Federal Office
for Information Security

Certification Report

BSI-DSZ-CC-0449-2009

for

ZKA SECCOS Sig v2.6.4 R1.1

from

Sagem Orga GmbH

BSI - Bundesamt für Sicherheit in der Informationstechnik, Postfach 20 03 63, D-53133 Bonn
Phone +49 (0)228 99 9582-0, Fax +49 (0)228 9582-5477, Infoline +49 (0)228 99 9582-111

Bundesamt
für Sicherheit in der
Informationstechnik

Deutsches IT-Sicherheitszertifikat

erteilt vom Bundesamt für Sicherheit in der Informationstechnik

BSI-DSZ-CC-0449-2009

ZKA SECCOS Sig v2.6.4 R1.1

from	Sagem Orga GmbH
Functionality:	Product Specific Security Target Common Criteria Part 2 extended
Assurance:	Common Criteria Part 3 conformant EAL 4 augmented by AVA_MSU.3 and AVA_VLA.4

Common Criteria Recognition Arrangement for components up to EAL 4

Common Criteria

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

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

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

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

Bonn, 22 July 2009
For the Federal Office for Information Security

IT Security Certified

SOGIS - MRA

Bernd Kowalski L.S.
Head of Department

Bundesamt für Sicherheit in der Informationstechnik
Godesberger Allee 185-189 - D-53175 Bonn - Postfach 20 03 63 - D-53133 Bonn
Phone +49 (0)228 99 9582-0 - Fax +49 (0)228 9582-5477 - Infoline +49 (0)228 99 9582-111

This page is intentionally left blank.

Preliminary Remarks

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

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

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

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

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

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

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

Contents

A Certification

1 Specifications of the Certification Procedure

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

- BSIG[2]
- BSI Certification Ordinance[3]
- BSI Schedule of Costs[4]
- Special decrees issued by the Bundesministerium des Innern (Federal Ministry of the Interior)
- DIN EN 45011 standard
- BSI certification: Procedural Description (BSI 7125) [3]
- Common Criteria for IT Security Evaluation (CC), Version 2.3 (ISO/IEC 15408:2005)[5] [1]
- Common Methodology for IT Security Evaluation, Version 2.3 [2]
- BSI certification: Application Notes and Interpretation of the Scheme (AIS) [4]
- Advice from the Certification Body on methodology for assurance components above EAL4 (AIS 34)

2 Recognition Agreements

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

---

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

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

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

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

2.1 European Recognition of ITSEC/CC - Certificates

The SOGIS-Mutual Recognition Agreement (MRA) for certificates based on ITSEC became initially effective in March 1998.

This agreement on the mutual recognition of IT security certificates was extended in April 1999 to include certificates based on the Common Criteria for the Evaluation Assurance Levels (EAL 1 – EAL 7). This agreement was signed by the national bodies of Finland, France, Germany, Greece, Italy, The Netherlands, Norway, Spain, Sweden and the United Kingdom. The German Federal Office for Information Security (BSI) recognises certificates issued by the national certification bodies of France and United Kingdom, and from The Netherlands since January 2009 within the terms of this agreement.

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

2.2 International Recognition of CC - Certificates

An arrangement (Common Criteria Recognition Arrangement) on the mutual recognition of certificates based on the CC Evaluation Assurance Levels up to and including EAL 4 has been signed in May 2000 (CCRA). It includes also the recognition of Protection Profiles based on the CC.

As of January 2009 the arrangement has been signed by the national bodies of: Australia, Austria, Canada, Czech Republic, Denmark, Finland, France, Germany, Greece, Hungary, India, Israel, Italy, Japan, Republic of Korea, Malaysia, The Netherlands, New Zealand, Norway, Pakistan, Republic of Singapore, Spain, Sweden, Turkey, United Kingdom, United States of America. The current list of signatory nations and approved certification schemes can be seen on the web site: http://www.commoncriteriaportal.org

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

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

3 Performance of Evaluation and Certification

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

The product ZKA SECCOS Sig v2.6.4 R1.1 has undergone the certification procedure at BSI.

The evaluation of the product ZKA SECCOS Sig v2.6.4 R1.1 was conducted by SRC Security Research & Consulting GmbH. The evaluation was completed on 7 July 2009. The SRC Security Research & Consulting GmbH is an evaluation facility (ITSEF)[6] recognised by the certification body of BSI.

For this certification procedure the sponsor and applicant is: Sagem Orga GmbH.

The product was developed by: Sagem Orga GmbH.

[6] Information Technology Security Evaluation Facility

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

4 Validity of the certification result

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

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

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

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

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

5 Publication

The product ZKA SECCOS Sig v2.6.4 R1.1 has been included in the BSI list of the certified products, which is published regularly (see also Internet: http://www.bsi.bund.de) and [5]. Further information can be obtained from BSI-Infoline +49 228 9582-111.

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

[7] Sagem Orga GmbH
Riemekestrasse 160
33106 Paderborn

This page is intentionally left blank.

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.

1 Executive Summary

The Target of Evaluation (TOE) is the product ZKA SECCOS Sig v2.6.4 R1.1 provided by Sagem ORGA GmbH.

The TOE is a smartcard product and 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 SECCOS operating system. This platform provides a fully interoperable ISO 7816 compliant multi-application platform which can be used for smartcards with high security applications. The product allows in particular beside the dedicated Signature Application of the TOE for further different kinds of (banking) applications.

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 [19], the German Signature Act [20] and the German Signature Ordinance [21]. The EU compliant Signature Application of the TOE is designed for the generation of legally binding qualified electronic signatures as defined in [19], [20] and [21].

The TOE´s dedicated Signature Application provides asymmetric cryptography based on RSA for key generation and signature-creation with a key length of 2048 bit. Digital signature schemes are either PKCS#1 with the hash algorithm SHA-256, SHA-384 or SHA-512 or ISO/IEC 9796-2 with random numbers with the hash algorithm RIPEMD-160.

The TOE comprises the following components:

- Integrated Circuit (IC) AT90SC28872RCU with related Cryptographic Toolbox 00.03.10.00 provided by Atmel Corp.
- 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 (possibly including additional applications such as GeldKarte Application, EMV Application, Electronic Cash Application).

Possible other applications are outside the scope of the certificate.

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 AT90SC28872RCU with related Cryptographic Toolbox 00.03.10.00 provided by Atmel Corp. The evaluation of the IC incl. toolbox is based on the Protection Profile [14] and is registered under the Certification-ID BSI-DSZ-CC-0421 [13].

For the delivery of the TOE different ways are established.

The TOE is delivered to the customer in form of a complete initialised smartcard. In this case, the initialisation will be performed by Sagem Orga GmbH.

Alternatively, the TOE is delivered to the customer in the form of an not-initialised module or smartcard. In this case, the delivery of the modules resp. smartcards will be combined with the delivery of the customer specific Initialisation Table (in particular containing the evaluated Signature Application) developed by Sagem Orga GmbH to the involved Verlag der Kreditwirtschaft. The finalised Initialisation Table has to be sent from the Verlag der Kreditwirtschaft (by a secured transfer way) to the Initialiser for loading the EEPROM

initialisation data into the TOE during its initialisation phase whereat the production requirements defined in the Guidance for the Initialiser (as well delivered by Sagem Orga) have to be considered.

In the case of the delivery of modules, the last part of the smartcard finishing process, i.e. the embedding of the delivered modules and final tests, is task of the customer.

The Security Target [6] is the basis for this certification. It is based on but not conformant to the certified Protection Profile Secure Signature-Creation Device Type 3, EAL 4+, BSI-PP-0006-2002 [10].

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

The TOE Security Functional Requirements (SFR) relevant for the TOE are outlined in the Security Target [6] and [9], chapter 5. They are selected from Common Criteria Part 2 and some of them are newly defined. Thus the TOE is CC Part 2 extended.

The Security Functional Requirements (SFR) relevant for the IT-Environment of the TOE are outlined in the Security Target [6] and [9], chapter 5.2.

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

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

Table 1: TOE Security Functions

For more details please refer to the Security Target [6] and [9], chapter 6.

The claimed TOE's Strength of Functions 'high' (SOF-high) for specific functions as indicated in the Security Target [6] and [9], chapter 6.2 is confirmed. The rating of the Strength of Functions does not include the cryptoalgorithms suitable for encryption and decryption (see BSIG Section 4, Para. 3, Clause 2). For details see chapter 9 of this report.

The assets to be protected by the TOE are defined in the Security Target [6] and [9], chapter 3.1. Based on these assets the TOE Security Environment is defined in terms of Assumptions, Threats and Organisational Security Policies. This is outlined in the Security Target [6] and [9], chapter 3.2 to 3.4.

This certification covers the following configurations and delivery forms of the TOE:

- completely initialised smartcard
- completely initialised module
- non-initialised smartcard
- non-initialised module

The TOE contains at its delivery unalterable identification information on the delivered configuration.

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 v2.6.4 R1.1

The following table outlines the TOE deliverables:

Item	Description / Additional Information	Type	Transfer Form
1	TOE consisting of • ATMEL AT90SC28872RCU revision E, whereat the ROM mask consisting of the Cryptographic Toolbox 00.03.10.00 and the Smartcard Embedded Software (SECCOS operating system) provided by Sagem Orga GmbH is already implemented • EEPROM Initialisation Table (provided by Sagem Orga GmbH)	TOE HW + SW part	Delivery of not-initialised / initialised modules or smartcards Delivery of Initialisation Tables in electronic form (if applicable) Note: The delivered Initialisation Tables have to be finalised by the Verlage der Kreditwirtschaft (insertion of additional verification data).
2	Administrator guidance for the Initialiser for the smartcard initialisation of the TOE (“System Administrator Guidance for the Initialiser of the Smartcard Product ZKA SECCOS Sig v2.6.4, Version V1.00, Sagem Orga GmbH, 08.10.2008) [15]	DOC	Document in paper / electronic form
3	Administrator guidance for the Personaliser for the	DOC	Document in paper /

Item	Description / Additional Information	Type	Transfer Form
	smartcard personalisation of the TOE (“System Administrator Guidance for the Personaliser of the Smartcard Product ZKA SECCOS Sig v2.6.4, Version V1.00, Sagem Orga GmbH, 08.10.2008) [16]		electronic form
4	Data Sheet with information on the actual identification data and configuration of the TOE delivered to the customer (customer specific; in particular information about the relevant Initialisation Table, “ZKA SECCOS Sig v2.6.4, Data Sheet, Version V1.03, Sagem ORGA GmbH, 07.07.2009”) [17]	DOC	Document in paper / electronic form
5	Konzept zur Personalisierung von ZKA-Chipkarten (insbesondere Signaturkarten) des deutschen Kreditgewerbes mit dem Betriebssystem SECCOS 6.x, Version 1.02, 30.11.2006, Bank-Verlag GmbH, Deutscher Genossenschafts-Verlag eG, Deutscher Sparkassen Verlag GmbH, Bundesverband Öffentlicher Banken-ZVD GmbH [18]	DOC	Document in paper / electronic form

Table 2: Deliverables of the TOE

Note 1:

The TOE will be delivered from Sagem Orga GmbH either as a not-initialised or initialised product (module / smartcard). To finalize the TOE as the not-initialised product, the Initialisation Table developed by Sagem Orga GmbH must be loaded during the initialisation phase by the Initialiser (Sagem Orga GmbH or other initialisation facility) following the production requirements defined in the Guidance for the Initialiser [15].

Note 2:

Deliverables in paper form require a personal passing on or a procedure of at least the same security. For deliverables in electronic form an integrity and authenticity attribute will be attached.

The customer can identify the TOE as the certified product as follows:

Non-initialised cards/modules can be identified with the historical bytes of the cold and warm ROM ATR.

The historical bytes of the Cold and Warm ROM ATR contain

- IC manufacturer’s ID: ’1A’
- Manufacturer's IC type ID: ’02’
- Manufacturer's ROM mask ID: ’62’
- Embedder’s ID (Embedder country code + Embedder national RID): ’02 80’ + ‘00 0F’
- Chip series number, ROM ATR: ’12 34 56 78’
- Chip series number, EEPROM ATR: dependent on the concrete copy of the TOE.
- Manufacturer’s OS Version (major+minor version number): ‘06 41’

The identifiers are not alterable.

Initialised cards/modules can be identified with the historical bytes of the Cold and Warm EEPROM ATR as well as with the command GET DATA.

The initialised TOE contains the initialisation protocol data which allow the unambiguous identification of the Initialiser and the hardware and software configuration at the moment of the initialisation and thereby of the Initialisation Table used in the initialisation. The Initialisation Table specifies the applications contained in the card. The initialisation protocol data are readable via the command GET DATA and are not alterable. (the data necessary for the verification are included in chapter 4 of the Identification Data Sheet [17]). Bytes 1-16 are reserved for the Initialiser and are specified by Orga in the following way:

The historical bytes of the Cold and Warm EEPROM ATR contain

- Byte 1, IC manufacturer's ID: '1A'
- Byte 2, Manufacturer's IC type ID: '02'
- Byte 3, Manufacturer's ROM mask ID: '62'
- Bytes 4-7, Chip series number: dependent on the concrete copy of the TOE
- Bytes 8-9, Manufacturer's OS Version (major+minor version number): '06 41'
- Bytes 10-13, Chip series number supplement: dependent on the concrete copy of the TOE
- Byte 14, ROM mask developer: '0F'
- Bytes 15-16, Not used in this version: '00 00'

All the identifiers and information are not alterable.

The data necessary for the verification (Cold and Warm ROM ATR as well as Cold and Warm EEPROM ATR) are included in chapter 5 of the Identification Data Sheet [17].

3 Security Policy

The TOE is the composition of an IC, a Smartcard Embedded Software comprising the SECCOS operating system, and the dedicated Signature Application 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

The Assumptions defined in the Security Target and some aspects of Threats and Organisational Security Policies are not covered by the TOE itself. These aspects lead to specific Security Objectives to be fulfilled by the TOE-Environment. The Security Objectives related to the environment of the TOE´s dedicated Signature Application can be

found in the Protection Profile [10] in chapter 4.2 on which the ST is based on but not conformant to, and in the Security Target [6] and [9] chapter 4.2.

5 Architectural Information

The TOE 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. A structural overview of the TOE and an overview of the architecture including a figure of the global architecture of the TOE is given in chapter 2.1.1 of the Security Target [6] and [9]. 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] and [9]. The TOE is the composition of an IC, Smartcard Embedded Software comprising the SECCOS operating system, and dedicated Signature Application. A top level block diagram of the hardware IC including an overview of subsystems can be found in chapter 2.1 of the Security Target of the chip [12].

6 Documentation

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

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

7 IT Product Testing

The developer tested all TOE Security Functions either on real cards or with emulator tests. For all commands and functionality test, test cases are specified in order to demonstrate its expected behaviour including error cases. Hereby a representative sample including all limit values of the parameter set, e.g. all command APDUs with valid and invalid inputs were tested and all functions were tested 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

- Testing all APDU commands related to Access Control for the SF F.ACS_SIG,
- Testing the APDU commands used within the smartcard initialisation and the smartcard personalisation for the SF F.ADMIN_SIG,
- Testing the APDU commands VERIFY, CHANGE REFERENCE DATA, RESET RETRY COUNTER and PSO COMPUTE DIGITAL SIGNATURE for the SF F.PIN_SIG,
- Source code analysis and other independent evaluator tests for the SF F.DATA_INT,
- Testing all commands which (may) use Secure Messaging for the SF F.SEC_EXCH,
- Emulator testing performed by the evaluators and source code analysis for the SF F.RIP,

- SPA/DPA Analysis for Triple-DES and RSA and Fault Injection Attacks (Laser attacks) for the commands VERIFY and PSO COMPUTE DIGITAL SIGNATURE and source code analysis for the SF F.SIDE_CHAN,
- Emulator testing performed by the evaluators and source code analysis for the SF F.SELF_TEST,
- Testing APDU commands with Secure Messaging, APDU commands HASH, ENCIPHER and DECIPHER and source code analysis for the SF F.CRYPTO,
- Testing the APDU commands GENERATE (personalization phase) and GENERATE ASYMMETRIC KEY PAIR and source code analysis for the SF F.RSA_KEYGEN,
- Testing the APDU command PSO COMPUTE DIGITAL SIGNATURE for the SF F.GEN_SIG,

The evaluators have tested the TOE systematically against high attack potential during their penetration testing.

The achieved test results correspond to the expected test results.

8 Evaluated Configuration

The TOE is defined uniquely by the name and version number.

With regard to the smartcard product life cycle of the TOE (for more details about the TOE life cycle phases please read the overview of the TOE Life Cycle explained in the ST [6] and [9], chapter 2.2), the different development and production phases of the TOE with its IC including its IC Dedicated Software, covering in particular the Crypto Library and with its IC, Smartcard Embedded Software comprising the operating system, and with the dedicated Signature Application are all part of the evaluation of the TOE. For the delivery of the TOE different ways are established.

The TOE is delivered in form of complete cards or modules, i.e. after the initialisation process of the TOE has been successfully finished, final tests have been successfully conducted and the card production has been fulfilled.

Alternatively, the TOE is delivered in form of a not-initialised module or smartcard. In this case, the delivery of the modules resp. smartcards will be combined with the delivery of the customer specific Initialisation Table containing the evaluated Signature Application developed by Sagem Orga GmbH to the involved Verlag der Kreditwirtschaft. The finalised Initialisation Table has to be sent from the Verlag der Kreditwirtschaft (by a secured transfer way) to the Initialiser for loading the EEPROM initialisation data into the TOE during its initialisation phase whereat the production requirements defined in the Guidance for the Initialiser (as well delivered by Sagem Orga) have to be considered.

In the case of the delivery of modules, the last part of the smartcard finishing process, i.e. the embedding of the delivered modules and final tests, is task of the customer.

The form of the delivery of the TOE does not concern the security features of the TOE. However, the initialisation process in Flintbek, Germany is considered within the framework of the CC evaluation of the product.

The development of the TOE is done in Paderborn. Production and, if applicable, initialisation of the TOE takes place in Flintbek. Regarding the development and production environment of the underlying IC please refer to Annex A of the certification report of the chip [13].

Beside the dedicated Signature Application the TOE allows for further different kinds of (banking) applications such as GeldKarte Application, EMV Application, electronic cash Application, etc. These further applications are outside the scope of the certificate.

The evaluation results are restricted to chip cards containing the TOE with SSCD application that has been inspected during the evaluation process.

9 Results of the Evaluation

9.1 CC specific results

The Evaluation Technical Report (ETR) [7] 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 up to EAL4 extended by advice of the Certification Body for components beyond EAL 4 and guidance specific for the technology of the product [4] (AIS 34).

The following guidance specific for the technology was used:

- The Application of CC to Integrated Circuits,
- Application of Attack Potential to Smart Cards,
- Functionality classes and evaluation methodology of physical random number generators.

(see [4], AIS 1, AIS 14, AIS 19, AIS 25, AIS 26, AIS 34, AIS 36, AIS 37.)

The assurance refinements outlined in the Security Target were followed in the course of the evaluation of the TOE.

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

- All components of the class ASE,
- All components of the EAL 4 package as defined in the CC (see also part C of this report),
- The components AVA_MSU.3 and AVA_VLA.4 augmented for this TOE evaluation.

The evaluation has confirmed:

- for the Functionality: Product Specific Security Target
Common Criteria Part 2 extended
- for the Assurance: Common Criteria Part 3 conformant
EAL 4 augmented by
AVA_MSU.3 and AVA_VLA.4
- The following TOE Security Functions fulfil the claimed Strength of Function: high
    - F.ADMIN_SIG (The TSF includes a probabilistic password mechanism for the authentication of the Administrator.)
    - F.PIN_SIG (The TSF includes a probabilistic password mechanism for the authentication of the Signatory.)
    - F.CRYPTO (The TSF includes permutational and probabilistic mechanisms.)

- F.RSA_KEYGEN (The TSF includes permutational and probabilistic mechanisms.)
- F.GEN_SIG (The TSF includes permutational and probabilistic mechanisms.)

In order to assess the Strength of Function the scheme interpretations AIS 25 and AIS 26 (see [4]) were used.

For specific evaluation results regarding the development and production environment see annex B in part D of this report.

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

9.2 Results of cryptographic assessment

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

- hash functions:
  - SHA-256, SHA-384 and SHA-512 hash value calculation according the standard FIPS 180-2,
  - RIPEMD-160 according to the standard ISO 10118-3.
- algorithms for the encryption and decryption:
  - RSA algorithm according the standards PKCS1 and ISO 9796-2 with a module length of 2048 bits,
  - 3DES algorithm according the standard ANSI X9.52 with an effective key length of 112bits.

This holds for the following Security Functions:

- F.CRYPTO Cryptographic Support (providing cryptographic support for the other TSFs using cryptographic mechanisms SHA-2, RIPEMD, 3DES, RSA, RNG),
- F.SEC_EXCH Integrity and Confidentiality of Data Exchange (DES),
- F.RSA_KEYGEN RSA Key Pair Generation (RNG),
- F.GEN_SIG RSA Generation of Electronic Signatures (RSA, SHA-2, RIPEMD).

The implemented cryptographic algorithms are protected by the Security Functions:

- F.SIDE_CHAN Side Channel Analysis Control,
- F.FAIL_PROT Hardware and Software Failure Protection

against side channel analysis and fault injection.

The strength of the cryptographic algorithms was not rated in the course of this evaluation (see BSIG Section 4, Para. 3, Clause 2). According to [22] the algorithms are suitable for encryption and decryption. The validity period of each algorithm is mentioned in the official catalogue [22]

10 Obligations and notes for the usage of the TOE

The operational documents as outlined in table 2 and the Security Target [6] and [9] contain necessary information about the usage of the TOE and all security hints therein have to be considered.

Principally, the user has to follow the instructions in the user guidance documents and has to ensure the fulfilment of the Assumptions about the environment in the Security Target [6] and [9].

11 Security Target

For the purpose of publishing, the Security Target [9] of the Target of Evaluation (TOE) is provided within a separate document as Annex A of this report. It is a sanitised version of the complete Security Target [6] used for the evaluation performed. Sanitisation was performed according to the rules as outlined in the relevant CCRA policy (see AIS 35 [4]).

12 Definitions

12.1 Acronyms

3DES Triple DES

ANSI American National Standards Institute

APDU Application Protocol Data Unit

AS Application Software

ATR Answer to Reset

BS Basic Software

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

BSIG BSI-Errichtungsgesetz

CCRA Common Criteria Recognition Arrangement

CC Common Criteria for IT Security Evaluation

CEM Evaluation Methodology

CM Card Manager

DES Data Encryption Standard

DFA Differential Fault Analysis

DOC Document

DPA Differential Power Analysis

DTBS: Data To Be Signed

EAL Evaluation Assurance Level

EEPROM Electronically Erasable Programmable Read Only Memory

EHC Electronic Health Card

ES Embedded Software

ETR Evaluation Technical Report

FIPS Federal Information Processing Standards Publication

IC Integrated Circuit

ISO	International Organization for Standardization
IT	Information Technology
ITSEF	Information Technology Security Evaluation Facility
JIL	Joint Interpretation Library
MAC	Message Authentication Code
OS	Operating System
PIN	Personal Identification Number
PKCS	Public Key Cryptography Standards
PP	Protection Profile
PW	Password
RIPEMD	RACE Integrity Primitives Evaluation Message Digest, a cryptographic hash function
RNG:	Random Number Generator
ROM	Read Only Memory
RSA	Rivest Shamir Adleman Algorithm
SF	Security Function
SFP	Security Function Policy
SHA	Secure Hash Algorithm
SOF	Strength of Function
SPA	Simple Power Analysis
SSCD:	Secure Signature Creation Device
SCD:	Signature Creation Data
ST	Security Target
TOE	Target of Evaluation
TSC	TSF Scope of Control
TSF	TOE Security Functions
TSP	TOE Security Policy

12.2 Glossary

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

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

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

Informal - Expressed in natural language.

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

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

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

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

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

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

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

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

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

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

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

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

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

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

13 Bibliography

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

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

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

[4] Application Notes and Interpretations of the Scheme (AIS) as relevant for the TOE.[8]

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

[6] Security Target BSI-DSZ-2009-0449, ZKA SECCOS Sig v2.6.4, Version V1.06, Sagem Orga GmbH, 02.07.2009 (confidential document)

[7] Evaluation Technical Report (ETR), Version 1.5, Date 08.07.2009, Product ZKA SECCOS Sig v2.6.4 R1.1, Developer Sagem ORGA GmbH (confidential document)

[8] Configuration List, Version V1.08, Sagem Orga GmbH, 07.07.2009, (confidential document)

[9] Security Target BSI-DSZ-2009-0449, ZKA SECCOS Sig v2.6.4, Version V1.05, Sagem Orga GmbH, 02.07.2009 (sanitised public document)

[10] Protection Profile – Secure Signature-Creation Device Type 3, EAL 4+, BSI-PP-0006-2002, Version 1.05, July 25th 2001

[11] ETR for composition evaluation according to AIS 36 for Atmel Smart Card IC AT90SC28872RCU, BSI-DSZ-CC-0421, T-Systems GEI GmbH, Version 1.06, 08.10.2008 (confidential document)

[12] Security Target for Atmel Smart Card IC AT90SC28872RCU, registered by Bundesamt für Sicherheit in der Informationstechnik (BSI) under the reference BSI-DSZ-CC-0421, Atmel Corporation, Version 2.3, 05.12.2008 and Version 2.4 for DSZ-CC-0421-2008-MA-02 (see also next reference)

---

[8] specifically

- AIS 25, Version 3, 6 August 2007, Anwendung der CC auf Integrierte Schaltungen including JIL Document and CC Supporting Document
- AIS 26, Version 3, 6 August 2007, Evaluationsmethodologie für in Hardware integrierte Schaltungen including JIL Document and CC Supporting Document
- AIS 32, Version 1, 2 July 2001, Übernahme international abgestimmter CC-Interpretationen ins deutsche Zertifizierungsschema.
- AIS 34, Version 1.00, 1 June 2004, Evaluation Methodology for CC Assurance Classes for EAL5+
- AIS 35, Version 2.0, 12 November 2007, Öffentliche Fassung des Security Targets (ST-Lite) including JIL Document and CC Supporting Document and CCRA policies
- AIS 36, Version 2, 12 November 2007, Kompositionsevaluierung including JIL Document and CC Supporting Document
- AIS 38, Version 2.0, 28 September 2007, Reuse of evaluation results

[13] Certification Report BSI-DSZ-CC-0421-2008 for Atmel Smartcard ICs AT90SC28872RCU / AT90SC28848RCU with Atmel Cryptographic Toolbox Version 00.03.10.00 or 00.03.13.00 from Atmel Corporation, BSI, 04.12.2008 in conjunction with Assurance Continuity Maintenance Report BSI-DSZ-CC-0421-2008-MA-01, Atmel Smartcard ICs AT90SC28872RCU / AT90SC28848RCU with Atmel Cryptographic Toolbox Version 00.03.10.00 or 00.03.13.00 from Atmel Corporation, BSI, 08.01.2009 in conjunction with Assurance Continuity Maintenance Report BSI-DSZ-CC-0421-2008-MA-02, Atmel Smartcard ICs AT90SC28872RCU / AT90SC28848RCU with Atmel Cryptographic Toolbox Version 00.03.10.00 or 00.03.13.00 from Atmel Corporation, BSI, 06.04.2009

[14] Smartcard IC Platform Protection Profile, Version 1.0, July 2001, registered and certified by Bundesamt für Sicherheit in der Informationstechnik under BSI-PP-0002

[15] System Administrator Guidance for the Initialiser of the Smartcard Product ZKA SECCOS Sig v2.6.4, Version V1.00, Sagem Orga GmbH, 08.10.2008

[16] System Administrator Guidance for the Personaliser of the Smartcard Product ZKA SECCOS Sig v2.6.4, Version V1.00, Sagem Orga GmbH, 08.10.2008

[17] ZKA SECCOS Sig v2.6.4, Data Sheet, Version V1.03, Sagem ORGA GmbH, 07.07.2009

[18] Konzept zur Personalisierung von ZKA-Chipkarten (insbesondere Signaturkarten) des deutschen Kreditgewerbes mit dem Betriebssystem SECCOS 6.x, Version 1.02, 30.11.2006, Bank-Verlag GmbH, Deutscher Genossenschafts-Verlag eG, Deutscher Sparkassen Verlag GmbH, Bundesverband Öffentlicher Banken-ZVD GmbH

[19] Richtlinie 1999/93/EG des Europäischen Parlaments und des Rates vom 13. Dezember 1999 über gemeinschaftliche Rahmenbedingungen für elektronische Signaturen, Amtblatt der Europäischen Gemeinschaften, L13/12-L13/20, 19.01.2001, Europäisches Parlament und Rat der Europäischen Union

[20] Gesetz über Rahmenbedingungen für elektronische Signaturen und zur Änderung weiterer Vorschriften, Bundesgesetzblatt Nr. 22, S. 876, 16.05.2001, Dtsch. Bundestag

[21] Verordnung zur elektronischen Signatur, Bundesgesetzblatt Nr. 509, S. 3074, 16.11.2001, Dtsch. Bundestag

[22] 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, 17.11.2008, published in the Bundesanzeiger No 13, page 346, 27.01.2009

This page is intentionally left blank.

C Excerpts from the Criteria

CC Part1:

Conformance results (chapter 7.4)

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

The conformance result consists of one of the following:

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

plus one of the following:

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

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

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

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

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

CC Part 3:

Protection Profile criteria overview (chapter 8.2)

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

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

Table 3 - Protection Profile families - CC extended requirements”

Security Target criteria overview (Chapter 8.3)

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

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

Table 5 - Security Target families - CC extended requirements ”

Assurance categorisation (chapter 7.5)

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

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

Table 1: Assurance family breakdown and mapping”

Evaluation assurance levels (chapter 11)

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

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

Evaluation assurance level (EAL) overview (chapter 11.1)

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

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

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

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

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

Table 6: Evaluation assurance level summary”

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

“Objectives

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

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

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

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

“Objectives

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

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

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

“Objectives

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

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

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

“Objectives

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

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

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

“Objectives

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

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

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

“Objectives

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

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

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

“Objectives

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

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

“Objectives

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

Vulnerability analysis (AVA_VLA) (chapter 19.4)

"Objectives

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

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

"Application notes

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

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

D Annexes

List of annexes of this certification report

Annex A: Security Target provided within a separate document.

Annex B: Evaluation results regarding development and production environment 37

This page is intentionally left blank.

Annex B of Certification Report BSI-DSZ-CC-0449-2009

Evaluation results regarding development and production environment

The IT product ZKA SECCOS Sig v2.6.4 R1.1 (Target of Evaluation, TOE) has been evaluated at an accredited and licensed / approved evaluation facility using the Common Methodology for IT Security Evaluation, Version 2.3 extended by advice of the Certification Body for components beyond EAL 4 and guidance specific for the technology of the product for conformance to the Common Criteria for IT Security Evaluation (CC), Version 2.3 (ISO/IEC 15408:2005).

As a result of the TOE certification, dated 22 July 2009, the following results regarding the development and production environment apply. The Common Criteria Security Assurance Requirements

- ACM – Configuration management (i.e. ACM_AUT.1, ACM_CAP.4, ACM_SCP.2),
- ADO – Delivery and operation (i.e. ADO_DEL.2, ADO_IGS.1) and
- ALC – Life cycle support (i.e. ALC_DVS.1, ALC_LCD.1, ALC_TAT.1),

are fulfilled for the development and production sites of the TOE listed below:

(a) Sagem Sécurité, 18 Chaussée Jules César, 95520 Osny, France (Development)

(b) Sagem Orga GmbH, Riemekestraße 160, Office Center Almepark, Building G, level 04 and 05, 33106 Paderborn, Germany (Development)

(c) Sagem Orga GmbH, Konrad-Zuse-Ring 1, 24220 Flintbek, Germany (card production and initialisation site)

(d) For development and productions sites regarding the "AT90SC28872RCU with related Cryptographic Toolbox 00.03.10.00 (TBX)" provided by Atmel Corporation please refer to the certification report BSI-DSZ-CC-0421.

For the sites listed above, the requirements have been specifically applied in accordance with the Security Target [6] and [9]. The evaluators verified, that the Threats, Security Objectives and Requirements for the TOE life cycle phases up to delivery (as stated in the Security Target [6] and [9]) are fulfilled by the procedures of these sites.

This page is intentionally left blank.