsystems. All incoming APDU commands are subject to initial checks by the subsystem “APDU dispatcher” and are then handed over to a subsystem in charge of the required functionality which can be:

- Identification and authentication,
- Key generation,
- Signing,
- Internal application.

These subsystems get required data from the subsystem “File System” subjected to the subsystem “Data Protection” and interact with the subsystem “Hardware Abstraction Layer” which calls functions of the IC. The entry points of every interface are denoted by function names of TOE embedded software functions (APDU commands if the interface externally visible) or by reference to the IC documentation.

The IC notifies errors to the subsystem “Error Handling” to maintain a secure TOE state.

6 Documentation

The evaluated documentation as outlined in table 2 is being provided with the product to the customer. This documentation contains the required information for secure usage of the TOE in accordance with the Security Target.

Additional obligations and notes for secure usage of the TOE as outlined in chapter 10 of this report have to be followed.

7 IT Product Testing

The evaluated TOE is the Touch&Sign2048 V1.00 consisting of:

- The SSCD Application Touch&Sign2048 V1.00
- The devices 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)

The tests are performed with the composite smartcard product consisting of the Touch&Sign2048 V1.00 embedded software by ST Incard S.r.l. implementing an SSCD type 3 application, device drivers on a ST19WR66I integrated circuit and its libraries by STMicroelectronics.

The developer has tested the 15 TSF of the TOE with 76 testing strategies which are refined into 681 individual test scenarios. All testing strategies of the TSF passed all tests of individual test scenarios so that all TSF have been successfully tested against the functional specification and the high level design of the TOE. The developer’s testing results demonstrate that the TSF perform as specified. The developer’s testing results demonstrate that the TOE performs as expected.

The evaluators have tested all 16 TSF. The evaluators have repeated developer tests and have performed own tests that cover all 16 TSF. During the evaluator’s TSF subset testing the TOE operated as specified. The evaluators

have verified the developer's test results by executing a sample of tests of the developer's test documentation.

The evaluators have performed penetration testing based on the developer's and on the evaluator's vulnerability analysis. During the evaluator's penetration testing the TOE operated as specified. In the intended environment of use the TOE does not feature exploitable vulnerabilities for attackers possessing a high attack potential if all the measures required are taken into consideration.

8 Evaluated Configuration

The TOE as a Secure Signature Creation Device (SSCD) type 3 only features one fixed configuration which cannot be altered by the user.

The TOE has a unique label associated. The label is stored in the OTP (one time programmable) memory area of the TOE and can be read by means of the commands GET DATA and GET CARD TRACEABILITY.

This certification covers the following configuration of the TOE 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)

The TOE is in initialisation state when it is delivered from the HW developer. The prepersonalisation state comprises of TOE patching and configuration. The Perso-A state is intended for the Card Manufacturer internal use. The state in which all the files required by the application are created by the Administrator is the Perso-B state. The TOE is finished after the end of Perso-A state. The delivery to the card holder is the Personalisation Agent's responsibility. The TOE is initialised and pre-personalised in the ST Incard S.r.l. production area before delivering to personalisation centre.

9 Results of the Evaluation

9.1 CC specific results

The Evaluation Technical Report (ETR), [8] was provided by the ITSEF according to the Common Criteria [1], the evaluation methodology CEM [2], the requirements of the Scheme [3] and all interpretations and guidelines of the Scheme (AIS) [4] as relevant for the TOE.

The evaluation methodology CEM [2] was used for those components used up to EAL4 extended by advice of the Certification Body for components beyond EAL 4 and guidance specific for the technology of the product [4] (AIS 34).

The following guidance specific for the technology was used:

(i) As the evaluation of the TOE was conducted as a composition evaluation, the ETR [8] includes also the evaluation results of the

composite evaluation activities in accordance with CC Supporting Document, ETR-lite for Composition: Annex A Composite smart card evaluation [4, AIS 36].

(ii) The ETR [8] builds up on the ETR-lite for Composition documents of the evaluation of the underlying hardware "ST Microelectronics microcontroller: ST19WR66I" ([16]). The ETR-lite for Composition [10] was provided by the ITSEF SERMA Technologoes according to CC Supporting Document, ETR-lite for Composition ([4, AIS 36]) and was validated by a recent re-assessment.

(iii) *For smart card specific methodology the scheme interpretations AIS 25 and AIS 26 (see [4]) were used.*

As a result of the evaluation the verdict PASS is confirmed for the following assurance components:

- All components of the class ASE
- All components of the EAL 4 package as defined in the CC (see also part C of this report)
- The components
  AVA_MSU.3 - Misuse analysis – Analysis and testing for insecure states
  AVA_VLA.4 – Vulnerability analysis – Highly resistant
  augmented for this TOE evaluation.

The evaluation has confirmed:

- for PP Conformance: Protection Profile Secure Signature-Creation Device Type 3, Version 1.05 ,BSI-PP-0006-2002 [9]
- for the functionality: PP conformant plus product specific extensions Common Criteria Part 2 extended
- for the assurance: Common Criteria Part 3 conformant EAL 4 augmented by AVA_MSU.3 and AVA_VLA.4
- The following TOE Security Functions fulfil the claimed Strength of Function high :
  SF.AUTH, SF.HASH, SF.SM, SF.HARDWARE
  In order to assess the strength of function the scheme interpretations AIS 20 and AIS 31 (see [4]) were used.

The results of the evaluation are only applicable to the TOE as defined in chapter 2 and the configuration as outlined in chapter 8 above.

9.2 Results of cryptographic assessment

The following cryptographic algorithms are used by the TOE to enforce its security policy:

- hash functions:

SHA-1 (provided by the hardware) and SHA-256, implemented by the ESW. SHA-256 is recommended.

- algorithms for the encryption and decryption:

  Triple DES with 2 or 3 keys, AES-128 or RSA with 1024-bit and 2048-bit key length. For high resistance to attacks only Triple DES and AES-128 algorithms are recommended as symmetric crypto algorithms. For Triple DES the secret key length must be 128-bit (2 keys) or 192-bit (3 keys). RSA with key length of 2048 bits is recommended.

This holds for the following security functions:

- SF.AUTH (Authentication functions),
- SF.KEY_GEN (Key Generation),
- SF.HASH (Hash computation),
- SF.MAC (MAC computation),
- SF.SIGN (Crypto functions),
- SF.SM (Secure Messaging)
- SF.HARDWARE (TRNG and physical protection, TOE Cryptographic support).

The strength of the cryptographic algorithms was not rated in the course of this evaluation (see BSIG Section 4, Para. 3, Clause 2). According to the “Bekanntmachung zur elektronischen Signatur nach dem Signaturgesetz und der Signaturverordnung (Übersicht über geeignete Algorithmen)“ [13] the algorithms are suitable for creation and verification of electronic signatures. The validity period of each algorithm is mentioned in the official catalogue [13] and summarised in chapter 10.

10 Obligations and notes for the usage of the TOE

The operational documents as outlined in table 2 contain necessary information about the usage of the TOE and all security hints therein have to be considered. The following aspects need to be fulfilled when using the TOE:

- 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).
- The length of generated SCD/SVD key pair must be 1024 or 2048 bits. As the algorithm RSA with key length of 1024-bit is regarded as sufficiently secure until the end of 2007 (see [13]), for periods later this date SCD/SVD key pair with 2048 bits have to be used.
- 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.

- 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)
- The hashing performed by the SCA can use the SHA-1 or the SHA-256 algorithm.
- The SHA-1 algorithm is, at the time this guidance is written, widely used for hashing processing. It is recommended to use the SHA-256 algorithm (see [FIPS 180-1] and [FIPS 180-2]) as the SHA-1 is regarded sufficiently secure only until the end of 2007.
- The PIN code value shall not be less than six digits.
- Before a signature operation is processed the Signatory and the SCA must be identified and authenticated in advance.

As outlined in chapter 9.2 of this report and in the Security Target, the TOE is able to use the hash functions SHA-1 and SHA-256. For encryption, decryption and for signature creation and verification the TOE uses Triple DES with 2 or 3 keys, AES-128 or RSA with 1024-bit and 2048-bit key length.

The following table describes the validity period of hash functions according to the “Bekanntmachung zur elektronischen Signatur nach dem Signaturgesetz und der Signaturverordnung (Übersicht über geeignete Algorithmen)” [13]:

Hash function	**Valid until end of**
SHA-1	2007 (transition period until end of June 2008)
SHA-256	2014

Table 3: Validity period of hash functions

As the Touch&Sign2048 V1.00 implements certain cryptographic algorithms for encryption, decryption, signature creation and verification, the following table summarizes the validity period of these algorithms as published in [13].

Algorithm with bitlength	**Valid until end of**
RSA 1024	2007 (transition period until end of March 2008)
RSA 2048	2014 or longer

Table 4: Validity period of cryptographic algorithms

Remark for table 4: A bitlength of 2048 bits for RSA is recommended for an acceptable long term security level.

For the expiry of the cryptographic algorithms please refer to the relevant and applicable national directives. The usage of the TOE within the scope of this certification is limited in accordance with the validity of the used cryptographic algorithms.

11 Security Target

For the purpose of publishing, the security target [7] of the target of evaluation (TOE) is provided within a separate document as Annex A of this report. It is a sanitised version of the complete security target [6] used for the evaluation performed. Sanitisation was performed according to the rules as outlined in the relevant CCRA policy (see AIS 35 [4]).

12 Definitions

12.1 Acronyms

AES Advanced Encryption Standard

APDU Application Protocol Data Unit, interface standard for smart cards, see ISO/IEC 7816 part 3

ATE Assurance class Test Activity

ATE_IND Independant testing

ATR Answer to Reset

AVA Assurance class Vulnerability Assessment Activity

AVA_VLA Vulnerability analysis

BSI Bundesamt für Sicherheit in der Informationstechnik / Federal Office for Information Security, Bonn, Germany

BSIG Act setting up the Federal Office for Information Security (BSI-Errichtungsgesetz, BSIG) of 17 December 1990, Bundesgesetzblatt I p. 2834

CCRA Common Criteria Recognition Arrangement

CC Common Criteria for IT Security Evaluation

CGA Certification generation application

CSP Certification-Service provider

DES Data Encryption Standard

DOC Documentation / documents

DTBS Data to be signed

DTBSR Representation of Data to be signed

EAL Evaluation Assurance Level

EEPROM Electronically Erasable Programmable Read Only Memory

ESW Embedded Software

ETR Evaluation Technical Report

HW Hardware

IC	Integrated Circuit
ID	Identification number
IMP	Implementation Representation
IT	Information Technology
ITSEF	Information Technology Security Evaluation Facility
MAC	Message Authentication Code
MAP	Modular Arithmetic Processor
OE	Operational Environment
ODP	One Time Programmable
PIN	Personal Identification Number
PP	Protection Profile
PW	Password
RAD	Reference Authentication Data
RNG	Random Number Generator
ROM	Read Only Memory
RSA	Rivest-Shamir-Adleman Algorithm
SCA	Signature creation application
SCD	Signature creation data
SDO	Signed Data Object
SF	Security Function
SFP	Security Function Policy
SFR	Security Functional Requirements
SHA	Secure Hash Algorithm
SOF	Strength of Function
SSCD	Secure Signature Creation Device
ST	Security Target
SVD	Signature verification data
SW	Software
TDES	Triple DES
TOE	Target of Evaluation
TRNG	True Random Number Generator
TSC	TSF Scope of Control
TSF	TOE Security Functions

TSP TOE Security Policy

TT Test Target

VAD Verification authentication data

12.2 Glossary

Augmentation - The addition of one or more assurance component(s) from CC Part 3 to an EAL or assurance package.

Extension - The addition to an ST or PP of functional requirements not contained in part 2 and/or assurance requirements not contained in part 3 of the CC.

Formal - Expressed in a restricted syntax language with defined semantics based on well-established mathematical concepts.

Informal - Expressed in natural language.

Object - An entity within the TSC that contains or receives information and upon which subjects perform operations.

Protection Profile - An implementation-independent set of security requirements for a category of TOEs that meet specific consumer needs.

Security Function - A part or parts of the TOE that have to be relied upon for enforcing a closely related subset of the rules from the TSP.

Security Target - A set of security requirements and specifications to be used as the basis for evaluation of an identified TOE.

Semiformal - Expressed in a restricted syntax language with defined semantics.

Strength of Function - A qualification of a TOE security function expressing the minimum efforts assumed necessary to defeat its expected security behaviour by directly attacking its underlying security mechanisms.

SOF-basic - A level of the TOE strength of function where analysis shows that the function provides adequate protection against casual breach of TOE security by attackers possessing a low attack potential.

SOF-medium - A level of the TOE strength of function where analysis shows that the function provides adequate protection against straightforward or intentional breach of TOE security by attackers possessing a moderate attack potential.

SOF-high - A level of the TOE strength of function where analysis shows that the function provides adequate protection against deliberately planned or organised breach of TOE security by attackers possessing a high attack potential.

Subject - An entity within the TSC that causes operations to be performed.

Target of Evaluation - An IT product or system and its associated administrator and user guidance documentation that is the subject of an evaluation.

TOE Security Functions - A set consisting of all hardware, software, and firmware of the TOE that must be relied upon for the correct enforcement of the TSP.

TOE Security Policy - A set of rules that regulate how assets are managed, protected and distributed within a TOE.

TSF Scope of Control - The set of interactions that can occur with or within a TOE and are subject to the rules of the TSP.

13 Bibliography

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

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

[3] BSI certification: Procedural Description (BSI 7125)

[4] 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

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

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

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

[8] 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)

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

[10] 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)

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

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

[13] 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

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

[15] ST Microelectronics, Security Target, SMD_ST19WR66_ST_05_001_V01.02

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

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

C Excerpts from the Criteria

CC Part1:

Conformance results (chapter 7.4)

„The conformance result indicates the source of the collection of requirements that is met by a TOE or PP that passes its evaluation. This conformance result is presented with respect to CC Part 2 (functional requirements), CC Part 3 (assurance requirements) and, if applicable, to a pre-defined set of requirements (e.g., EAL, Protection Profile).

The conformance result consists of one of the following:

- **CC Part 2 conformant** - A PP or TOE is CC Part 2 conformant if the functional requirements are based only upon functional components in CC Part 2.
- **CC Part 2 extended** - A PP or TOE is CC Part 2 extended if the functional requirements include functional components not in CC Part 2.

plus one of the following:

- **CC Part 3 conformant** - A PP or TOE is CC Part 3 conformant if the assurance requirements are based only upon assurance components in CC Part 3.
- **CC Part 3 extended** - A PP or TOE is CC Part 3 extended if the assurance requirements include assurance requirements not in CC Part 3.

Additionally, the conformance result may include a statement made with respect to sets of defined requirements, in which case it consists of one of the following:

- **Package name Conformant** - A PP or TOE is conformant to a pre-defined named functional and/or assurance package (e.g. EAL) if the requirements (functions or assurance) include all components in the packages listed as part of the conformance result.
- **Package name Augmented** - A PP or TOE is an augmentation of a pre-defined named functional and/or assurance package (e.g. EAL) if the requirements (functions or assurance) are a proper superset of all components in the packages listed as part of the conformance result.

Finally, the conformance result may also include a statement made with respect to Protection Profiles, in which case it includes the following:

- **PP Conformant** - A TOE meets specific PP(s), which are listed as part of the conformance result.“

CC Part 3:

Protection Profile criteria overview (chapter 8.2)

“The goal of a PP evaluation is to demonstrate that the PP is complete, consistent, technically sound, and hence suitable for use as a statement of requirements for one or more evaluatable TOEs. Such a PP may be eligible for inclusion within a PP registry.”

“Assurance Class	**Assurance Family**
Class APE: Protection Profile evaluation	TOE description (APE_DES)
	Security environment (APE_ENV)
	PP introduction (APE_INT)
	Security objectives (APE_OBJ)
	IT security requirements (APE_REQ)
	Explicitly stated IT security requirements (APE_SRE)

Table 3 - Protection Profile families - CC extended requirements ”

Security Target criteria overview (Chapter 8.3)

“The goal of an ST evaluation is to demonstrate that the ST is complete, consistent, technically sound, and hence suitable for use as the basis for the corresponding TOE evaluation.”

“Assurance Class	**Assurance Family**
Class ASE: Security Target evaluation	TOE description (ASE_DES)
	Security environment (ASE_ENV)
	ST introduction (ASE_INT)
	Security objectives (ASE_OBJ)
	PP claims (ASE_PPC)
	IT security requirements (ASE_REQ)
	Explicitly stated IT security requirements (ASE_SRE)
	TOE summary specification (ASE_TSS)

Table 5 - Security Target families - CC extended requirements ”

Assurance categorisation (chapter 7.5)

"The assurance classes, families, and the abbreviation for each family are shown in Table 1.

Assurance Class	Assurance Family
ACM: Configuration management	CM automation (ACM_AUT)
	CM capabilities (ACM_CAP)
	CM scope (ACM_SCP)
ADO: Delivery and operation	Delivery (ADO_DEL)
	Installation, generation and start-up (ADO_IGS)
ADV: Development	Functional specification (ADV_FSP)
	High-level design (ADV_HLD)
	Implementation representation (ADV_IMP)
	TSF internals (ADV_INT)
	Low-level design (ADV_LLD)
	Representation correspondence (ADV_RCR)
	Security policy modeling (ADV_SPM)
AGD: Guidance documents	Administrator guidance (AGD_ADM)
	User guidance (AGD_USR)
ALC: Life cycle support	Development security (ALC_DVS)
	Flaw remediation (ALC_FLR)
	Life cycle definition (ALC_LCD)
	Tools and techniques (ALC_TAT)
ATE: Tests	Coverage (ATE_COV)
	Depth (ATE_DPT)
	Functional tests (ATE_FUN)
	Independent testing (ATE_IND)
AVA: Vulnerability assessment	Covert channel analysis (AVA_CCA)
	Misuse (AVA_MSU)
	Strength of TOE security functions (AVA_SOF)
	Vulnerability analysis (AVA_VLA)

Table 1: Assurance family breakdown and mapping"

Evaluation assurance levels (chapter 11)

“The Evaluation Assurance Levels (EALs) provide an increasing scale that balances the level of assurance obtained with the cost and feasibility of acquiring that degree of assurance. The CC approach identifies the separate concepts of assurance in a TOE at the end of the evaluation, and of maintenance of that assurance during the operational use of the TOE.

It is important to note that not all families and components from CC Part 3 are included in the EALs. This is not to say that these do not provide meaningful and desirable assurances. Instead, it is expected that these families and components will be considered for augmentation of an EAL in those PPs and STs for which they provide utility.”

Evaluation assurance level (EAL) overview (chapter 11.1)

“Table 6 represents a summary of the EALs. The columns represent a hierarchically ordered set of EALs, while the rows represent assurance families. Each number in the resulting matrix identifies a specific assurance component where applicable.

As outlined in the next section, seven hierarchically ordered evaluation assurance levels are defined in the CC for the rating of a TOE's assurance. They are hierarchically ordered inasmuch as each EAL represents more assurance than all lower EALs. The increase in assurance from EAL to EAL is accomplished by substitution of a hierarchically higher assurance component from the same assurance family (i.e. increasing rigour, scope, and/or depth) and from the addition of assurance components from other assurance families (i.e. adding new requirements).

These EALs consist of an appropriate combination of assurance components as described in chapter 7 of this Part 3. More precisely, each EAL includes no more than one component of each assurance family and all assurance dependencies of every component are addressed.

While the EALs are defined in the CC, it is possible to represent other combinations of assurance. Specifically, the notion of “augmentation” allows the addition of assurance components (from assurance families not already included in the EAL) or the substitution of assurance components (with another hierarchically higher assurance component in the same assurance family) to an EAL. Of the assurance constructs defined in the CC, only EALs may be augmented. The notion of an “EAL minus a constituent assurance component” is not recognised by the standard as a valid claim. Augmentation carries with it the obligation on the part of the claimant to justify the utility and added value of the added assurance component to the EAL. An EAL may also be extended with explicitly stated assurance requirements.

Assurance Class	Assurance Family	Assurance Components by Evaluation Assurance Level						
		EAL1	EAL2	EAL3	EAL4	EAL5	EAL6	EAL7
Configuration management	ACM_AUT				1	1	2	2
	ACM_CAP	1	2	3	4	4	5	5
	ACM_SCP			1	2	3	3	3
Delivery and operation	ADO_DEL		1	1	2	2	2	3
	ADO_IGS	1	1	1	1	1	1	1
Development	ADV_FSP	1	1	1	2	3	3	4
	ADV_HLD		1	2	2	3	4	5
	ADV_IMP				1	2	3	3
	ADV_INT					1	2	3
	ADV_LLD				1	1	2	2
	ADV_RCR	1	1	1	1	2	2	3
	ADV_SPM				1	3	3	3
Guidance documents	AGD_ADM	1	1	1	1	1	1	1
	AGD_USR	1	1	1	1	1	1	1
Life cycle support	ALC_DVS			1	1	1	2	2
	ALC_FLR							
	ALC_LCD				1	2	2	3
	ALC_TAT				1	2	3	3
Tests	ATE_COV		1	2	2	2	3	3
	ATE_DPT			1	1	2	2	3
	ATE_FUN		1	1	1	1	2	2
	ATE_IND	1	2	2	2	2	2	3
Vulnerability assessment	AVA_CCA					1	2	2
	AVA_MSU			1	2	2	3	3
	AVA_SOF		1	1	1	1	1	1
	AVA_VLA		1	1	2	3	4	4

Table 6: Evaluation assurance level summary”

Evaluation assurance level 1 (EAL1) - functionally tested (chapter 11.3)

“Objectives

EAL1 is applicable where some confidence in correct operation is required, but the threats to security are not viewed as serious. It will be of value where independent assurance is required to support the contention that due care has been exercised with respect to the protection of personal or similar information.

EAL1 provides an evaluation of the TOE as made available to the customer, including independent testing against a specification, and an examination of the guidance documentation provided. It is intended that an EAL1 evaluation could be successfully conducted without assistance from the developer of the TOE, and for minimal outlay.

An evaluation at this level should provide evidence that the TOE functions in a manner consistent with its documentation, and that it provides useful protection against identified threats.”

Evaluation assurance level 2 (EAL2) - structurally tested (chapter 11.4)

“Objectives

EAL2 requires the co-operation of the developer in terms of the delivery of design information and test results, but should not demand more effort on the part of the developer than is consistent with good commercial practice. As such it should not require a substantially increased investment of cost or time.

EAL2 is therefore applicable in those circumstances where developers or users require a low to moderate level of independently assured security in the absence of ready availability of the complete development record. Such a situation may arise when securing legacy systems, or where access to the developer may be limited.”

Evaluation assurance level 3 (EAL3) - methodically tested and checked (chapter 11.5)

“Objectives

EAL3 permits a conscientious developer to gain maximum assurance from positive security engineering at the design stage without substantial alteration of existing sound development practices.

EAL3 is applicable in those circumstances where developers or users require a moderate level of independently assured security, and require a thorough investigation of the TOE and its development without substantial re-engineering.”

Evaluation assurance level 4 (EAL4) - methodically designed, tested, and reviewed (chapter 11.6)

“Objectives

EAL4 permits a developer to gain maximum assurance from positive security engineering based on good commercial development practices which, though rigorous, do not require substantial specialist knowledge, skills, and other resources. EAL4 is the highest level at which it is likely to be economically feasible to retrofit to an existing product line.

EAL4 is therefore applicable in those circumstances where developers or users require a moderate to high level of independently assured security in conventional commodity TOEs and are prepared to incur additional security-specific engineering costs.”

Evaluation assurance level 5 (EAL5) - semiformally designed and tested (chapter 11.7)

“Objectives

EAL5 permits a developer to gain maximum assurance from security engineering based upon rigorous commercial development practices supported by moderate application of specialist security engineering techniques. Such a TOE will probably be designed and developed with the intent of achieving EAL5 assurance. It is likely that the additional costs attributable to the EAL5 requirements, relative to rigorous development without the application of specialised techniques, will not be large.

EAL5 is therefore applicable in those circumstances where developers or users require a high level of independently assured security in a planned development and require a rigorous development approach without incurring unreasonable costs attributable to specialist security engineering techniques.”

Evaluation assurance level 6 (EAL6) - semiformally verified design and tested (chapter 11.8)

“Objectives

EAL6 permits developers to gain high assurance from application of security engineering techniques to a rigorous development environment in order to produce a premium TOE for protecting high value assets against significant risks.

EAL6 is therefore applicable to the development of security TOEs for application in high risk situations where the value of the protected assets justifies the additional costs.”

Evaluation assurance level 7 (EAL7) - formally verified design and tested (chapter 11.9)

“Objectives

EAL7 is applicable to the development of security TOEs for application in extremely high risk situations and/or where the high value of the assets justifies the higher costs. Practical application of EAL7 is currently limited to TOEs with tightly focused security functionality that is amenable to extensive formal analysis.“

Strength of TOE security functions (AVA_SOF) (chapter 19.3)

“Objectives

Even if a TOE security function cannot be bypassed, deactivated, or corrupted, it may still be possible to defeat it because there is a vulnerability in the concept of its underlying security mechanisms. For those functions a qualification of their security behaviour can be made using the results of a quantitative or statistical analysis of the security behaviour of these mechanisms and the effort required to overcome them. The qualification is made in the form of a strength of TOE security function claim.”

Vulnerability analysis (AVA_VLA) (chapter 19.4)

"Objectives

Vulnerability analysis is an assessment to determine whether vulnerabilities identified, during the evaluation of the construction and anticipated operation of the TOE or by other methods (e.g. by flaw hypotheses), could allow users to violate the TSP.

Vulnerability analysis deals with the threats that a user will be able to discover flaws that will allow unauthorised access to resources (e.g. data), allow the ability to interfere with or alter the TSF, or interfere with the authorised capabilities of other users.”

"Application notes

A vulnerability analysis is performed by the developer in order to ascertain the presence of security vulnerabilities, and should consider at least the contents of all the TOE deliverables including the ST for the targeted evaluation assurance level. The developer is required to document the disposition of identified vulnerabilities to allow the evaluator to make use of that information if it is found useful as a support for the evaluator's independent vulnerability analysis.”

“Independent vulnerability analysis goes beyond the vulnerabilities identified by the developer. The main intent of the evaluator analysis is to determine that the TOE is resistant to penetration attacks performed by an attacker possessing a low (for AVA_VLA.2 Independent vulnerability analysis), moderate (for AVA_VLA.3 Moderately resistant) or high (for AVA_VLA.4 Highly resistant) attack potential.”

D Annexes

List of annexes of this certification report

Annex A: Security Target provided within a separate document.

This page is intentionally left blank.