Certification Report

Bundesamt für Sicherheit in der Informationstechnik

BSI-DSZ-CC-0386-2006

for

ZKA SECCOS Sig v1.5.3

from

Sagem Orga GmbH

BSI - Bundesamt für Sicherheit in der Informationstechnik, Postfach 20 03 63, D-53133 Bonn
Phone +49 (0)3018 9582-0, Fax +49 (0)3018 9582-5455, Infoline +49 (0)3018 9582-111

Deutsches
IT-Sicherheitszertifikat

erteilt vom

Bundesamt für Sicherheit in der Informationstechnik

BSI

Bundesamt für Sicherheit
in der Informationstechnik

BSI-DSZ-CC-0386-2006

ZKA SECCOS Sig v1.5.3

from

Sagem Orga GmbH

Common Criteria Arrangement
for components up to EAL4

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* (ISO/IEC 15408:2005) 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 2.3 (ISO/IEC 15408:2005)*.

Evaluation Results:

Functionality:	**Product specific Security Target** **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, 08. September 2006

The Vice President of the Federal Office
for Information Security

Hange L.S.

IT Security Certified

SOGIS - MRA

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 9582-5455 - 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 2.3[5]
- Common Methodology for IT Security Evaluation (CEM), 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 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 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 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, the Czech Republic in September 2004, the Republic of Singapore in March 2005, India in April 2005.

This evaluation contains the components AVA_MSU.3 (Vulnerability assessment - Analysis and testing for insecure states) and AVA_VLA.4 (Vulnerability assessment - Highly resistant) 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 ZKA SECCOS Sig v1.5.3 has undergone the certification procedure at BSI. This is a re-certification based on BSI-DSZ-CC-0341-2006.

The evaluation of the product ZKA SECCOS Sig v1.5.3 was conducted by SRC Security Research & Consulting GmbH. The SRC Security Research & Consulting GmbH is an evaluation facility (ITSEF)[6] recognised by BSI.

The sponsor, vendor and distributor is:

Sagem Orga GmbH
Am Hoppenhof 33
33104 Paderborn
Germany

The certification is concluded with

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

This work was completed by the BSI on 08. September 2006.

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-24.

The product ZKA SECCOS Sig v1.5.3 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.

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] Sagem Orga GmbH
Am Hoppenhof 33
33104 Paderborn
Germany

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 the smartcard product ZKA SECCOS Sig v1.5.3 developed by Sagem Orga GmbH. It is a re-evaluation of ZKA SECCOS Sig v1.5.2 which is certified unter the certification ID BSI-DSZ-341-2006, see [23] and [24]. The re-evaluation was done mainly due to the addition of new routines to compute SHA-256 hash values in the Renesas cryptographic library ACL which was certified under the certification ID BSI-DSZ-CC-0379-2006, see [9] and [10].

The TOE is realised as Smartcard Integrated Circuit (IC with contacts) with Cryptographic Library, Smartcard Embedded Software and the EEPROM part containing a dedicated Signature Application.

The Smartcard Embedded Software comprises the so-called SECCOS operating system. This platform provides a fully interoperable ISO 7816 compliant multi-application platform.

The TOE is intended to be used as Secure Signature-Creation Device (SSCD) for qualified electronic signatures in accordance with the European Directive 1999/93/EC on electronic signatures [13], the German Signature Act [14], the German Signature Change Act (Signaturänderungsgesetz) [22], and the German Signature Ordinance [15].

The TOE as SSCD is configured software and hardware used to implement the Signature-Creation Data (SCD) and to guarantee for the secure usage of the SCD and comprises the following components:

- Integrated Circuit (IC) AE55C1 (HD65255C1), Version 02 with related Advanced Cryptographic Library, Version 1.43 incl. module SHA-256 (ACL) provided by Renesas Technology Corp. certified under BSI-DSZ-CC-0379-2006, see [9] and [10].
- Smartcard Embedded Software comprising the SECCOS operating system platform provided by Sagem Orga GmbH
- EEPROM Initialisation Tables with the dedicated Signature Application provided by Sagem Orga GmbH and including additional applications

The TOE provides the following functions necessary for devices involved in creating qualified electronic signatures according to the SSCD Type 3 Protection Profile [12]:

- Generation of the SCD and the correspondent Signature-Verification Data (SVD)
- Creation of qualified electronic signatures
  (a) after allowing for the data to be signed (DTBS) to be displayed correctly where the display function has to be provided by an appropriate environment

(b) using appropriate hash functions that are, according to [16], agreed as suitable for qualified electronic signatures

(c) after appropriate authentication of the signatory by the TOE

(d) using appropriate cryptographic signature functions that employ appropriate cryptographic parameters agreed as suitable according to [16].

To prevent the unauthorised usage of the SCD, the TOE provides user authentication and access control. The user authenticates himself by supplying the verification authentication data (VAD) to the TOE which compares the VAD against the reference authentication data (RAD) securely stored inside the TOE. The TOE implements IT measures to support a trusted path to a trusted human interface device that can optionally be connected via a trusted channel with the TOE.

The TOE does not implement the Signature-Creation Application (SCA) which presents the data to be signed (DTBS) to the signatory and prepares the DTBS-representation the signatory wishes to sign for performing the cryptographic function of the signature. The SCA belongs to the environment of the TOE.

The TOE protects the SCD during the whole life-cycle as to be solely used in the signature-creation process by the legitimate signatory. The TOE as SSCD of Type 3 generates the signatory's SCD oncard and serves for a secure storage of this data. The initialisation and personalisation of the TOE for the signatory's use in the sense of the Protection Profile [12] include:

- Generation of the SCD/SVD pair
- Personalisation for the signatory by means of the signatory's verification authentication data (VAD).

From the structural perspective, the TOE as SSCD comprises the underlying IC including the related ACL, the SECCOS operating system and the Signature Application with SCD/SVD generation, SCD storage and use, SVD export, and the signature-creation functionality. The SCA and the CGA (beside additional other applications) are part of the immediate environment of the TOE. They may communicate with the TOE over a trusted channel, a trusted path for the human interface provided by the SCA, respectively. In case a trusted channel or trusted path is not established with cryptographic means the TOE shall only be used within a Trusted Environment.

The TOE as a multi-application smart card implements additional applications that are not part of the TOE.

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, the Renesas AE55C1 (HD65255C1) smartcard integrated circuit version 02 with ACL version 1.43 and additional SHA-256 function provided by Renesas Technology Corp. and which was evaluated as BSI-DSZ-CC-0379-2006 ([9] and [10]). The IC was evaluated according to Common Criteria EAL 4 augmented with a minimum strength level for its security

functions of SOF-high for specific functionality based on the Protection Profile BSI-PP-0002 [11] and as outlined in [9] and [10]. This platform evaluation was performed by T-Systems GEI GmbH.

The IT product ZKA SECCOS Sig v1.5.3 was evaluated by SRC Security Research & Consulting GmbH. The evaluation was completed on 02. August 2006. The SRC Security Research & Consulting GmbH is an evaluation facility (ITSEF)[8] recognised by BSI.

The sponsor, vendor and distributor is

Sagem Orga GmbH
Am Hoppenhof 33
33104 Paderborn
Germany

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: Assurance components and EAL-augmentation

1.2 Functionality

The TOE Security Functional Requirements (SFR) selected in the Security Target [6] are Common Criteria Part 2 extended as shown in the following tables.

The following SFRs are taken from the SSCD Type 3 PP [12] and from CC part 2:

Security Functional Requirement	**Addressed issue**
FCS	**Cryptographic support**
FCS_CKM.1	Cryptographic key generation

[8] Information Technology Security Evaluation Facility

Security Functional Requirement	Addressed issue
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 for the TOE taken from CC Part 2

The following CC part 2 extended SFRs are defined:

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

Table 3: SFRs for the TOE, CC part 2 extended

Note: only the titles of the Security Functional Requirements are provided. For more details and application notes please refer to the ST [6] chapter 5.

The following Security Functional Requirements are defined for the Certification Generation Application (CGA) in the IT- Environment of the TOE:

Security Functional Requirement	Addressed issue
FCS	**Cryptographic support**
FCS_CKM.2	Cryptographic key distribution
FCS_CKM.3	Cryptographic key access
FDP	**User data protection**
FDP_UIT.1	Data exchange integrity
FTP	**Trusted Path/Channels**
FTP_ITC.1	Inter-TSF trusted channel

Table 4: SFRs for the CGA in the IT-Environment

The following Security Functional Requirements are defined for the Signature Creation Application (SCA) in the IT- Environment of the TOE:

Security Functional Requirement	Addressed issue
FCS	**Cryptographic support**
FCS_COP.1	Cryptographic operation
FDP	**User data protection**
FDP_UIT.1	Data exchange integrity
FTP	**Trusted Path/Channels**
FTP_ITC.1	Inter-TSF trusted channel
FTP_TRP.1	Trusted Path

Table 5: SFRs for the SCA in the IT-Environment

Note: only the titles of the Security Functional Requirements are provided. For more details and application notes please refer to the ST [6], chapter 5.2.1.

For a detailed overview of the SFRs defined for the underlying IC and ACL refer to [10], Chapter 5.1.1, 8.4, 8.5 and 8.6.

These Security Functional Requirements are implemented by the TOE Security Functions:

TOE Security Function	Addressed issue
Access Control	
F.ACS_SIG	Security Attribute Based Access Control / ZKA-SigG-Q Application
F.ADMIN_SIG	Administration of the TOE / ZKA-SigG-Q Application
Identification and Authentication	
F.PIN_SIG	PIN Based User Authentication for the Signatory
Integrity of Stored Data	
F.DATA_INT	Stored Data Integrity Monitoring and Action
Secure Data Exchange	
F.SEC_EXCH	Integrity and Confidentiality of Data Exchange
Object Reuse	
F.RIP	Residual Information Protection
Protection	
F.FAIL_PROT	Hardware and Software Failure Protection
F.SIDE_CHAN	Side Channel Analysis Control
F.SELFTEST	Self Test
Cryptographic Operations	
F.CRYPTO	Cryptographic Support
F.RSA_KEYGEN	RSA Key Pair Generation
F.GEN_SIG	RSA Generation of Electronic Signatures

Table 6: TOE Security Functions

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

For a detailed overview of the TOE Security Functions defined for the underlying IC and ACL refer to [10].

1.3 Strength of Function

The TOE's strength of functions is claimed high (SOF-high) for specific functions as indicated in the Security Target [6], chapter 6.2.

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.

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 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
T.INIT_Aut	Authentication for Initialisation Process
T.INIT_Data	Loading of Manipulated Initialisation Data
T.PERS_Aut	Authentication for Personalisation Process
T.PERS_Data	Modification or Disclosure of Personalisation Data

Table 7: Threats for the TOE

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

Table 8: OSPs

Note: Only the titles of the threats and OSPs are provided. For more details please refer to the Security Target [6], chapter 3, where also assets and subjects of the TOE are described.

1.5 Special configuration requirements

The TOE is intended to be used as a secure signature creation device. It is defined uniquely by the name and version number ZKA SECCOS Sig v1.5.3. Its implementation representation and its configuration are specified by the Configuration List [21].

The evaluation results are restricted to chip cards or modules containing the TOE in combination with other applications that are listed below in table 9. All applications are listed in the table below. During the evaluation, tests have been

performed to demonstrate that the separation mechanism of the SECCOS Application Layer realises a separation between these additional applications and the dedicated Signature Application. The additional applications did not influence the security of the Signature Application.

Application Name	AID (Application Identifier)	Application name in the card
MF MF	3F 00	52 4F 4F 54
Signature application DF_SIG	AB 00	D2 76 00 00 66 01
Zusatzanwendungen ZA_MF_NEU	A7 00	D2 76 00 00 25 5A 41 02 00
ec-Cash DF_EC_CASH_NEU	A1 00	D2 76 00 00 25 45 43 02 00
Geldkarte DF_BOERSE_NEU	A2 00	D2 76 00 00 25 45 50 02 00 A0 00 00 00 59 50 41 43 45 01 00
GA-Maestro DF_GA_MAESTRO	AC 00	D2 76 00 00 25 47 41 01 00 A0 00 00 00 04 30 60
TAN-Anwendung DF_TAN	AC 02	D2 76 00 00 25 54 44 01 00
Marktplatz DF_MARKTPLATZ_NEU	B0 01	D2 76 00 00 25 4D 01 02 00
Fahrschein DF_FAHRSCHEIN_NEU	B0 00	D2 76 00 00 25 46 53 02 00
HBCI DF_BANKING_20	A6 00	D2 76 00 00 25 48 42 02 00
Notepad DF_NOTEPAD	A6 10	D2 76 00 00 25 4E 50 01 00

Table 9: Signature application and optional applications

1.6 Assumptions about the operating environment

The following constraints concerning the operating environment are made in the Security Target, please refer to the Security Target [6], chapter 3.2:

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.INIT_Process	Security of the Initialisation Process The initialisation table and process are handled in a secure manner.
A.PERS_Process	Security of the Personalisation Process The personalisation data and process are handled 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:

ZKA SECCOS Sig v1.5.3

The following table outlines the TOE deliverables:

No	Type	TOE component	Remarks	Form of Delivery
1	HW / SW	TOE-IC and Embedded Software	Renesas IC AE55C1 (HD65255C1), Version 02, the ROM mask SECCOS_5.0_AE55C1_R1.2_SHA256 consisting of the Advanced Cryptographic Library, Version 1.43 (ACL) with additional SHA-256 function and the Smartcard Embedded Software (SECCOS operating system) provided by Sagem Orga GmbH.	Delivery of non-initialised / initialised modules or smartcards.
			EEPROM Initialisation Table SDR0O1G0.A_3 (provided by Sagem Orga GmbH) with the dedicated Signature Application	Delivery of Initialisation Tables in electronic form (if applicable).

No	Type	TOE component	Remarks	Form of Delivery
2	DOC	Administrator Guide / Smartcard Initialisation	Administrator guidance for the Initialiser for the smartcard initialisation of the TOE Version V1.01 [17]	Document in paper / electronic form
3	DOC	Administrator Guide / Smartcard Personalisation	Administrator guidance for the Personaliser for the smartcard personalisation of the TOE Version V1.01 [18]	Document in paper / electronic form
4	DOC	Identification Data Sheet	Data Sheet with information on the actual identification data and configuration of the TOE delivered to the customer (in particular information on the relevant Initialisation Table) Version V1.01, Option BES0/2 [19]	Document in paper / electronic form
5	DOC	Document „Konzept zur Personalisierung von ZKA-Chipkarten (insbesondere Signaturkarten) des deutschen Kreditgewerbes mit dem Betriebssystem SECCOS“	Specification describing Initialisation and Personalisation processes, Version 1.3 [20]	Document in paper / electronic form

Table 10: Deliverables of the TOE

The TOE’s evaluated configuration also contains other applications which have been listed in table 9 of chapter 1.5.

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 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

The following usage assumptions defined by the Security Target have to be met (refer to Security Target [6], chapter 3.2):

- The initialisation table and process are handled in a secure manner (A.INIT_Process).
- The personalisation data and process are handled in a secure manner (A.PERS_Process).

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 3.2):

- 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).

Furthermore, the Security Target [6], chapter 3.4 defines three Organisational Security Policies 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 3.4 for more detail.

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 (ZKA SECCOS Sig v1.5.3) is intended to be used as a secure signature creation device comprising an integrated circuit (IC) with an operating system (OS) and a signature application. An overview of the architecture including a figure of the global architecture of the TOE is given in chapter 2 of the Security Target [6]. A description and a top level block diagram of the

dedicated Signature Application can be found in chapter 2.1.2 of the Security Target [6]. The TOE is the composition of an IC, IC Dedicated Software and Smart Card Embedded Software. A top level block diagram of the hardware IC including an overview of subsystems can be found within the TOE description of the Security Target of the chip [10].

6 Documentation

The following documentation is provided with the product by the developer to the customer (see also table 10 of this report):

- Administrator Guidance / Smartcard Initialisation - Administrator Guidance for the Initialiser of the Smartcard Product ZKA SECCOS Sig v1.5.3, Version V1.01 [17]
- Administrator Guide / Smartcard Personalisation - System Administrator Guidance for the Personaliser of the Smartcard Product ZKA SECCOS Sig v1.5.3, Version V1.01 [18]
- Identification Data Sheet - Data Sheet with information on the actual identification data and configuration of the TOE delivered to the customer (in particular information on the relevant Initialisation Table), Version V1.01, Option BES0/2 [19]
- Document "Konzept zur Personalisierung von ZKA-Chipkarten (insbesondere Signaturkarten) des deutschen Kreditgewerbes mit dem Betriebssystem SECCOS" - Specification describing Initialisation and Personalisation processes, Version 1.3 [20]

7 IT Product Testing

The developer tested all TOE Security functions either on real cards or with emulator tests. All command APDU with valid and invalid inputs were tested as well as all functions with valid and invalid inputs. Repetition of developer tests were performed during the independent evaluator tests.

Since many Security Functions can be tested by ISO-7816 APDU command sequences, the evaluators performed these tests with real cards. This is considered to be a reasonable approach because the developers tests include a full coverage of all security functionality with emulator tests. Tests with emulators were chosen by the evaluators for those security functions where internal resources of the card needed to be modified or observed during the test. During their independent testing, the evaluators covered

- the Initialisation and Personalisation commands used by the Initialiser and Personaliser,
- the APDU commands of SECCOS Application Layer used by TOE’s Signature Application,

- Secure Messaging and Access Condition Validation of SECCOS Application Layer,
- a significant subset of the Microkernel functionality and
- tests of TOE's Signature Application data structures.

Tests were performed on cards in several lifecycle states:

- non-initialised cards
- initialised cards
- personalised cards
- cards in end-usage state

Source code analysis was also performed during the evaluation.

The evaluators also performed tests that verified that the additional applications do not have a negative influence on the signature application.

The evaluators have tested the TOE systematically against high attack potential during their penetration testing. The tests included the resistance of the RSA and Triple-DES Implementation against Side Channel Analysis.

The achieved test results correspond to the expected test results.

As this is a re-evaluation of an already certified product, some correctness and penetration tests were re-used, however, other tests were re-done and specific tests were performed for this evaluation.

8 Evaluated Configuration

The TOE is defined uniquely by the name and version number ZKA SECCOS Sig v1.5.3.

For the delivery of the TOE different ways are established (for more details about the TOE life cycle phases please read the Overview of the TOE Life Cycle explained in the ST [6], chapter 2.2.1):

- The TOE is delivered to the customer in form of a complete initialised smartcard.
- Alternatively, the TOE is delivered to the customer in form of an initialised module. In this case, the smartcard finishing process (embedding of the delivered modules, final card tests) is task of the customer.
- ZKA SECCOS Sig v1.5.3 may as well be delivered as not-initialised modules or smartcards, for details see chapter 1.2 of the Security Target [6], however, the TOE is defined as the initialised smartcard. In this case, initialisation outside the development and production environment Sagem Orga GmbH in Flintbek, Germany is outside the scope of this certification and the assumption A.INIT_Process applies.

The form of the delivery of the TOE does not concern the security features of the TOE. However, the initialisation process at Sagem Orga GmbH in Flintbek, Germany is considered as well within the framework of the CC evaluation of the Sagem Orga GmbH product. The responsibility for the delivery of the personalised TOE to the end-user is up to the Card Issuer.

The development of the TOE is done in Sagem Orga GmbH Paderborn; production and if necessary initialisation of the TOE takes place at Sagem Orga GmbH Flintbek. Regarding the development and production environment of the underlying IC please refer to Annex A of [9].

The evaluation results are restricted to chip cards containing the TOE with applications that have been inspected during the evaluation process and that are listed in table 7 of this report. See also chapter 1.5 of this report.

9 Results of the Evaluation

The Evaluation Technical Report (ETR), [8] was provided by the ITSEF 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.

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 [4, AIS 34]).

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].

The ETR [8] builds up on the ETR-lite for Composition documents of the evaluations of the underlying Renesas AE55C1 (HD65255C1) smartcard integrated circuit version 02 with related Advanced Cryptographic Library version 1.43 incl. module SHA-256 (ACL) provided by Renesas Technology Corp. ([9] and [10]). The ETR-lite for Composition documents were provided by the ITSEF T-Systems GEI GmbH according to CC Supporting Document, ETR-lite for Composition ([4, AIS 36]).

For smart card specific methodology the scheme interpretations AIS 25, AIS 26 and AIS 36 (see [4]) were used. For specific methodology on random number generator evaluation the scheme interpretations AIS 20 and AIS 31 (see [4]) were used.

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
Installation, generation, and start-up procedures	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
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

Assurance classes and components		Verdict
Testing: high-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
Analysis and testing for insecure states	**AVA_MSU.3**	PASS
Strength of TOE security function evaluation	AVA_SOF.1	PASS
Highly resistant	**AVA_VLA.4**	PASS

Table 11: Verdicts for the assurance components

As this certification was a re-certification of ZKA SECCOS Sig v1.5.2 where new routines to compute SHA-256 hash values were added in the Renesas cryptographic library ACL, emphasis was put on Tests and Vulnerability Assessment in this certification.

The evaluation has shown that

- 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 security functions F.ADMIN_SIG, F.PIN_SIG, F.CRYPTO, F.RSA_KEYGEN, F.GEN_SIG as outlined in chapter 1.3. The underlying hardware had been successfully assessed by T-Systems GEI GmbH.

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 results of the evaluation are only applicable to ZKA SECCOS Sig v1.5.3 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 or assurance continuity 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 operational documentation (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.

The TOE is a multi-application card. Only those applications listed in table 9 shall be used within the evaluated configuration.

Furthermore an appropriate protection during packaging, finishing, and personalisation must be ensured up to delivery to the end-user to prevent any possible copy, modification, retention, theft, or unauthorised use of the TOE and of its manufacturing and test data (the assumption A.Process-Card from the ST of the hardware platform [10]).

11 Annexes

None.

12 Security Target

For the purpose of publishing, the security target [7] of the target of evaluation (TOE) is provided within a separate document. It is a sanitized version of the complete security target [6] used for the evaluation performed.

13 Definitions

13.1 Acronyms

ACL	Advanced Cryptographic Library
AID	Application identifier
AIS	Application Notes and Interpretation of the Scheme
APDU	Application Protocol Data Unit, interface standard for smart cards, see ISO/IEC 7816 part 3
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
CSP	Certification-service-provider
DES	Data Encryption Standard, symmetric crypto algorithm
DTBS	Data to be signed
EAL	Evaluation Assurance Level
EEPROM	Electrically erasable programmable read-only memory; EEPROM is a special type of PROM that can be erased by exposing it to an electrical charge
ETR	Evaluation Technical Report

EU	European Union
HW	Hardware
IC	Integrated Circuit
ISO	International Organization for Standardization
IT	Information Technology
OS	Operating System
OSP	Organisational Security Policy
PIN	Personal identification number
PP	Protection Profile
PROM	Programmable read-only memory, a memory chip on which data can be written only once
RAD	Reference authentication data
RSA	Asymmetric crypto algorithm by R. L. Rivest, A. Shamir, L. Adleman
SCA	Signature creation application
SCD	Signature creation data
SECCOS	Secure Chip Card Operating System
SF	Security Function
SFR	Security Functional Requirement
SigG	(German) Signaturgesetz
SigV	(German) Signaturverordnung
SOF	Strength of Function
SSCD	Secure signature creation device
ST	Security Target
SVD	Signature verification data
SW	Software
TOE	Target of Evaluation
TRNG	True Random Number Generator (a term used and introduced in AIS31)
TSF	TOE Security Functions
TSP	TOE Security Policy
VAD	Verification authentication data
ZKA	Zentraler Kreditausschuss

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 2.3, 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 20, Version 1, 2 Dec. 1999 Functionality classes and evaluation methodology for deterministic random number generators
- AIS 25, Version 2, 29 July 2002 for: CC Supporting Document, - The Application of CC to Integrated Circuits, Version 1.2, July 2002
- AIS 26, Version 2, 6 August 2002 for: CC Supporting Document, - Application of Attack Potential to Smartcards, Version 1.1, July 2002
- 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 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

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

[6] Security Target BSI-DSZ-0386-2006, Version V1.00, 07 June 2006, Security Target – ZKA SECCOS Sig v1.5.3, Sagem Orga GmbH (confidential document)

[7] Security Target BSI-DSZ-CC-0386-2006, Version V1.01, 21 June 2006, Sagem Orga GmbH; ZKA SECCOS Sig v1.5.3; ST-Lite (sanitized public document)

[8] Evaluation Technical Report (ETR); BSI-DSZ-CC-0386-2006; Version: 2.3; 02.08.06; Product: ZKA SECCOS Sig v1.5.3 (confidential document)

[9] Certification Report BSI-DSZ-CC-0379-2006 for Renesas AE55C1 (HD65255C1) smartcard integrated circuit version 02 with ACL version 1.43 and additional SHA-256 function from Renesas Technology Corp., Bundesamt für Sicherheit in der Informationstechnik, 15.05.2006

[10] Security Target BSI-DSZ-0379-2006, Revision 5.0, 7 April, 2006, AE55C1 (HD65255C1) Version 02 with ACL version 1.43 Smartcard Security Target, Public Version, Renesas Technology Corp.

[11] Smartcard IC Platform Protection Profile (SSVG-PP), Version 1.0, July 2001; registered and certified by Bundesamt für Sicherheit in der Informationstechnik (BSI) under the reference BSI-PP-0002-2001

[12] Protection Profile - Secure Signature Creation Device (SSCD-PP) Type 3, Version 1.05, EAL 4+ BSI-PP-0006-2002T, 03.04.2002

[13] Directive 1999/93/ec of the European parliament and of the council of 13 December 1999 on a Community framework for electronic signatures

[14] (German) Gesetz über Rahmenbedingungen für elektronische Signaturen und zur Änderung weiterer Vorschriften vom 16. Mai 2001 (BGBI. I S.876 ff)

[15] Verordnung zur elektronischen Signatur; Bundesgesetzblatt Nr. 509, S. 3074; 16.11.2001

[16] Geeignete Algorithmen zur Erfüllung der Anforderungen nach §17 Abs.1 bis 3 SigG vom 22. Mai 2001 in Verbindung mit Anlage 1 Anschnitt I Nr. 2 SigV vom 22. Nov. 2001; Bundesanzeiger Nr. 58, S. 1913-1915, 23.03.2006, Bundesnetzagentur

[17] Administrator Guidance for the Initialiser of the Smartcard Product ZKA SECCOS Sig v1.5.3 - ZKA SECCOS Sig v1.5.3, Version V1.01, Sagem Orga GmbH, 07.07.2006

[18] System Administrator Guidance for the Personaliser of the Smartcard Product ZKA SECCOS Sig v1.5.3 - ZKA SECCOS Sig v1.5.3, Version V1.01, Sagem Orga GmbH, 07.07.2006

[19] ZKA SECCOS Sig v1.5.3, Data Sheet, Version V1.01, Option BES0/2, Sagem Orga GmbH, 07.07.2006

[20] Konzept zur Personalisierung von ZKA-Chipkarten (insbesondere Signaturkarten) des deutschen Kreditgewerbes mit dem Betriebssystem SECCOS, Version 1.3, 29.12.2004

[21] Configuration List - ZKA SECCOS Sig v1.5.3, Version V1.01, Sagem Orga GmbH, 07.07.2006 (confidential document)

[22] (German) Erstes Gesetz zur Änderung des Signaturgesetzes vom 4. Januar 2005

[23] Certification Report BSI-DSZ-CC-0341-2006 for ZKA SECCOS Sig v1.5.2 from Sagem Orga GmbH, Bundesamt für Sicherheit in der Informationstechnik, 13. June 2006

[24] Security Target BSI-DSZ-CC-0341-2006, Version V1.00, 25 April 2006, Sagem Orga GmbH; ZKA SECCOS Sig v1.5.2; ST-Lite (sanitized public document)

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:

a) **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.

b) **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:

a) **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.

b) **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:

a) **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.

b) **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:

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

CC Part 3:

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.”