Federal Office
for Information Security

Certification Report

BSI-DSZ-CC-0821-2014

for

AKD eID Card 1.0

from

Agencija za komercijalnu djelatnost d.o.o.

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-0821-2014

Secure Signature Creation Device (SSCD)

AKD eID Card 1.0

from	Agencija za komercijalnu djelatnost d.o.o.
PP Conformance:	Protection Profile for Secure Signature Creation Device - Part 2: Device with Key Generation Version 2.01, January 2012, BSI-CC-PP-0059-2009-MA-01, Protection profiles for secure signature creation device - Part 4: Extension for device with key generation and trusted communication with certificate generation application 1.0.1, November 2012, BSI-CC-PP-0071-2012 , Protection profiles for secure signature creation device - Part 3: Device with key import Version 1.0.2, July 2012, BSI-CC-PP-0075-2012
Functionality:	PP conformant Common Criteria Part 2 extended
Assurance:	Common Criteria Part 3 conformant EAL 4 augmented by AVA_VAN.5, ALC_DVS.2

SOGIS
Recognition Agreement

Common Criteria

The IT product identified in this certificate has been evaluated at an approved evaluation facility using the Common Methodology for IT Security Evaluation (CEM), Version 3.1 extended by advice of the Certification Body for components beyond EAL 5 and guidance specific for the technology of the product for conformance to the Common Criteria for IT Security Evaluation (CC), Version 3.1.

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.

Common Criteria
Recognition Arrangement
for components up to
EAL 4

Bonn, 29 October 2014

For the Federal Office for Information Security

DAkkS
Deutsche
Akkreditierungsstelle
D-ZE-19615-01-00

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 on the Federal Office for Information Security (BSI-Gesetz - BSIG) of 14 August 2009, Bundesgesetzblatt I p. 2821

Contents

A Certification....7
1 Specifications of the Certification Procedure....7
2 Recognition Agreements....7
3 Performance of Evaluation and Certification....8
4 Validity of the Certification Result....9
5 Publication....9
B Certification Results....11
1 Executive Summary....12
2 Identification of the TOE....13
3 Security Policy....14
4 Assumptions and Clarification of Scope....14
5 Architectural Information....15
6 Documentation....15
7 IT Product Testing....15
8 Evaluated Configuration....17
9 Results of the Evaluation....17
10 Obligations and Notes for the Usage of the TOE....18
11 Security Target....19
12 Definitions....19
13 Bibliography....21
C Excerpts from the Criteria....23
CC Part 1:....23
CC Part 3:....24
D Annexes....33

A Certification

1 Specifications of the Certification Procedure

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

- Act on the Federal Office for Information Security[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 ISO/IEC 17065 standard
- BSI certification: Technical information on the IT security certification, Procedural Description (BSI 7138) [3]
- BSI certification: Requirements regarding the Evaluation Facility (BSI 7125) [3]
- Common Criteria for IT Security Evaluation (CC), Version 3.1[5] [1] also published as ISO/IEC 15408.
- Common Methodology for IT Security Evaluation (CEM), Version 3.1 [2] also published as ISO/IEC 18045.
- BSI certification: Application Notes and Interpretation of the Scheme (AIS) [4]

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 European Recognition of ITSEC/CC – Certificates (SOGIS-MRA)

The SOGIS-Mutual Recognition Agreement (SOGIS-MRA) Version 3 became effective in April 2010. It defines the recognition of certificates for IT-Products at a basic recognition level and in addition at higher recognition levels for IT-Products related to certain technical domains only.

The basic recognition level includes Common Criteria (CC) Evaluation Assurance Levels EAL1 to EAL4 and ITSEC Evaluation Assurance Levels E1 to E3 (basic). For higher

---

2 Act on the Federal Office for Information Security (BSI-Gesetz - BSIG) of 14 August 2009, Bundesgesetzblatt I p. 2821

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 12 February 2007 in the Bundesanzeiger dated 23 February 2007, p. 3730

recognition levels the technical domain Smart card and similar Devices has been defined. It includes assurance levels beyond EAL4 resp. E3 (basic). In addition, certificates issued for Protection Profiles based on Common Criteria are part of the recognition agreement.

As of September 2011 the new agreement has been signed by the national bodies of Austria, Finland, France, Germany, Italy, The Netherlands, Norway, Spain, Sweden and the United Kingdom. Details on recognition and the history of the agreement can be found at https://www.bsi.bund.de/zertifizierung.

The SOGIS-MRA logo printed on the certificate indicates that it is recognised under the terms of this agreement by the nations listed above. This certificate is recognized under SOGIS-MRA for all assurance components selected.

2.2 International Recognition of CC – Certificates (CCRA)

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 September 2011 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 website: 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 by the nations listed above.

As the product certified has been accepted into the certification process before 08 September 2014, this certificate is recognized according to the rules of CCRA-2000, i.e. up to and including CC part 3 EAL 4 components. The evaluation contained the components AVA_VAN.5 and ALC_DVS.2 that are not mutually recognised in accordance with the provisions of the CCRA-2000, for mutual recognition the EAL 4 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 AKD eID Card 1.0 has undergone the certification procedure at BSI.

The evaluation of the product AKD eID Card 1.0 was conducted by TÜV Informationstechnik GmbH. The evaluation was completed on 1 October 2014. TÜV Informationstechnik GmbH is an evaluation facility (ITSEF)[6] recognised by the certification body of BSI.

For this certification procedure the sponsor and applicant is: Agencija za komercijalnu djelatnost d.o.o..

The product was developed by: Agencija za komercijalnu djelatnost d.o.o..

[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, as specified in the following report and in the Security Target.

For the meaning of the assurance levels 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 evolve over time, the resistance of the certified version of the product against new attack methods needs to be re-assessed. Therefore, the sponsor should apply for the certified product being monitored within the assurance continuity program of the BSI Certification Scheme (e.g. by a re-certification). Specifically, if results of the certification are used in subsequent evaluation and certification procedures, in a system integration process or if a user's risk management needs regularly updated results, it is recommended to perform a re-assessment on a regular e.g. annual 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 AKD eID Card 1.0 has been included in the BSI list of certified products, which is published regularly (see also Internet: https://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] Agencija za komercijalnu djelatnost d.o.o.
Savska cesta 31
10000 Zagreb

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 AKD Electronic Identity Card 1.0 is a SSCD (Secure Signature Creation Device) in the appearance of a contact smart card. The TOE consists of the Java Card applet AKD eID Card 1.0, executed on the underlying JCOP platform NXP J2E081_M64 Secure Smart Card Controller Revision 3 (certification ID NSCIB-CC-13-37761-CR2 [15]), and the hardware platform. The hardware platform comprises the Crypto Library V2.7/V2.9 (certification ID BSI-DSZ-CC-0633-V2-2014 [16]) and the NXP Secure Smart Card Controller P5CC081V1A (certification ID BSI-DSZ-CC-0857-2013 [17]). The TOE may generate internally or externally signing key and communicates with the signature creation application in a protected manner. In secure environment the TOE may also be used to create advanced electronic signatures or qualified electronic signatures. The TOE implements the following functionalities, according to the strictly claimed protection profiles for secure signature creation devices, certificated by the BSI (BSI-CC-PP-0059-2009-MA-01 [7], BSI-CC-PP-0071-2012 [8] and BSI-CC-PP-0075-2012 [9]):

- On chip and external key generation
- Advanced or qualified digital signature
- Certificate information application
- Knowledge based user authentication with two PINs and one PUK
- Secure Messaging
- Symmetric or asymmetric device authentication
- Administrator role authentication and post issuance management of the card
- Signature generation for Client/Server authentication
- Encryption key decipherment
- Certificate verification
- Self protection

The Security Target [6] is the basis for this certification. It is based on the certified

- Protection Profile for Secure Signature Creation Device - Part 2: Device with Key Generation Version 2.01, January 2012, BSI-CC-PP-0059-2009-MA-01 [7];
- Protection profiles for secure signature creation device - Part 4: Extension for device with key generation and trusted communication with certificate generation application 1.0.1, November 2012, BSI-CC-PP-0071-2012 [8];
- Protection profiles for secure signature creation device - Part 3: Device with key import Version 1.0.2, July 2012, BSI-CC-PP-0075-2012 [9].

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_VAN.5, ALC_DVS.2.

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

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

TOE Security Functionality	Addressed issue
SF.USER	User authentication
SF.DEV	Device authentication
SF.SM	Trusted channel
SF.ACCESS	Role authentication
SF.CRYPTO	Cryptographic functions - provided by the certified platform
SF.PROTECT	Self protection

Table 1: TOE Security Functionalities

For more details please refer to the Security Target [6], chapter 10.

The assets to be protected by the TOE are defined in the Security Target [6], chapter 6.1. Based on these assets the TOE Security Problem is defined in terms of Assumptions, Threats and Organisational Security Policies. This is outlined in the Security Target [6], chapter 6 and 7.

This certification covers the configurations of the TOE as outlined in chapter 8 of this report.

The vulnerability assessment results as stated within this certificate do not include a rating for those cryptographic algorithms and their implementation suitable for encryption and decryption (see BSIG Section 9, Para. 4, Clause 2).

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:

AKD eID Card 1.0

The following table outlines the TOE deliverables:

No	Type	Identifier	Release	Form of Delivery
1	HW/ SW	Finalized composite TOE	Java Card applet AKD eID Card 1.0, executed on the underlying JCOP platform NXP J2E081_M64 Secure Smart Card Controller Revision 3, comprising of Crypto Library V2.7/V2.9 and the NXP Secure Smart Card Controller P5CC081V1A	Delivery in sealed boxes / crates by shipping company or courier under dual control

No	Type	Identifier	Release	Form of Delivery
2	KEYS	Personalization-key-set	n/a	Delivery in three separated components either in three separate PGP encrypted mails or the three Key Custodians enter the components directly to the personalization centre HSM.
3	DOC	User guidance [12]	Version 1.2 Date 2014-08-14	Delivery by PGP encrypted e-mail with previous verification of the client recipient authenticity.

Table 2: Deliverables of the TOE

The IC is delivered from the IC production site of NXP to AKD. This delivery is covered by the certified JCOP platform (NSCIB-CC-13-37761-CR2). At the AKD production and development site, the composite TOE is manufactured including the chip integration and the applet installation. According to the Security Target, the composite TOE is finalized after initialization / pre-personalization at AKD and then delivered to the personalization site. Therefore the personalization agent is the client and the receiver of the finalized TOE. See also figure 3, TOE life cycle, in the Security Target [6].

The verification of the delivered composite TOEs unique identity is gained by the identification mechanisms according to the user guidance [12]. The finalized composite TOE is delivered from AKD to the personalization agent who verifies the identity by the ATR (Answer To Reset) check which should return the expected value: ‘3B FF 13 00 00 81 31 FE 45 00 31 B9 64 04 44 EC C1 73 94 01 80 82 90 00 12’ [12], chapter 5.1. Additional the INS_GET_VERSION command is used to verify the correct version of the applet by sending ’80 26 00 00 00’ or ‘8C 26 00 00 00’ and checking that the returned version matches the expected value for the applet version 1.0: ’02 00 01 00 00’ [12], chapters 5.1.2 and 6.8.2.

3 Security Policy

The Security Policy is expressed by the set of Security Functional Requirements and implemented by the TOE. It is defined according to the certified Protection Profiles for Secure Signature Creation Device - Part 2: Device with Key Generation Version 2.01, January 2012, BSI-CC-PP-0059-2009-MA-01[7], for secure signature creation device - Part 4: Extension for device with key generation and trusted communication with certificate generation application 1.0.1, November 2012, BSI-CC-PP-0071-2012 [8], and for secure signature creation device - Part 3: Device with key import Version 1.0.2, July 2012, BSI-CC-PP-0075-2012 [9] by the Security Objectives and Requirements given in these Protection Profiles and according the the Security Target [6].

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 List of objectives which have to be met by the the environment can be found in the Security Target [6], chapter 7.2.

5 Architectural Information

The AKD Electronic Identity Card 1.0 is a composite TOE which consists of the Java Card applet AKD eID Card 1.0, executed on the underlying JCOP platform NXP J2E081_M64 Secure Smart Card Controller Revision 3 (certification ID NSCIB-CC-13-37761-CR2 [15]), and the hardware platform. The hardware platform comprises the Crypto Library V2.7/V2.9 (certification ID BSI-DSZ-CC-0633-V2-2014 [16]) and the NXP Secure Smart Card Controller P5CC081V1A (certification ID BSI-DSZ-CC-0857-2013 [17]).

The AKD Electronic Identity Card 1.0 applet consists of four subsystems. Each subsystem package implements functionalities in modules.

- The applet subsystem contains two modules regarding secure messaging and the applet itself.
- The file system subsystem contains the modules for the usage of dedicated, elementary and normal files.
- The Security Data Object subsystem implements the management of the security functionality and summarizes modules for the security context and environment, the different key-sets, and the PIN.
- The Utility subsystem includes, besides other functions, also a common module providing utilities used by most of all other modules.

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

Developer Tests

The TOE consists of the AKD eID Card which is a Java Card applet developed by AKD, built on secure platform NXP J2E081 Secure Smart Card Controller Rev 3 (JCOP 2.4.2 R3).

All functional tests are done on a test platform including a set of libraries that are used for tests and test scripts development. The test scripts are further organized in test campaigns and executed either as all tests of a campaign or as single tests, with an automatic creation of tests reports. The test reports are generated in HTML format and provide all information about the test execution event: general information, summary results and execution result for each test.

To run a test campaign the TOE on the smartcard shall undergo well-defined preparative procedures. The card preparation is implemented as a script by the developer.

The test reports include details and comments of the used command structure and the expected results. The evaluator determined that the test prerequisites, test steps, and expected results adequately test each TSFI, and they are consistent with the descriptions of the TSFI in the functional specification.

The test documentation includes all details about the set-up procedures, the test procedure and information about the execution of the tests. They are suitable to test the TSF portion mediated by the related interface adequately.

The analysis of the test procedures show that all interfaces of SFR-enforcing modules are tested. All TSFI are present and covered by tests.

The actual test results correspond to the expected test results. The TOE has passed all tests so that all TSF have been successfully tested against the functional specification and the design of the TOE. The developer test results demonstrate that the TSF perform as specified.

Evaluator Tests

The TOE consists of the Java Card applet AKD eID Card which is developed by AKD and built on secure platform NXP J2E081 Secure Smart Card Controller Rev 3 (JCOP 2.4.2 R3).

The evaluator repeated all developer tests independently and additionally performed tests regarding the TSF and the preparative procedures on his own, for which he used the scripts provided by the developer.

The evaluator used test samples provided by the developer. Additionally the evaluator created, installed and configured test samples of the TOE on his own according to the user guidance documentation. There is only one configuration of the TOE that is delivered in to personalization agent. For the tests this configuration was used.

The test logs and the test documentation include details and comments on the test configuration, on the test equipment used, on the used command structure and the expected results. The test prerequisites, test steps, and expected results adequately test the related TSFI, and they are consistent with the descriptions of the TSFI in the functional specification.

The test results have not shown any deviations between the expected test results and the actual test results.

Penetration Testing

Based on the list of potential vulnerabilities applicable to the TOE in its operational environment the evaluator devised the attack scenarios for penetration tests to verify if they could be exploited in the TOE’s operational environment.

The evaluator performed applet code review during his evaluation, to verify the implementation of the requirements recommended in the platform's ETR for composition and guidance, as well as of the security mechanisms of the applet in general. Further aspects were covered by additional independent tests.

There is only one allowed configuration of the TOE which will be delivered to personalization agent. The evaluator performed penetration testing on this configuration and additional tests on other test configurations.

Attack scenarios that have been tested are Perturbation attacks: Program flow disturbance with LFI. The SFRs that were penetration tested belong to the security funtion SF.PROTECT and are FDP_RIP.1, FDP_SDI.2/Persistent, FDP_SDI.2/DTBS, FPT_EMS.1, FPT_FLS.1, FPT_PHP.1, FPT_PHP.3, FPT_TST.1. The remaining SFRs were analysed, but not penetration tested due to non-exploitability of the related attack scenarios in the TOE’s operational environment, assuming an attacker with a High attack potential.

The overall test result is that no deviations were found between the expected and the actual test results. No attack scenario with the attack potential High was actually successful in the TOE's operational environment as defined in the ST [6] provided that all measures required by the developer are applied.

8 Evaluated Configuration

The AKD Electronic Identity Card 1.0 is a composite TOE which consists of the Java Card applet AKD eID Card 1.0, executed on the underlying JCOP platform NXP J2E081_M64 Secure Smart Card Controller Revision 3 (certification ID NSCIB-CC-13-37761-CR2 [15]), and the hardware platform. The hardware platform comprises the Crypto Library V2.7/V2.9 (certification ID BSI-DSZ-CC-0633-V2-2014 [16]) and the NXP Secure Smart Card Controller P5CC081V1A (certification ID BSI-DSZ-CC-0857-2013 [17]). The evaluated TOE is delivered in one configuration, parameterized for symmetric and asymmetric authentication. According to the Security Target, the TOE is finalized after initialization / pre-personalization and then delivered to the personalization site. Therefore the personalization agent is the client and the receiver of the finalized TOE.

9 Results of the Evaluation

9.1 CC specific results

The Evaluation Technical Report (ETR) [11] 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 EAL5 extended by advice of the Certification Body for components beyond EAL 5 and guidance specific for the technology of the product [4] (AIS 34).

The following guidance specific for the technology was used:

(i) The Application of CC to Integrated Circuits

(ii) Application of Attack Potential to Smart Cards

(iii) Composite product evaluation for Smart Cards and similar devices (see AIS 36). According to this concept the relevant guidance documents of the underlying platform and the documents ETR for Composition from the platform evaluations (i.e. on the underlying JCOP platform NXP J2E081_M64 Secure Smart Card Controller Revision 3 (certification ID NSCIB-CC-13-37761-CR2) [18], on the Crypto Library V2.7/V2.9 (certification ID BSI-DSZ-CC-0633-V2-2014) [19] and on the NXP Secure Smart Card Controller P5CC081V1A (certification ID BSI-DSZ-CC-0857-2013) [20]) have been applied in the TOE evaluation.

(see [4], AIS 25, AIS 26, AIS 34, AIS 36).

Random number generation according to class DRG.3 and DRG.2 of AIS 20 is JCOP-functionality and has been covered by the platform certificate.

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

- All components of the EAL 4 package including the class ASE as defined in the CC (see also part C of this report)

- The components AVA_VAN.5, ALC_DVS.2 augmented for this TOE evaluation.

The evaluation has confirmed:

- PP Conformance:
  - Protection Profile for Secure Signature Creation Device - Part 2: Device with Key Generation Version 2.01, January 2012, BSI-CC-PP-0059-2009-MA-01 [7]
  - Protection Profile for secure signature creation device - Part 4: Extension for device with key generation and trusted communication with certificate generation application 1.0.1, November 2012, BSI-CC-PP-0071-2012 [8]
  - Protection Profile for secure signature creation device - Part 3: Device with key import Version 1.0.2, July 2012, BSI-CC-PP-0075-2012 [9]
- for the Functionality: PP conformant
  Common Criteria Part 2 extended
- for the Assurance: Common Criteria Part 3 conformant / extended
  EAL 4 augmented by AVA_VAN.5, ALC_DVS.2

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 strength of the cryptographic algorithms was not rated in the course of this certification procedure (see BSIG Section 9, Para. 4, Clause 2). But Cryptographic Functionalities with a security level of lower than 100 bits can no longer be regarded as secure without considering the application context. Therefore, for these functionalities it shall be checked whether the related crypto operations are appropriate for the intended system. Some further hints and guidelines can be derived from the 'Technische Richtlinie BSI TR-02102' (https://www.bsi.bund.de).

The cryptographic algorithms that are used by the TOE to enforce its security policy are detailed with all necessary information in the ST [6] chapter 12, Crypto-Disclaimer.

Any Cryptographic Functionality that is marked in column '*Security Level above 100 Bits*' in the referenced table with '*no*' achieves a security level of lower than 100 Bits (in general context).

According to [13] and [14] the algorithms are suitable for create advanced electronic signatures or qualified electronic signatures The validity period of each algorithm is mentioned in [13] and [14].

10 Obligations and Notes for the Usage of the TOE

The documents as outlined in table 2 contain necessary information about the usage of the TOE and all security hints therein have to be considered. In addition all aspects of Assumptions, Threats and OSPs as outlined in the Security Target not covered by the TOE itself need to be fulfilled by the operational environment of the TOE.

The customer or user of the product shall consider the results of the certification within his system risk management process. In order for the evolution of attack methods and techniques to be covered, he should define the period of time until a re-assessment of the TOE is required and thus requested from the sponsor of the certificate.

The limited validity for the usage of cryptographic algorithms as outlined in chapter 9 has to be considered by the user and his system risk management process.

11 Security Target

For the purpose of publishing, the Security Target [6] 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 [10] 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

AIS Application Notes and Interpretations of the Scheme

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

BSIG BSI-Gesetz / Act on the Federal Office for Information Security

CCRA Common Criteria Recognition Arrangement

CC Common Criteria for IT Security Evaluation

CEM Common Methodology for Information Technology Security Evaluation

EAL Evaluation Assurance Level

ETR Evaluation Technical Report

IT Information Technology

ITSEC Information Technology Security Evaluation Criteria

ITSEF Information Technology Security Evaluation Facility

PP Protection Profile

SAR Security Assurance Requirement

SFP Security Function Policy

SFR Security Functional Requirement

ST Security Target

TOE Target of Evaluation

TSF TOE Security Functionality

12.2 Glossary

Augmentation - The addition of one or more requirement(s) to a 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 - A passive entity in the TOE, that contains or receives information, and upon which subjects perform operations.

Protection Profile - An implementation-independent statement of security needs for a TOE type.

Security Target - An implementation-dependent statement of security needs for a specific identified TOE.

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

Subject - An active entity in the TOE that performs operations on objects.

Target of Evaluation - A set of software, firmware and/or hardware possibly accompanied by guidance.

TOE Security Functionality - Combined functionality of all hardware, software, and firmware of a TOE that must be relied upon for the correct enforcement of the SFRs.

13 Bibliography

[1] Common Criteria for Information Technology Security Evaluation, Version 3.1,
Part 1: Introduction and general model, Revision 4, September 2012
Part 2: Security functional components, Revision 4, September 2012
Part 3: Security assurance components, Revision 4, September 2012

[2] Common Methodology for Information Technology Security Evaluation (CEM), Evaluation Methodology, Version 3.1, Rev. 4, September 2012

[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), periodically updated list published also in the BSI Website

[6] Security Target Lite BSI-DSZ-CC-0821-2014, AKD Electronic Identity Card, Version 1.3, Date 2014-09-26, AKD (sanitised public document)

[7] Protection Profile for Secure Signature Creation Device - Part 2: Device with Key Generation Version 2.01, January 2012, BSI-CC-PP-0059-2009-MA-01,

[8] Protection Profile for secure signature creation device - Part 4: Extension for device with key generation and trusted communication with certificate generation application 1.0.1, November 2012, BSI-CC-PP-0071-2012

[9] Protection Profile for secure signature creation device - Part 3: Device with key import Version 1.0.2, July 2012, BSI-CC-PP-0075-2012

[10] Security Target BSI-DSZ-CC-0821-2014, AKD Electronic Identity Card, Version 1.3, Date 2014-09-26, AKD (confidential document)

[11] Evaluation Technical Report (ETR) for AKD Electronic Identity Card 1.0, Version 2, Date 2014-09-26, TÜV Informationstechnik GmbH, (confidential document)

[12] AKD Electronic Identity Card, User Guidance, Version 1.2, Date 2014-08-14, AKD

[13] Bekanntmachung zur elektronischen Signatur nach dem Signaturgesetz und der Signaturveraordnung (Übersicht über geeignete Algorithmen), BNetzA Banz AT 20.02.2014

[8] specifically

- AIS 25, Version 8, Anwendung der CC auf Integrierte Schaltungen including JIL Document and CC Supporting Document
- AIS 26, Version 9, Evaluationsmethodologie für in Hardware integrierte Schaltungen including JIL Document and CC Supporting Document
- AIS 32, Version 7, CC-Interpretationen im deutschen Zertifizierungsschema
- AIS 34, Version 3, Evaluation Methodology for CC Assurance Classes for EAL5+ (CCv2.3 & CCv3.1) and EAL6 (CCv3.1)
- AIS 35, Version 1, Öffentliche Fassung des Security Targets (ST-Lite) including JIL Document and CC Supporting Document and CCRA policies
- AIS 36, Version 4, Kompositionsevaluierung including JIL Document and CC Supporting Document

[14] BSI – Technische Richtlinie BSI TR-02102-1, Kryptographische Verfahren: Empfehlungen und Schlüssellängen, Version 1.0, Stand 2014, 10.02.2014, Bundesamt für Sicherheit in der Informationstechnik

[15] Certification Report NXP J3E081_M64, J3E081_M66, J2E081_M64, J3E041_M66, J3E016_M66, J3E016_M64, J3E041_M64 Secure Smart Card Controller Revision 3, Version 1, 05.08.2013, NSCIB-CC-13-37761-CR, TÜV Rheinland Nederland B.V. including maintenance certification report NSCIB-CC-13-37761-CR2, 25.08.2014

[16] Certification Report, BSI-DSZ-CC-0633-V2-2014 for Crypto Library V2.7/V2.9 on SmartMX P5CD016/021/041/051 and P5Cx081 V1A/V1A(s) from NXP Semiconductors Germany GmbH, 16 July 2014 BSI

[17] Certification Report, BSI-DSZ-CC-0857-2013 for NXP Secure Smart Card ControllersP5CD016/021/041/051 and P5Cx081 V1A/ V1A(s) from NXP Semiconductors Germany GmbH, 12.06.2013, BSI

[18] ETR for Composite Evaluation NXP J3E081_M64, J3E081_M66, J2E081_M64, J3E041_M66, J3E016_M66, J3E016_M64, J3E041_M64 Secure Smart Card Controller Revision 3 EAL5+, Version 3.0, 13.08.2014, NSCIB-13-37761-CR2, Brightsight, (confidential document)

[19] ETR for Composition, Crypto Library V2.7/2.9 on SmartMX P5CD016/021/041/051 and P5Cx081 V1A/V1A(s) according to AIS36, version 6, certification ID BSI-DSZ-CC-0633-V2-2014, 26.06.2014, (confidential document)

[20] ETR for Composition according to AIS 36, NXP Secure Smart Card Controllers P5CD016/021/041/051 and P5Cx081V1A/ V1A(s), Version 1.5, 04.06.2013, BSI-DSZ-CC-0857-2013, (confidential document)

C Excerpts from the Criteria

CC Part 1:

Conformance Claim

“The conformance claim indicates the source of the collection of requirements that is met by a PP or ST that passes its evaluation. This conformance claim contains a CC conformance claim that:

- describes the version of the CC to which the PP or ST claims conformance.
- describes the conformance to CC Part 2 (security functional requirements) as either:
  - **CC Part 2 conformant** - A PP or ST is CC Part 2 conformant if all SFRs in that PP or ST are based only upon functional components in CC Part 2, or
  - **CC Part 2 extended** - A PP or ST is CC Part 2 extended if at least one SFR in that PP or ST is not based upon functional components in CC Part 2.
- describes the conformance to CC Part 3 (security assurance requirements) as either:
  - **CC Part 3 conformant** - A PP or ST is CC Part 3 conformant if all SARs in that PP or ST are based only upon assurance components in CC Part 3, or
  - **CC Part 3 extended** - A PP or ST is CC Part 3 extended if at least one SAR in that PP or ST is not based upon assurance components in CC Part 3.

Additionally, the conformance claim may include a statement made with respect to packages, in which case it consists of one of the following:

- Package name Conformant - A PP or ST is conformant to a pre-defined package (e.g. EAL) if:
  - the SFRs of that PP or ST are identical to the SFRs in the package, or
  - the SARs of that PP or ST are identical to the SARs in the package.
- Package name Augmented - A PP or ST is an augmentation of a predefined package if:
  - the SFRs of that PP or ST contain all SFRs in the package, but have at least one additional SFR or one SFR that is hierarchically higher than an SFR in the package.
  - the SARs of that PP or ST contain all SARs in the package, but have at least one additional SAR or one SAR that is hierarchically higher than an SAR in the package.

Note that when a TOE is successfully evaluated to a given ST, any conformance claims of the ST also hold for the TOE. A TOE can therefore also be e.g. CC Part 2 conformant.

Finally, the conformance claim may also include two statements with respect to Protection Profiles:

- PP Conformant - A PP or TOE meets specific PP(s), which are listed as part of the conformance result.
- Conformance Statement (Only for PPs) - This statement describes the manner in which PPs or STs must conform to this PP: strict or demonstrable. For more information on this Conformance Statement, see Annex D.”

CC Part 3:

Class APE: Protection Profile evaluation (chapter 10)

“Evaluating a PP is required to demonstrate that the PP is sound and internally consistent, and, if the PP is based on one or more other PPs or on packages, that the PP is a correct instantiation of these PPs and packages. These properties are necessary for the PP to be suitable for use as the basis for writing an ST or another PP.

Assurance Class	Assurance Components
Class APE: Protection Profile evaluation	APE_INT.1 PP introduction
	APE_CCL.1 Conformance claims
	APE_SPD.1 Security problem definition
	APE_OBJ.1 Security objectives for the operational environment APE_OBJ.2 Security objectives
	APE_ECD.1 Extended components definition
	APE_REQ.1 Stated security requirements APE_REQ.2 Derived security requirements

APE: Protection Profile evaluation class decomposition”

Class ASE: Security Target evaluation (chapter 11)

“Evaluating an ST is required to demonstrate that the ST is sound and internally consistent, and, if the ST is based on one or more PPs or packages, that the ST is a correct instantiation of these PPs and packages. These properties are necessary for the ST to be suitable for use as the basis for a TOE evaluation.”

Assurance Class	Assurance Components
Class ASE: Security Target evaluation	ASE_INT.1 ST introduction
	ASE_CCL.1 Conformance claims
	ASE_SPD.1 Security problem definition
	ASE_OBJ.1 Security objectives for the operational environment ASE_OBJ.2 Security objectives
	ASE_ECD.1 Extended components definition
	ASE_REQ.1 Stated security requirements ASE_REQ.2 Derived security requirements
	ASE_TSS.1 TOE summary specification ASE_TSS.2 TOE summary specification with architectural design summary

ASE: Security Target evaluation class decomposition

Security assurance components (chapter 7)

“The following Sections describe the constructs used in representing the assurance classes, families, and components.“
“Each assurance class contains at least one assurance family.”
“Each assurance family contains one or more assurance components.”

The following table shows the assurance class decomposition.

Assurance Class	Assurance Components
ADV: Development	ADV_ARC.1 Security architecture description
	ADV_FSP.1 Basic functional specification ADV_FSP.2 Security-enforcing functional specification ADV_FSP.3 Functional specification with complete summary ADV_FSP.4 Complete functional specification ADV_FSP.5 Complete semi-formal functional specification with additional error information ADV_FSP.6 Complete semi-formal functional specification with additional formal specification
	ADV_IMP.1 Implementation representation of the TSF ADV_IMP.2 Implementation of the TSF
	ADV_INT.1 Well-structured subset of TSF internals ADV_INT.2 Well-structured internals ADV_INT.3 Minimally complex internals
	ADV_SPM.1 Formal TOE security policy model
	ADV_TDS.1 Basic design ADV_TDS.2 Architectural design ADV_TDS.3 Basic modular design ADV_TDS.4 Semiformal modular design ADV_TDS.5 Complete semiformal modular design ADV_TDS.6 Complete semiformal modular design with formal high-level design presentation

Assurance Class	Assurance Components
AGD: Guidance documents	AGD_OPE.1 Operational user guidance
	AGD_PRE.1 Preparative procedures
ALC: Life cycle support	ALC_CMC.1 Labelling of the TOE ALC_CMC.2 Use of a CM system ALC_CMC.3 Authorisation controls ALC_CMC.4 Production support, acceptance procedures and automation ALC_CMC.5 Advanced support
	ALC_CMS.1 TOE CM coverage ALC_CMS.2 Parts of the TOE CM coverage ALC_CMS.3 Implementation representation CM coverage ALC_CMS.4 Problem tracking CM coverage ALC_CMS.5 Development tools CM coverage
	ALC_DEL.1 Delivery procedures
	ALC_DVS.1 Identification of security measures ALC_DVS.2 Sufficiency of security measures
	ALC_FLR.1 Basic flaw remediation ALC_FLR.2 Flaw reporting procedures ALC_FLR.3 Systematic flaw remediation
	ALC_LCD.1 Developer defined life-cycle model ALC_LCD.2 Measurable life-cycle model
	ALC_TAT.1 Well-defined development tools ALC_TAT.2 Compliance with implementation standards ALC_TAT.3 Compliance with implementation standards - all parts
ATE: Tests	ATE_COV.1 Evidence of coverage ATE_COV.2 Analysis of coverage ATE_COV.3 Rigorous analysis of coverage
	ATE_DPT.1 Testing: basic design ATE_DPT.2 Testing: security enforcing modules ATE_DPT.3 Testing: modular design ATE_DPT.4 Testing: implementation representation
	ATE_FUN.1 Functional testing ATE_FUN.2 Ordered functional testing
	ATE_IND.1 Independent testing – conformance ATE_IND.2 Independent testing – sample ATE_IND.3 Independent testing – complete
AVA: Vulnerability assessment	AVA_VAN.1 Vulnerability survey AVA_VAN.2 Vulnerability analysis AVA_VAN.3 Focused vulnerability analysis AVA_VAN.4 Methodical vulnerability analysis AVA_VAN.5 Advanced methodical vulnerability analysis

Assurance class decomposition

Evaluation assurance levels (chapter 8)

“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 8.1)

“Table 1 represents a summary of the EALs. The columns represent a hierarchically ordered set of EALs, while the rows represent assurance families. Each number in the resulting matrix identifies a specific assurance component where applicable.

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

These EALs consist of an appropriate combination of assurance components as described in Chapter 7 of this CC 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 augmented with extended assurance requirements.

Assurance Class	Assurance Family	Assurance Components by Evaluation Assurance Level						
		EAL1	EAL2	EAL3	EAL4	EAL5	EAL6	EAL7
Development	ADV_ARC		1	1	1	1	1	1
	ADV_FSP	1	2	3	4	5	5	6
	ADV_IMP				1	1	2	2
	ADV_INT					2	3	3
	ADV_SPM						1	1
	ADV_TDS		1	2	3	4	5	6
Guidance Documents	AGD_OPE	1	1	1	1	1	1	1
	AGD_PRE	1	1	1	1	1	1	1
Life cycle Support	ALC_CMC	1	2	3	4	4	5	5
	ALC_CMS	1	2	3	4	5	5	5
	ALC_DEL		1	1	1	1	1	1
	ALC_DVS			1	1	1	2	2
	ALC_FLR							
	ALC_LCD			1	1	1	1	2
	ALC_TAT				1	2	3	3
Security Target Evaluation	ASE_CCL	1	1	1	1	1	1	1
	ASE_ECD	1	1	1	1	1	1	1
	ASE_INT	1	1	1	1	1	1	1
	ASE_OBJ	1	2	2	2	2	2	2
	ASR_REQ	1	2	2	2	2	2	2
	ASE_SPD		1	1	1	1	1	1
	ASE_TSS	1	1	1	1	1	1	1
Tests	ATE_COV		1	2	2	2	3	3
	ATE_DPT			1	1	3	3	4
	ATE_FUN		1	1	1	1	2	2
	ATE_IND	1	2	2	2	2	2	3
Vulnerability assessment	AVA_VAN	1	2	2	3	4	5	5

Table 1: Evaluation assurance level summary”

Evaluation assurance level 1 (EAL1) - functionally tested (chapter 8.3)

“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 requires only a limited security target. It is sufficient to simply state the SFRs that the TOE must meet, rather than deriving them from threats, OSPs and assumptions through security objectives.

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.”

Evaluation assurance level 2 (EAL2) - structurally tested (chapter 8.4)

“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 practise. 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 8.5)

“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 practises.

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 8.6)

“Objectives

EAL4 permits a developer to gain maximum assurance from positive security engineering based on good commercial development practises 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 8.7)

“Objectives

EAL5 permits a developer to gain maximum assurance from security engineering based upon rigorous commercial development practises 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 8.8)

“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 8.9)

“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.”

Class AVA: Vulnerability assessment (chapter 16)

“The AVA: Vulnerability assessment class addresses the possibility of exploitable vulnerabilities introduced in the development or the operation of the TOE.”

Vulnerability analysis (AVA_VAN) (chapter 16.1)

“Objectives

Vulnerability analysis is an assessment to determine whether potential vulnerabilities identified, during the evaluation of the development and anticipated operation of the TOE or by other methods (e.g. by flaw hypotheses or quantitative or statistical analysis of the security behaviour of the underlying security mechanisms), could allow attackers to violate the SFRs.

Vulnerability analysis deals with the threats that an attacker will be able to discover flaws that will allow unauthorised access to data and functionality, allow the ability to interfere with or alter the TSF, or interfere with the authorised capabilities of other users.”

This page is intentionally left blank

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

This page is intentionally left blank.

Annex B of Certification Report BSI-DSZ-CC-0821-2014

Evaluation results regarding development and production environment

The IT product AKD eID Card 1.0 (Target of Evaluation, TOE) has been evaluated at an approved evaluation facility using the Common Methodology for IT Security Evaluation (CEM), Version 3.1 extended by advice of the Certification Body for components beyond EAL 5 and guidance specific for the technology of the product for conformance to the Common Criteria for IT Security Evaluation (CC), Version 3.1.

As a result of the TOE certification, dated 29 October 2014, the following results regarding the development and production environment apply. The Common Criteria assurance requirements ALC – Life cycle support (i.e. ALC_CMC.4, ALC_CMS.4, ALC_DEL.1, ALC_DVS.2, ALC_LCD.1, ALC_TAT.1)

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

a) Agencija za komercijalnu djelatnost d.o.o., Savska cesta 31, HR - 10000 Zagreb (Development and Production - card body manufacturing)

For the sites listed above, the requirements have been specifically applied in accordance with the Security Target [6]. 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]) are fulfilled by the procedures of these sites.

This page is intentionally left blank.