Certification Report

Bundesamt für Sicherheit in der Informationstechnik

BSI-DSZ-CC-0202-2005

for

InCrypto34v2

from

ST INCARD S. r. l.

BSI - Bundesamt für Sicherheit in der Informationstechnik, Postfach 20 03 63, D-53133 Bonn
Phone +49 228 9582-0, Fax +49 228 9582-455, Infoline +49 228 9582-111

Deutsches IT-Sicherheitszertifikat

erteilt vom

Bundesamt für Sicherheit in der Informationstechnik

Bundesamt für Sicherheit
in der Informationstechnik

IT Security Certified

SOGIS-MRA

BSI-DSZ-CC-0202-2005

Secure Signature Creation Device

InCrypto34v2

from

ST INCARD S. r. l.

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, Part 1 Version 0.6*, *Part 2 Version 1.0* extended by advice of the Certification Body for components beyond EAL4 and smart card specific guidance for conformance to the *Common Criteria for IT Security Evaluation, Version 2.1 (ISO/IEC 15408:1999)* and including final interpretations for compliance with Common Criteria Version 2.2 and Common Methodology Part 2, Version 2.2.

Evaluation Results:

PP Conformance:	**Protection Profile BSI-PP-0006-2002**
Functionality:	**PP BSI-PP-0006-2002 conformant plus product specific extensions** **Common Criteria Part 2 extended**
Assurance Package:	**Common Criteria Part 3 conformant** **EAL4 augmented by** AVA_MSU.3 (Vulnerability assessment - Analysis and testing for insecure states) AVA_VLA.4 (Vulnerability assessment - Highly resistant)

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.

The notes mentioned on the reverse side are part of this certificate.

Bonn, 02. February 2005

The President of the Federal Office
for Information Security

Common Criteria

Dr. Helmbrecht L.S.

Bundesamt für Sicherheit in der Informationstechnik
Godesberger Allee 185-189 - D-53175 Bonn - Postfach 20 03 63 - D-53133 Bonn
Phone +49 228 9582-0 - Fax +49 228 9582-455 - Infoline +49 228 9582-111

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)

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.

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 2.1[5]
- Common Methodology for IT Security Evaluation (CEM)
  - Part 1, Version 0.6
  - Part 2, Version 1.0
- BSI certification: Application Notes and Interpretation of the Scheme (AIS)
- Advice from the Certification Body on methodology for assurance components above EAL4

The use of Common Criteria Version 2.1, Common Methodology, part 2, Version 1.0 and final interpretations as part of AIS 32 results in compliance of the certification results with Common Criteria Version 2.2 and Common Methodology Part 2, Version 2.2 as endorsed by the Common Criteria recognition arrangement committees.

---

[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 7 July 1992, Bundesgesetzblatt I p. 1230

[4] Schedule of Cost for Official Procedures of the Federal Office for Information Security (BSI-Kostenverordnung, BSI-KostV) of 29th October 1992, Bundesgesetzblatt I p. 1838

[5] Proclamation of the Bundesministerium des Innern of 22nd September 2000 in the Bundesanzeiger p. 19445

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.

2.1 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).

2.2 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 was signed in May 2000. It includes also the recognition of Protection Profiles based on the CC. The arrangement was signed by the national bodies of Australia, Canada, Finland France, Germany, Greece, Italy, The Netherlands, New Zealand, Norway, Spain, United Kingdom and the United States. Israel joined the arrangement in November 2000, Sweden in February 2002, Austria in November 2002, Hungary and Turkey in September 2003, Japan in November 2003.

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 InCrypto34v2, a smartcard product implementing a SSCD type 3 device has undergone the certification procedure at BSI.

The evaluation of the product InCrypto34v2 was conducted by TÜV Informationstechnik GmbH. The TÜV Informationstechnik GmbH is an evaluation facility (ITSEF)[6] recognised by BSI.

The sponsor and vendor and distributor is:

ST INCARD S. r. l.
Z.I. Marcianise Sud
81025 Marcianise (CE)
Italia

The certification is concluded with

- the comparability check and
- the production of this Certification Report.

This work was completed by the BSI on 02.02.2005.

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, where specified in the following report.

This Certification Report only applies to the version of the product indicated here. The validity can be extended to new versions and releases of the product, provided the sponsor applies for re-certification of the modified product, in accordance with the procedural requirements, and the evaluation does not reveal any security deficiencies.

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.

[6] Information Technology Security Evaluation Facility

4 Publication

The following Certification Results contain pages B-1 to B-22.

The product InCrypto34v2 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 0228/9582-111.

Further copies of this Certification Report can be requested from the vendor[7] of the product. The Certification Report can also be downloaded from the above-mentioned website.

[7] ST INCARD S. r.l.
Z.I. Marcianise Sud
81025 Marcianise (CE)
Italia

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 InCrypto34v2. InCrypto34v2 will be used to provide all capabilities required to devices involved in creating qualified electronic signatures.

The TOE comprises of following components:

- The SSCD Application INCRYPTO34 V2.00
- The INCRYPTO34 devices drivers INCRYPTO34 V2.00
- The Integrated Circuit and its libraries ST19XL34P
- User and Administrator guidance

Figure 1 gives an overview of the components of the TOE and its structural view while figure 2 shows the functional scope of the TOE.

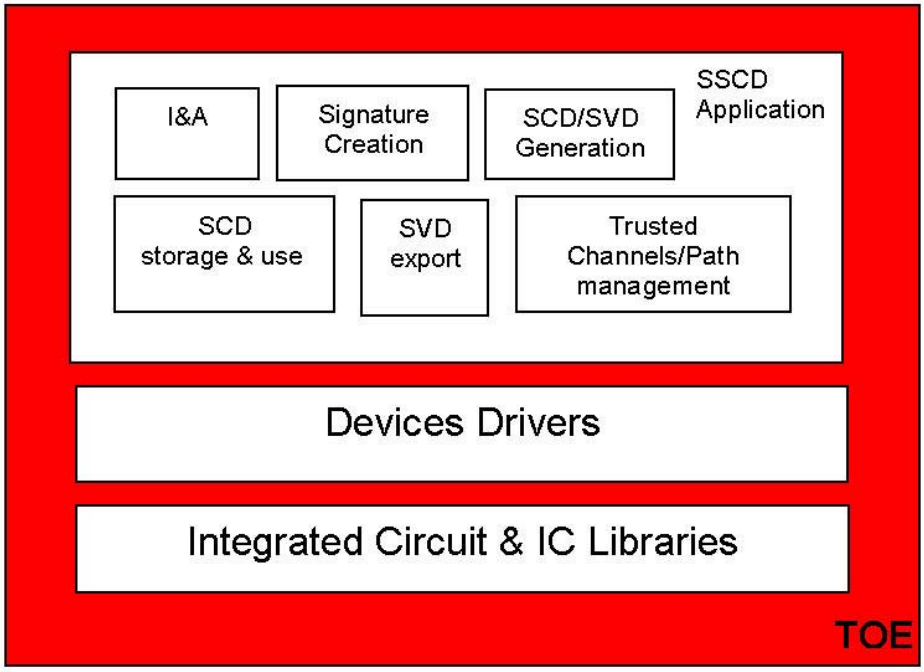

Figure 1: TOE components

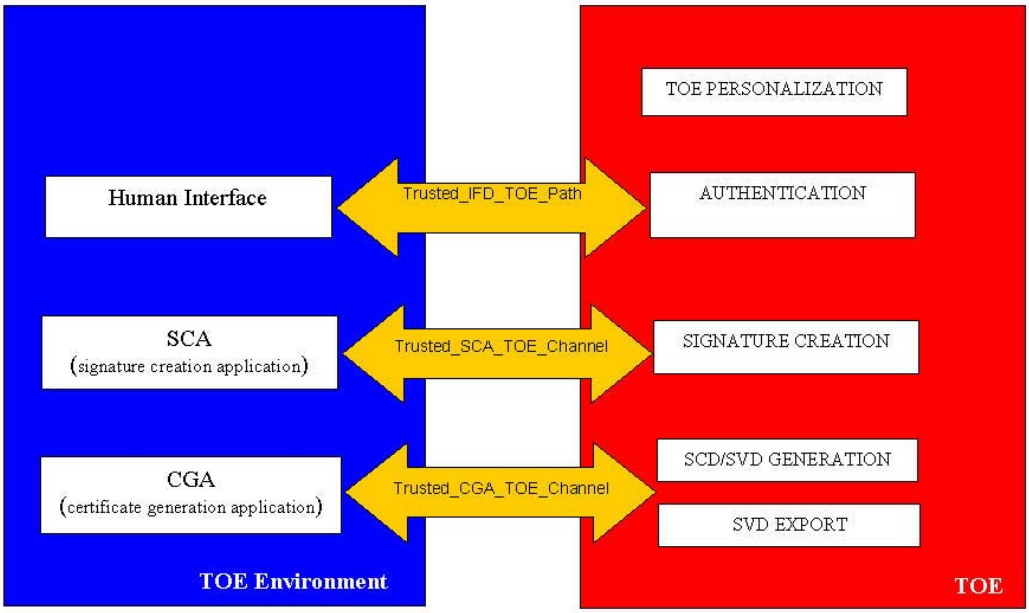

Figure 2: TOE scope and boundaries

After its personalisation the TOE is able to perform the signature operation under sole control of the signatory using the RSA cryptographic algorithm and the parameters agreed as suitable according to [17]. It has to be securely personalised by a trusted and competent administrator according to User and Administrator Documentation [14].

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 signatures 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 [12] chapter 2.1). The TOE, when requested by the SCA, is able to generate data to be signed representation (DTBSR) using a hash function agreed as suitable according to [17].

The embedded SW of the TOE is structured on two layers consisting of the devices drivers and the SSCD application, in which SW functions are implemented as APDU commands compliant with ISO/IEC 7816- part 4 and 8 [18] (see figure 2 of this report).

The evaluation of the TOE was conducted as a composition evaluation making use of the platform evaluation results of the CC evaluation of the underlying semiconductor "ST19XL34P microcontroller" provided by ST Microelectronics [9]. The IC was evaluated according to Common Criteria EAL 4 augmented and with a minimum strength level for its security functions of SOF-high for specific functionality. The evaluation is based on the Protection Profile PP/9806, Smart Card Integrated Circuit Version 2.0, Issue September 1998 [11] and as outlined in [10]. This platform evaluation was performed by the ITSEF of SERMA Terchologies. The certificate was provides by the French Direction centrale de la sécurité des systèmes d'information.

The embedded Software of InCrypto34v2 and the overall composition were evaluated by TÜV Informationstechnik GmbH.

The evaluation was completed on 22.12.2004. The TÜV Informationstechnik GmbH is an evaluation facility (ITSEF)[8] recognised by BSI.

The concept for composition as outlined in CC Supporting Document AIS 36 [4] was used.

The sponsor and vendor and distributor is

ST INCARD S. r. l.
Z.I. Marcianise Sud
81025 Marcianise (CE)
Italia.

1.1 Assurance package

The TOE security assurance requirements are based entirely on the assurance components defined in part 3 of the Common Criteria (see Annex C or [1], part 3 for details). The TOE meets the assurance requirements of assurance level EAL4+ (Evaluation Assurance Level 4 augmented). The following table shows the augmented assurance components.

Requirement	Identifier
EAL4	TOE evaluation: Methodically designed, tested and reviewed
+ AVA_MSU.3	Vulnerability assessment - Analysis and testing for insecure states
+ AVA_VLA.4	Vulnerability assessment – Highly resistant

Table 1: EAL-augmentation of Assurance Components

[8] Information Technology Security Evaluation Facility

1.2 Functionality

The TOE Security Functional Requirements (SFR) selected in the Security Target are Common Criteria Part 2 extended as shown in the following tables.

The following SFRs are taken from CC Part 2:

Security Functional Requirement	**Identifier**
FCS	**Cryptographic support**
FCS_CKM.1	Cryptographic key generation
FCS_CKM.4	Cryptographic key destruction
FCS_COP.1	Cryptographic operation
FDP	**User data protection**
FDP_ACC.1	Subset access control
FDP_ACF.1	Security attribute based access control
FDP_ETC.1	Export of user data without security attributes
FDP_ITC.1	Import of user data without security attributes
FDP_RIP.1	Subset residual information protection
FDP_SDI.2	Stored data integrity monitoring and action
FDP_UIT.1	Data exchange integrity
FIA	**Identification and Authentication**
FIA_AFL.1	Authentication failure handling
FIA_ATD.1	User attribute definition
FIA_UAU.1	Timing of authentication
FIA_UID.1	Timing of identification
FMT	**Security Management**
FMT_MOF.1	Management of security functions behaviour
FMT_MSA.1	Management of security attributes
FMT_MSA.2	Secure security attributes
FMT_MSA.3	Static attribute initialisation
FMT_MTD.1	Management of TSF data
FMT_SMF.1	Specification of management functions
FMT_SMR.1	Security roles
FPT	**Protection of the TOE Security Functions**
FPT_AMT.1	Abstract machine testing
FPT_FLS.1	Failure with preservation of secure state
FPT_PHP.1	Passive detection of physical attack
FPT_PHP.3	Resistance to physical attack

FPT_TST.1	TSF testing
FTP	**Trusted Path/Channels**
FTP_ITC.1	Inter-TSF trusted channel
FTP_TRP.1	Trusted path

Table 2: SFRs taken from CC Part 2

The following CC part 2 extended SFR is defined.

Security Functional Requirement	**Identifier**
FPT	**Protection of the TOE Security Functions**
FPT_EMSEC.1	TOE Emanation

Table 3: SFRs CC part 2 extended.

Note: Only the titles of the Security Functional Requirements are provided. For more details please refer to the Security Target [6], chapter 5.

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

TOE Security Functions	**Description**
Identification and Authentication	
SF.AUTH	Authentication functions
SF.RAD	RAD management
Access Control	
SF.AC	Access control
Key Management and Cryptography	
SF.KEY_GEN	Key generation
SF.HASH	Hash computation
SF.MAC	MAC computation
SF.SIGN	Crypto functions
Secure Messaging	
SF.SM	Secure messaging
Stored Data Protection	
SF.OBS_A	Un-observability
SF.INT_A	TOE logical integrity
SF.DATA_ERASE	Secure destruction of the data
SF.TRANSACTION	Anti-tearing function
Test	

TOE Security Functions	Description
SF.TEST	Self test and audit
Failure	
SF.EXCEPTION	Error message and exception
TOE Life Cycle	
SF.LIFE_CYCLE	TOE life phase management

Table 4: TOE Security Functions

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

1.3 Strength of Function

The TOE's strength of functions is rated 'high' (SOF-high) for those functions, identified in the Security Target [6], chapter 8.4, TOE Strength of Function Claim. 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) (see also Chapter 9 of this report).

1.4 Summary of threats and Organisational Security Policies (OSPs) addressed by the evaluated IT product

The threats and Organisational Security Policies (OSPs) which were assumed for the evaluation and averted by the TOE are specified in the BSI-PP-0006-2002 [12] and mentioned in the Security Target [6]:

Name	Definition
T.Hack_Phys	Physical attacks through the TOE interfaces
T.SCD_Divulg	Storing, copying, and releasing of the signature creation data
T.SCD_Derive	Derive the signature creation data
T.Sig_Forgery	Forgery of the electronic signature
T.Sig_Repud	Repudiation of signatures
T.SVD_Forgery	Forgery of the signature-verification data
T.DTBS_Forgery	Forgery of the DTBS-representation
T.SigF_Misuse	Misuse of the signature creation function of the TOE

Table 5: Threats for the TOE

Name	Definition
P.CSP_Qcert	Qualified certificate

Name	Definition
P.Qsign	Qualified electronic signatures
P.Sigy_SSCD	TOE as secure signature creation device

Table 6: OSPs

Note: Only the titles of the threats and OSPs are provided. For more details please refer to the Security Target [6], chapter 3.5 and to the Protection Profile BSI-PP-0006-2002 [12], chapter 3.3.

1.5 Special configuration requirements

The TOE lifecycle phases are described in the Security Target [6] and are compliant to the Protection Profile [12]. The TOE is initialised and pre-personalised in the ST-Incard S.r.l. production area before its delivery to a personalisation centre. Only TOEs in personalisation mode are delivered. For personalisation, the administrator has to follow the User and Administrator Guidance [14] chapter 10 to ensure that the TOE is able to perform all security functionality as defined in the Security Target [6] and Protection Profile [12].

In particular, the

- Authentication processes and secure messaging must use Triple DES algorithm with secret key lengths 128-bit (2 keys) or 192-bit (3 keys)
- Signature creation keys must be generated with a length of 1024-bit
- PIN and PUK code values must have a length of at least 6 and an error counter of 3
- Signatory and the SCA must be identified and authenticated before a signature operation is processed.

This latter issue is particularly important for compliance with the Signature Creation Policy of the Secure Signature Creation Device defined in the Security Target [6] based on the Protection Profile [12]. Therefore, the administrator has to set up the secure file system during personalisation as described in User and Administrator Guidance [14], chapter 10.2 and the related object creation scenarios as described in the same document [14], chapter 10.3 in order to comply with this constraint. The issuer has to verify that the guidance is followed.

1.6 Assumptions about the operating environment

Since the Security Target claims conformance to the Protection Profile [12], the assumptions defined in section 3.1 of the Protection Profile are valid for the Security Target of this TOE. Additionally, there are three more assumptions defined in the Security Target [6]. The following constraints concerning the operating environment are made in the Protection Profile and in Security Target, please refer to the Security Target [6], chapter 3.4:

A.CGA Trustworthy certification-generation application

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.SCA Trustworthy signature creation application

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.PERSONALIZATION Trustworthy personalization

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.MANAGE Trustworthy administration of the TOE

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.VAD Trustworthy VAD transport

Information needed for positive identification and authentication by the TOE is delivered to TOE users in a secure manner.

1.7 Disclaimers

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:

InCrypto34v2, smartcard product implementing an SSCD type 3 device

The TOE consisting of the ST Microelectronics ST19XL34P IC together with its libraries including a cryptographic library, the INCRYPTO34 V2.00 ROM mask

and the PD/P6 register patch incorporated in the CNS V1.03 package as described in the configuration list [13] and which realises an Italian national service card (CNS) product.

The following table outlines the TOE deliverables:

No	Type	Name
1	HW/SW	Smartcard integrated circuit ST19XL34P by ST Microelectronics
2	SW	Smartcard embedded software InCrypto34v2 consisting of - SSCD application INCRYPTO34 V2.00 and - The INCRYPTO34 device drivers INCRYPTO34 V2.00
3	Doc	InCrypto34v2 USER and ADMINISTRATOR GUIDANCE [14]

Table 7: TOE Deliverables

The User and Administrator Guidance [14] is only delivered to the smart card issuer, an application developer of certification generation applications (CGA) and signature creation applications (SCA) and the personalisation centre, as applicable, whereas the signatory has to receive adequate information on secure TOE usage as provided in the guidance [14], chapter 10.3.

The TOE can be uniquely identified by a string of bytes known as the ATR according to [14], chapter 5, and by its product identification data described in the guidance [14], chapter 5 and chapter 10.1, respectively. The TOE product identification data consists of 2 bytes identifying the ROM mask ID and EEPROM loaded package ID.

On reset the TOE replies in the T=0 communication protocol with its default ATR data in hexadecimal notation (0x) as described in [14], chapter 5, Table 28:

0x 3B C4 FF 00 00 31 80 00

3 Security Policy

The TOE is the composition of an IC, IC Dedicated Software and Smart Card Embedded Software and will be used as a secure signature creation device (SSCD) for the creation of qualified electronic signatures. It is able to generate its own signature keys (the SCD/SVD pair) and performs the signature operation using the RSA cryptographic algorithm and the parameters agreed as suitable according to [6]. The security policy is to provide protection against

- 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

4.1 Usage assumptions

General assumptions are made based on the PP [12] as well as the Security Target [6] chapter 3.4.

In order to ensure that the TOE is able to perform all security functionality as defined in the Security Target [6] and Protection Profile [12] the administrator has to follow the User and Administrator guidance [14] and comply with the recommendations for a secure TOE use as provided in [14], chapter 10.3 including secure messaging requirements and TOE activation.

4.2 Environmental assumptions

The following assumptions about physical and connectivity aspects defined by the Security Target have to be met (refer to Security Target [6], chapter 3.4):

- 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 3.3 refers to three Organisational Security Policies in the Protection Profile [12] 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 3.3 and to the Protection Profile [12], chapter 3.3 for more details.

4.3 Clarification of scope

Additional threats that are not countered by the TOE and its evaluated security functions were not addressed by this product evaluation.

5 Architectural Information

The TOE (InCrypto34v2) is a secure signature creation device comprising an integrated circuit (IC) together with its libraries and a smartcard embedded software consisting of SSCD application and device drivers. An overview of the architecture is given in section 2 of the Security Target [6]. A top level block diagram can be found in figure 1 of this report and in chapter 2 of the Security Target [6]. The TOE is the composition of an IC and Smart Card Embedded Software. A top level block diagram of the hardware IC can be found within the TOE description of the Security Target of the chip [9], chapter 2.

6 Documentation

The following documentation is provided with the product by the developer to the customer (see also table 7 of this report):

- InCrypto34v2 User and Administrator Guidance, version A-8, dated 23.11.2004 ST Incard, [14]

7 IT Product Testing

The developer tested all 15 TSFs and related sub-functions and subsystems to assure coverage of all SFRs. The developer has tested the TOE systematically at the level of TSF functionality as given in the Functional Specification [15] and at the level of the subsystems as given in the High Level Design document [16]. Test cases covered in test suites for automated testing are implemented in accordance with [15] and with [14] in order to verify the TOE's compliance with its expected behaviour. Validation tests of the TOE were performed on a smartcard emulator and on real cards. The tests are performed on APDU level. All test cases in each test suite were run successfully on the evaluated TOE version. The developer's testing results demonstrate that the TSFs perform as specified and that the TOE performs as expected from [15] and [16].

Evaluator testing was performed on TOE smart cards whenever possible as well as with a TOE emulator. Tests were performed in the TOE development

environment on an emulator and on smart cards using script based developer test tools with an automated comparison of expected and actual test results and within the premises of the ITSEF where the TOE was tested in the form of smart cards using test scripts. The evaluator has chosen a sample of developer tests to be repeated that cover test scenarios of all TSF. The independent tests covered a subset of all TSF as well.

The evaluator has performed penetration testing based on the developer vulnerability analysis and independent penetration testing based on the independent vulnerability analysis. During the evaluator's penetration testing the TOE operated as specified. The evaluator's penetration testing on the composite TOE considered the implemented security measures required by the HW evaluation.

During the evaluator's penetration testing no information leakage of the TOE could be observed. The evaluator testing took into account recommendations of the ETR lite for the hardware IC [8], chapter 6.2 by verifying that the developer recommendations have been implemented in the composite TOE. The ITSEF performing the composite evaluation verified that the side channel analysis of the hardware IC with its embedded ROM software including its cryptographic library as outlined in [8] is still valid. The independently identified vulnerabilities were tested with regard to their exploitation. Security measures required for the composite TOE by the IC evaluation are effectively implemented. The results of the evaluator's independent vulnerability analysis and penetration testing showed that the TOE is resistant to attackers with high attack potential.

8 Evaluated Configuration

The tests are performed with the composite smartcard product consisting of the InCrypto34 V2.00 embedded software by ST INCARD S.r.l. realising an SSCD type 3 application and device drivers on a ST19XL34P integrated circuit and its libraries by ST Microelectronics. The composite smartcard TOE was tested in the package CNS V1.03 which realises an Italian electronic ID card. The TOE is delivered from the smart card manufacturer as one fixed configuration to the personalization centre which writes user specific data into the TOE during the personalisation process without changing the TOE configuration.

9 Results of the Evaluation

The Evaluation Technical Report (ETR) [7] was provided by the ITSEF TÜV Informationstechnik GmbH according to the Common Criteria [1], the Methodology [2], the requirements of the Scheme [3] and all interpretations and guidelines of the Scheme (AIS) [4] as relevant for the TOE.

As the evaluation of the TOE was conducted as a composition evaluation, the ETR [7] 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, AIS 36 [4].

The ETR [7] builds up on the ETR-lite for Composition documents of the evaluations of the underlying hardware ST Microelectronics "ST19XL34P" ([8]). The ETR-lite for Composition documents was provided by the ITSEF of SERMA Technologies.

The evaluation methodology CEM [2] was used for those components identical with EAL4. For components beyond EAL4 the methodology was defined in co-ordination with the Certification Body.

The verdicts for the CC, Part 3 assurance components (according to EAL4 augmented and the class ASE for the Security Target evaluation) are summarised in the following table.

Assurance classes and components		**Verdict**
Security Target evaluation	CC Class ASE	PASS
TOE description	ASE_DES.1	PASS
Security environment	ASE_ENV.1	PASS
ST introduction	ASE_INT.1	PASS
Security objectives	ASE_OBJ.1	PASS
PP claims	ASE_PPC.1	PASS
IT security requirements	ASE_REQ.1	PASS
Explicitly stated IT security requirements	ASE_SRE.1	PASS
TOE summary specification	ASE_TSS.1	PASS
Configuration management	CC Class ACM	PASS
Partial CM automation	ACM_AUT.1	PASS
Generation support and acceptance procedures	ACM_CAP.4	PASS
Problem tracking CM coverage	ACM_SCP.2	PASS
Delivery and operation	CC Class ADO	PASS
Detection of modification	ADO_DEL.2	PASS
Generation log	ADO_IGS.1	PASS
Development	CC Class ADV	PASS
Fully defined external interfaces	ADV_FSP.2	PASS
Security enforcing high-level design	ADV_HLD.2	PASS
Implementation of the TSF	ADV_IMP.1	PASS
Descriptive low-level design	ADV_LLD.1	PASS
Informal correspondence demonstration	ADV_RCR.1	PASS
Informal TOE security policy model	ADV_SPM.1	PASS
Guidance documents	CC Class AGD	PASS

Assurance classes and components		Verdict
Administrator guidance	AGD_ADM.1	PASS
User guidance	AGD_USR.1	PASS
Life cycle support	CC Class ALC	PASS
Identification of security measures	ALC_DVS.1	PASS
Developer defined life-cycle model	ALC_LCD.1	PASS
Well-defined development tools	ALC_TAT.1	PASS
Tests	CC Class ATE	PASS
Analysis of coverage	ATE_COV.2	PASS
Testing: low-level design	ATE_DPT.1	PASS
Functional testing	ATE_FUN.1	PASS
Independent testing - sample	ATE_IND.2	PASS
Vulnerability assessment	CC Class AVA	PASS
Validation of analysis	**AVA_MSU.3**	PASS
Strength of TOE security function evaluation	AVA_SOF.1	PASS
Highly resistant	**AVA_VLA.4**	PASS

Table 8: Verdicts for the assurance components (augmented requirements in bold)

The evaluation has shown that:

- the TOE is conformant to Protection Profile BSI-PP-0006-2002 [12]
- the Security Functional Requirements specified for the TOE are Common Criteria Part 2 extended
- the assurance of the TOE is Common Criteria Part 3 conformant, EAL4 augmented by AVA_MSU.3 and AVA_VLA.4
- the TOE fulfils the claimed strength of function SOF-high for the functions as outlined in chapter 1.3. 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).

The underlying hardware had been successfully assessed by the ITSEF of SERMA Technologies.

The results of the evaluation are only applicable to InCrypto34v2 as outlined in chapter 8 of this report and that is produced and initialised in an environment that was subject to an audit in the cause of the evaluation. The validity can be extended to new versions and releases of the product, provided the sponsor applies for re-certification of the modified product, in accordance with the procedural requirements, and the evaluation of the modified product does not reveal any security deficiencies.

10 Comments/Recommendations

The User and Administrator Guidance documentation [14] (refer to chapter 6 of this report) contains necessary information about the secure usage of the TOE. Additionally, for secure usage of the TOE the fulfilment of the assumptions about the environment in the Security Target [6] and the Security Target as a whole has to be taken into account. Therefore a user/administrator has to follow the guidance in these documents.

Namely, the User and Administrator Guidance documentation [14] points to recommendations in chapter 10.3 that relate to the applied algorithm and key (chapter 10.3.1), to the use of secure messaging (chapter 10.3.2), to PIN delivery and use (chapter 10.3.3), to the signature generation (chapter 10.3.4), to TOE end users (chapter 10.3.5), to TOE disposal (chapter 10.3.6), and to TOE activation (chapter 10.3.7).

Recommendations for application developer contain the following:

- Application developers have to implement applications in accordance with the security functional requirements for the TOE in [6], chapter 5.1 and for the IT environment in [6], chapter 5.3.
- Application developers have to comply with the technical guidance on secure TOE use as provided in [14], chapter 10.3 including secure messaging requirements and TOE activation.
- In particular developers of a SCA have to implement that the signatory and the SCA must be identified and authenticated before any signature operation is processed as required in [14], chapter 10.3.7, see also [14], chapter 10.3.4. This constraint is important for compliance with the Signature Creation Policy of the Secure Signature Creation Device defined in the [6] based on [12]. The secure file system in [14], chapter 10.2 and the related object creation scenarios in [14], chapter 10.3 are set up to comply with this constraint and must be used.

The issuer has to verify that the guidance is followed.

Recommendations for TOE administrators contain the following:

- Technical guidance on secure TOE use as provided in [14], chapter 10.3 including TOE activation has to be transferred by the administrator to developers of certification generation applications (CGA) and signature creation applications (SCA).
- Application guidance on secure TOE use provided in [14], chapter 10.3 and summarized below including TOE activation has to be transferred by the administrator to final users.
- The administrator has to transfer to the end user (signatory) all relevant recommendations.
- The administrator has to comply with recommendations for algorithm parameters (Authentication processes and secure messaging must use

Triple DES algorithm with secret key lengths 128-bit {2 keys} or 192-bit {3 keys} [14], chapter 10.3.1 and 10.3.2) and key parameters (Signature creation keys must be generated with a length of 1024-bit [14], chapter 10.3.1) as well as PIN length and error code values (PIN and PUK code values must have a length of at least 6 and an error counter of 3 [14], chapters 10.2.4, 10.2.5, 10.2.6, 10.3.3) as implemented in the administrator guidance for object creation in [14], chapter 10.2 and the related object creation scenarios in [14], chapter 10.3.

Recommendations for TOE end users (signatories) contain the following:

- When receiving the smartcard (TOE) and the protected sealed PIN envelope the user must verify the integrity of the TOE and the protected sealed PIN envelope.
- Before using the TOE for signature creation, the user must verify that the TOE has never before been used following the TOE activation guidance.
- The user must use a trusted IT environment for TOE activation, user identification and authentication, PIN change, SVD export into the CGA and signature creation with the SCA.
- The user must keep the TOE in a secure place.
- The user must keep authentication data (PIN/PUK codes) secret.
- The user must keep the PIN codes and the TOE in different places to avoid unauthorized use.
- The user must change the PIN codes after receiving the smart card (TOE).
- When changing the PIN, the end user shall avoid non-random and trivial PIN numbers.
- The user must perform user identification and authentication using a PIN entering device in a trusted environment so that the integrity and confidentiality of the PIN are assured.
- The user must perform signature generation in a trusted environment so that the integrity and confidentiality of data exchanged between the TOE and the SCA is assured.

11 Annexes

None.

12 Security Target

For the purpose of publishing, the Security Target [6] of the target of evaluation (TOE) is provided within a separate document.

13 Definitions

13.1 Acronyms

AIS	Application Notes and Interpretation of the Scheme
APDU	Application Protocol Data Unit, interface standard for smart cards, see ISO/IEC 7816 part 3
ATR	Answer to Reset
BSI	Bundesamt für Sicherheit in der Informationstechnik / Federal Office for Information Security
CEM	Common Methodology for IT Security Evaluation
CGA	Certification generation application
CC	Common Criteria for IT Security Evaluation
DPA	Differential Power Analysis, an attack, which may compromise cryptographic keys by analysing the power consumption of the smart card chip
EAL	Evaluation Assurance Level
ETR	Evaluation Technical Report
IC	Integrated Circuit
OSP	Organisational Security Policy
PIN	Personal identification number
PP	Protection Profile
PUK	Personal unblock key
RAD	Reference authentication data
RSA	Asymmetric crypto algorithm by R. L. Rivest, A. Shamir, L. Adleman
SCA	Signature creation application
SCD	Signature creation data
SF	Security Function
SFR	Security Functional Requirement
SM	Secure Messaging

SOF	Strength of Function
SSCD	Secure signature creation device
ST	Security Target
SVD	Signature verification data
TOE	Target of Evaluation
TSC	TSF Scope of Control
TSF	TOE Security Functions
TSFI	TOE security functions interface
TSP	TOE Security Policy
VAD	Verification authentication data

13.2 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.

14 Bibliography

[1] Common Criteria for Information Technology Security Evaluation, Version 2.1, August 1999

[2] Common Methodology for Information Technology Security Evaluation (CEM), Part 1, Version 0.6; Part 2: Evaluation Methodology, Version 1.0, August 1999

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

[4] Applicaton Notes and Interpretations of the Scheme (AIS) as relevant for the TOE.

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

[6] Security Target BSI-DSZ-CC-0202; InCrypto34v2 Security Target, Version 1.58 (A-6), 23.11.2003, ST Incard

[7] Evaluation Technical Report, CC Evaluation of InCrypto34v2, Version 5, 20.12.2004, TÜViT, in combination with Evaluation Reference List (RefList); CC Evaluation of InCrypto34v2; Version: 28; Date: 20.12.2004 (confidential document)

[8] ETR-lite for composition ST19XL34P, ITSEF of SERMA Technologies, Version 1.0, Date 12/07/2004, Document reference: GRENAT_XL34P_ETR_lite v1.0, (confidential document)

[9] ST19XL34, SECURITY TARGET, SMD_ST19XL34_ST_04_001_V1.00, V1_00, issued in July 2004 by ST Microelectronics

[10] Rapport de certification 2004/26 bis; Micro-circuit ST19XL34P; Paris, le 20 août 2004

[11] Protection Profile - Smart Card Integrated Circuit Version 2.0, Issue September 1998, Registered at the French Certification Body as PP/9806

[12] Protection Profile - Secure Signature Creation Device (SSCD-PP) Type 3, Version 1.05, EAL 4+ BSI-PP-0006-2002, 25. July.2001

[13] InCrypto34v2 ACM Configuration List A-4 23.09.2004 (confidential document)

[14] InCrypto34v2 - USER and ADMINISTRATOR Guidance, Issued: 23.11.2004, Revision: A - 8

[15] InCrypto34v2-Functional Specification, Issued 12.12.2003, Revision A – 4, (confidential document)

[16] InCrypto34v2-High Level Design, Issued 03.09.2003, Revision: A – 3, (confidential document)

[17] Algorithms and parameters for algorithms, list of algorithms and parameters eligible for electronic signatures, procedures as defined in the directive 1999/93/EC, article 9 on the ‘Electronic Signature Committee’ in the Directive

[18] ISO/IEC 7816: Part 3, Signal and transmission protocols, Second Edition 1997 Part 4, Interindustry commands for interchange, Edition 1995; Part 5, Numbering System and registration procedure for application identifiers, First Edition 1994; Part 8, Security related interindustry commands, Edition 1998; Part 9, Additional interindustry commands and security attributes, First Edition 2001

C Excerpts from the Criteria

CC Part 1:

Caveats on evaluation results (chapter 5.4) / **Final Interpretation 008**

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 Part 2 (functional requirements), 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:

Part 2 conformant - A PP or TOE is Part 2 conformant if the functional requirements are based only upon functional components in Part 2

Part 2 extended - A PP or TOE is Part 2 extended if the functional requirements include functional components not in Part 2

plus one of the following:

Part 3 conformant - A PP or TOE is Part 3 conformant if the assurance requirements are based only upon assurance components in Part 3

Part 3 extended - A PP or TOE is Part 3 extended if the assurance requirements include assurance requirements not in 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:

Assurance categorisation (chapter 2.5)

„The assurance classes, families, and the abbreviation for each family are shown in Table 2.1.

Assurance Class	Assurance Family	Abbreviated Name
Class ACM: Configuration management	CM automation	ACM_AUT
	CM capabilities	ACM_CAP
	CM scope	ACM_SCP
Class ADO: Delivery and operation	Delivery	ADO_DEL
	Installation, generation and start-up	ADO_IGS
Class 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
Class AGD: Guidance documents	Administrator guidance	AGD_ADM
	User guidance	AGD_USR
Class ALC: Life cycle support	Development security	ALC_DVS
	Flaw remediation	ALC_FLR
	Life cycle definition	ALC_LCD
	Tools and techniques	ALC_TAT
Class ATE: Tests	Coverage	ATE_COV
	Depth	ATE_DPT
	Functional tests	ATE_FUN
	Independent testing	ATE_IND
Class AVA: Vulnerability assessment	Covert channel analysis	AVA_CCA
	Misuse	AVA_MSU
	Strength of TOE security functions	AVA_SOF
	Vulnerability analysis	AVA_VLA

Table 2.1 -Assurance family breakdown and mapping“

Evaluation assurance levels (chapter 6)

„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 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 6.1)

Table 6.1 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 2 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 CC 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 6.1 - Evaluation assurance level summary“

Evaluation assurance level 1 (EAL1) - functionally tested (chapter 6.2.1)

„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 6.2.2)

„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 6.2.3)

„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 6.2.4)

„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 6.2.5)

„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 6.2.6)

„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 6.2.7)

„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 14.3)

AVA_SOF Strength of TOE security functions

„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 14.4)

AVA_VLA Vulnerability analysis

„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), moderate (for AVA_VLA.3) or high (for AVA_VLA.4) attack potential.“

This page is intentionally left blank. (Leerseite nur einfügen damit die letzte Seite in Teil C eine gerade Seite ist)