Federal Office
for Information Security

Certification Report

BSI-DSZ-CC-0825-2017

for

DIGITTRADE High Security HS256 S3, Version 1.0

from

DIGITTRADE 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-0825-2017 (*)

Portable Storage Media

DIGITTRADE High Security HS256 S3
Version 1.0

from	DIGITTRADE GmbH
PP Conformance:	Protection Profile for Portable Storage Media (PSMPP), Version 1.0, 31 July 2012, BSI-CC-PP-0081-2012
Functionality:	PP conformant Common Criteria Part 2 extended
Assurance:	Common Criteria Part 3 conformant EAL 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 Scheme Interpretations for conformance to the Common Criteria for IT Security Evaluation (CC), Version 3.1. CC and CEM are also published as ISO/IEC 15408 and ISO/IEC 18045.

(*) 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 and Notification. For details on the validity see Certification Report part A chapter 4

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

Bonn, 6 October 2017

For the Federal Office for Information Security

Bernd Kowalski
Head of Division

L.S.

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

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.....9
4. Validity of the Certification Result.....9
5. Publication.....10

B. Certification Results.....11

1. Executive Summary.....12
2. Identification of the TOE.....14
3. Security Policy.....16
4. Assumptions and Clarification of Scope.....16
5. Architectural Information.....16
6. Documentation.....17
7. IT Product Testing.....17
8. Evaluated Configuration.....18
9. Results of the Evaluation.....19
10. Obligations and Notes for the Usage of the TOE.....20
11. Security Target.....20
12. Definitions.....21
13. Bibliography.....23

C. Excerpts from the Criteria.....25

CC Part 1:.....25
CC Part 3:.....26

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 and Approval 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: Scheme documentation describing the certification process (CC-Produkte) [3]
- BSI certification: Scheme documentation on requirements for the Evaluation Facility, its approval and licencing process (CC-Stellen) [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 SOGIS Technical Domains only.

[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 Security Certificates and approval by the Federal Office for Information Security (BSI-Zertifizierungs- und -Anerkennungsverordnung - BSIZertV) of 17 December 2014, Bundesgesetzblatt 2014, part I, no. 61, p. 2231

[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

The basic recognition level includes Common Criteria (CC) Evaluation Assurance Levels EAL 1 to EAL 4 and ITSEC Evaluation Assurance Levels E1 to E3 (basic). For "Smartcards and similar devices" a SOGIS Technical Domain is in place. For "HW Devices with Security Boxes" a SOGIS Technical Domains is in place, too. In addition, certificates issued for Protection Profiles based on Common Criteria are part of the recognition agreement.

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. The current list of signatory nations and approved certification schemes, details on recognition, and the history of the agreement can be seen on the website at https://www.sogisportal.eu.

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)

The international arrangement on the mutual recognition of certificates based on the CC (Common Criteria Recognition Arrangement, CCRA-2014) has been ratified on 08 September 2014. It covers CC certificates based on collaborative Protection Profiles (cPP) (exact use), CC certificates based on assurance components up to and including EAL 2 or the assurance family Flaw Remediation (ALC_FLR) and CC certificates for Protection Profiles and for collaborative Protection Profiles (cPP).

The CCRA-2014 replaces the old CCRA signed in May 2000 (CCRA-2000). Certificates based on CCRA-2000, issued before 08 September 2014 are still under recognition according to the rules of CCRA-2000. For on 08 September 2014 ongoing certification procedures and for Assurance Continuity (maintenance and re-certification) of old certificates a transition period on the recognition of certificates according to the rules of CCRA-2000 (i.e. assurance components up to and including EAL 4 or the assurance family Flaw Remediation (ALC_FLR)) is defined until 08 September 2017.

As of September 2014 the signatories of the new CCRA-2014 are government representatives from the following nations: Australia, Austria, Canada, Czech Republic, Denmark, Finland, France, Germany, Greece, Hungary, India, Israel, Italy, Japan, Malaysia, The Netherlands, New Zealand, Norway, Pakistan, Republic of Korea, Singapore, Spain, Sweden, Turkey, United Kingdom, and the United States.

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.

This certificate is recognized under CCRA-2014 for all assurance components selected.

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 DIGITTRADE High Security HS256 S3, Version 1.0 has undergone the certification procedure at BSI.

The evaluation of the product DIGITTRADE High Security HS256 S3, Version 1.0 was conducted by DFKI. The evaluation was completed on 22 September 2017. DFKI is an evaluation facility (ITSEF)[6] recognised by the certification body of BSI.

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

The product was developed by: DIGITTRADE GmbH.

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 or in the CC itself.

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 order to avoid an indefinite usage of the certificate when evolved attack methods require a re-assessment of the products resistance to state of the art attack methods, the maximum validity of the certificate has been limited. The certificate issued on 6 October 2017 is valid until 5 October 2022. Validity can be re-newed by re-certification.

The owner of the certificate is obliged:

1. when advertising the certificate or the fact of the product's certification, to refer to the Certification Report as well as to provide the Certification Report, the Security Target and user guidance documentation mentioned herein to any customer of the product for the application and usage of the certified product,

[6] Information Technology Security Evaluation Facility

2. to inform the Certification Body at BSI immediately about vulnerabilities of the product that have been identified by the developer or any third party after issuance of the certificate,
3. to inform the Certification Body at BSI immediately in the case that security relevant changes in the evaluated life cycle, e.g. related to development and production sites or processes, occur, or the confidentiality of documentation and information related to the Target of Evaluation (TOE) or resulting from the evaluation and certification procedure where the certification of the product has assumed this confidentiality being maintained, is not given any longer. In particular, prior to the dissemination of confidential documentation and information related to the TOE or resulting from the evaluation and certification procedure that do not belong to the deliverables according to the Certification Report part B, or for those where no dissemination rules have been agreed on, to third parties, the Certification Body at BSI has to be informed.

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 DIGITTRADE High Security HS256 S3, Version 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] DIGITTRADE GmbH
Ernst-Thälmann-Str. 39
06179 Holleben

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 DIGITTRADE High Security HS256 S3 (external encrypted HDD/SSD), Version 1.0. The TOE is a portable, self-contained storage device with a physical host connection providing encrypted storage of user data and strong authentication to unlock access to the encrypted user data.

The Security Target [6] is the basis for this certification. It is based on the certified Protection Profile for Portable Storage Media (PSMPP), Version 1.0, 31 July 2012, BSI-CC-PP-0081-2012 [8].

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 2.

The TOE Security Functional Requirements (SFR) relevant for the TOE are outlined in the Security Target [6], chapter 6.1. They are selected from Common Criteria Part 2 and one of them is newly defined. Thus the TOE is CC Part 2 extended.

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

TOE Security Functions	Addressed issue
SF1 „Access control“	Access to the encrypted storage area via the USB 2.0/3.0 connection to the host PC is granted after successfully verifying the smart card PIN (knowledge factor) and transferring the encryption key (possession factor) from the smart card to the storage device. It is ensured that the smart card PIN consists of 8 decimal digits and no compromising feedback is given during any authentication attempt. Therefore the probability for a random authentication attempt to be successful is 1 out of 10^8. If the smart card PIN had been entered 8 times incorrectly, the smart card PIN and the encryption key on the smart card will be destroyed and the smart card will be terminated. The smart card PIN and the encryption key are securely stored on the individual smart card.
SF2 „Change PIN“	Changing the smart card PIN is supported after successful (re-)authentication by verifying the current smart card PIN. It is ensured that both the old and new smart card PIN consist of 8 decimal digits and no compromising feedback is given during any authentication attempt. After successfully changing the smart card PIN (knowledge factor), access to the encrypted storage area via the USB 2.0/3.0 connection to the host PC is immediately granted by transferring the encryption key (possession factor) from the smart card to the storage device.
SF3 „Key generation and key destruction"	Changing the encryption key on the smart card is supported after successful (re-)authentication by verifying the current smart card PIN. If the smart card PIN had been entered 8 times incorrectly, the smart card PIN and the encryption key on the smart card will be destroyed and the smart card will be terminated. Changing the encryption key is realised by either generating a new key using the secure random number generator of the smart card, or copying the encryption key from another smart card (requiring successful PIN verification on both the source and target smart card). The smart card generates two AES-256 keys (FIPS-197 [12]) using the built-in

TOE Security Functions	Addressed issue
	random number generator. The smart card PIN and the encryption key are securely stored on the individual smart card. The preceding encryption key (if any) is destroyed by overwriting it with the changed encryption key. When removing the smart card in activated lock-out mode, the storage device is logically disconnected from the host PC. When removing the USB cable (also in case of power failure or other disruptions), the storage device is physically disconnected from the host PC. Upon logical or physical disconnection from the host PC, the encryption key will be deleted on the storage device. In order to regain access to the encrypted storage area, a successful re-authentication is necessary (see SF1 or SF2).
SF4 „Encryption and decryption“	The storage device uses the encryption key received from the smart card (see SF1 and SF2) for encryption and decryption of the protected storage area. It implements the cryptographic operation XTS-AES-256, i.e. AES in XTS mode with two 256 Bit AES keys (FIPS-197 [12], SP 800-38E [13], IEEE 1619-2007 [14]). The Logical Block Address (LBA) of the HDD / SSD is used as the data unit number for the XTS tweak generation.
SF5 „Secure state“	The TSF preserves a secure state and provides re-authentication (see SF1 or SF2) when the following types of failures occur: ● abnormal abort of the TSF, ● system crash in the host, ● power failure, ● unintentional physical disconnection, or ● other disruption to the connection.

Table 1: TOE Security Functions

For more details please refer to the Security Target [6], chapter 7.1.

The assets to be protected by the TOE are defined in the Security Targ et [6], chapter 3.1. Based on these assets the TOE Security Problem is defined in terms of Assumptions, and Threats. This is outlined in the Security Target [6], chapters 3.3 and 3.5.

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

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:

DIGITTRADE High Security HS256 S3, Version 1.0

The following table outlines the TOE deliverables:

No	Type	Identifier	Release	Form of Delivery
1	HW/FW	DIGITTRADE High Security HS256 S3 (external encrypted HDD/SSD) Portable storage device with internal 2.5" SATA HDD or SSD drive (with 512 byte external sector size) from Samsung (preferred), Seagate, Western Digital, Toshiba or Hitachi. The following capacities are available: 120GB SSD, 160GB HDD, 250GB SSD, 320GB HDD, 500GB HDD/SSD, 640GB HDD, 750GB HDD/SSD, 1TB HDD/SSD, 1,5TB HDD/SSD, 2TB HDD/SSD, 4TB HDD/SSD.	TOE device Version 1.0	Delivered inside the security bag and packaging box
2	HW/SW	Two smart cards NXP J2E081_M64 R3 with JCOP v2.4.2 R3 (Java Card) certified by NSCIB-CC-13-37761-CR2 [15] loaded with DIGITTRADE HS256 S3 Java Card Applet	TOE smart card Version 1.0 Version 1.1.0	Delivered inside the security bag and packaging box
3	DOC	DIGITTRADE High Security HS256 S3 Benutzerhandbuch / User Manual [10] Note: Printed version is inside the packaging box, but not part of the evaluated configuration.	Version 1.8 for TOE Version 1.0	Download
3	DOC	Benutzerhandbuch / User Manual - Wichtiger Hinweis / Important notice [11]	Version 1.8 for TOE Version 1.0	Delivered inside the security bag and packaging box
4	Accessory	USB cable	non-TOE	Delivered inside the packaging box
6	Accessory	Hard case	non-TOE	Delivered inside the packaging box

Table 2: Deliverables of the TOE

Additional smart cards:

No	Type	Identifier	Release	Form of Delivery
1	HW/SW	Some smart cards (variable amount) NXP J2E081_M64 R3 with JCOP v2.4.2 R3 (Java Card) certified by NSCIB-CC-13-37761-CR2 [15] loaded with DIGITTRADE HS256 S3 Java Card Applet	TOE smart card Version 1.0 Version 1.1.0	Delivered inside the security bag and packaging box

Table 3: Deliverables of the TOE

The physical delivery items of the complete product resp. additional smart cards, as listed in the above tables, are shipped using standard packaging boxes.

Only the electronic edition of the "Benutzerhandbuch / User Manual” is part of the evaluated configuration of the TOE. It can be downloaded from: http://www.digittrade.de/cms/support-center/download-center/?did=83

The SHA-512 hash of the electronic edition of the “Benutzerhandbuch / User Manual” is:
5AFF4CA83276CDB572842EC131DE0FB7A0F7A2BDB192E858A800238C1075C2D3
233A90CFB537AFCBCDBB2F36D9EB21F8E3707781E06696E2711CD9EE25F8A3E0

There are three different delivery procedures:

- physical delivery of the complete TOE
- physical delivery of additional smart cards
- electronic delivery of the user guidance (download)

The procedure for physical delivery of the complete TOE (storage device and smart cards) and accessories are separated in two stages.

In the first stage of physical delivery, the complete TOE (storage device and smart cards) resp. additional smart cards are packed into a security bag that is labelled with name/version of the TOE. The second stage of physical delivery requires that the security bag remains in place, undamaged and closed until the TOE is received by the end user. The security bag ensures detection of any tampering or masquerading attempts during physical delivery. Moreover, the security bag contains a download notice indicating the SHA-256 hash value of the electronic edition of the user guidance, ensuring detection of any tampering or masquerading during electronic delivery (download) of the user guidance.

Overall, the developer uses two mechanism, i.e. a tamper-evident/-proof packaging (security bag) and a strong cryptographic checksum, to ensure that the TOE is protected against tampering and masquerading attacks during physical and electronic delivery.

In case of physical delivery of the complete TOE resp. additional smart cards, the user shall verify the correct packaging of the TOE (see electronic user manual), i.e. check whether the security bag is in place and closed and its security indicators are neither damaged nor removed.

After electronic delivery of the user manual the user shall verify its SHA-512 hash value after download (see [11]).

The print edition of the user guidance is not sufficiently protected since it is not packed into the security bag. Therefore, only the digital version of the user manual is part of the evaluation.

Although the user manual also describes the presence of a hologram sticker and epoxy glue, these sealings are indicated as not being evaluated. They do not make any contribution to the secure delivery and acceptance procedures.

The TOE parts can be identified via the labels of the

- portable storage device, printed on a sticker at the back side of its housing;
- smart card (JCOP v2.4.2 R3 from NXP), printed on its back side;
- user guidance [10], printed at the bottom of the inside front cover of its German (p. 2) resp. English (p. 53) section.

3. Security Policy

The Security Policy is expressed by the set of Security Functional Requirements and implemented by the TOE. It covers the following issues:

- Protection of TSF data, i.e. authentication data and the cryptographic key material (smart card PIN and encryption key)
- Provision of a two-factor authentication mechanism
  - Possession factor: encryption key
  - Knowledge factor: smart card PIN
- Encryption of all data stored in the protected storage area of the TOE
- Allowing only authenticated users to change the authentication data
- Reverting to a secure, stable and consistent state following a disruption

4. Assumptions and Clarification of Scope

The Assumptions defined in the Security Target and some aspects of Threats and Organisational Security Policies are not covered by the TOE itself. These aspects lead to specific security objectives to be fulfilled by the TOE-Environment. The following topics are of relevance:

- OE.TrustedWS: The responsibility of the user is to ensure that all data retrieved from the protected storage area of the TOE is properly protected resp. and no malware is transferred to the TOE. This is explicitly reflected and supplemented by additional instructions to monitor the activation of the lock-out mode and locking the TOE when it is unattended.
- OE.AuthConf: The responsibility of the user for protecting confidentiality of the authentication data is explicitly reflected and supplemented by additional instructions for the destruction of encryption key, periodical resp. event-driven change of the smart card PIN and individual and secure choice of the smart card PIN.

Details can be found in the Security Target [6], chapter 4.2.

5. Architectural Information

The TOE consists of three subsystems:

- Storage device
- Java card applet
- Smart card

The storage device provides the host connection and contains the encrypted storage. It is composed of the controller, USB-to-SATA bridge, protected storage and authentication interfaces (smart card, keypad) as parts of the subsystem. It implements the data and control relationships within the functionality for access control, user authentication, encryption and administration of the encryption key.

While the Java card applet provides the storage, handling and management of the match ID (for pairing with the storage device), the encryption key and the smart card PIN, it uses basic functionality of the smart card platform including secure cryptographic primitives (random number generator), secure storage of sensitive data (smart card PIN, encryption key) and relies on the management of an authenticated state.

The interfaces of the storage device and the Java card applet correspond to the TSF interfaces. The interaction between the Java card applet and the smart card platform is not visible to the user.

The architecture of the TOE ensures that the data encryption key is strictly separated from the encrypted data, unless the storage device is in its authenticated state. The separation provides the possession factor (encryption key) in addition to the knowledge factor (smart card PIN) for 2-factor authentication. With the help of the storage device and the Java card applet, the encryption key and the smart card PIN can be changed.

Further, with the help of the storage device and the Java card applet, the encryption key can be copied to several smart cards. Each of these smart cards can be used in the authentication process. Destruction of the encryption key requires either deletion on all smart cards that store a copy of the encryption key, or generation of a new encryption key and wiping the storage media using the new encryption key.

Physical disconnection of the storage device from the host PC locks the encrypted user data by making the encryption key unavailable. Removing the smart card from the storage device leads to a logical disconnection of the storage device from the host PC, which also locks the encrypted user data by making the encryption key unavailable[8].

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

In addition to the evaluated configuration, several test configurations of the TOE are used for the functional and penetration testing as described below.

The developer designed seven classes of tests:

- Functional external interface tests use the evaluated configuration and some specifically prepared smart cards for testing the functionalities:
  - Automatic power on tests
  - Access control only after successful user authentication
  - Management functions
- Encryption specific tests examine the storage media for testing whether the proper cryptographic algorithm (XTS-AES-256) is used.

[8] This so called lock-out mode can be deactivated by the user, but must remain activated in order to use the TOE in the evaluated configuration.

- Java Card applet tests use a standard smart card reader for testing all relevant APDU opcodes of the applet interface
- Smart card integrity tests use a standard smart card reader for testing the protection against manipulating the smart card applet by using the smart card platform functionality to install and configure applications.
- USB-to-SATA Bridge integrity tests use equipment on the host PC for testing the protection of the TOE against manipulating the firmware on the USB bridge by attempting to use the update mechanism.
- RAM tracking tests use an appropriate debugging tool for tracking the deletion of sensitive information in the internal RAM.
- Data transmission integrity tests use an appropriate debugging tool and an adapted test configuration for testing the detection and handling of integrity errors during internal transmission of the data encryption key.

In addition to repeating an appropriate sample of the developer tests, the evaluator has conducted independent tests which complement

- The tests of the behaviour of the security functionality,
- The tests of the interface actions in additional ways and combinations,
- The standard IEEE Std 1619-2007 test vectors, and
- The choice of encrypted sectors on storage media.

Moreover, the evaluator has conducted penetration tests for three identified potential vulnerabilities:

- Sensitive information stored on storage media;
- Access to the internal memory of the device;
- Improper handling of unused APDU opcodes.

The test results do not indicate any unexpected behaviour. The potential vulnerabilities being tested actually do not exist.

8. Evaluated Configuration

This certification covers the following configurations of the TOE: The TOE shall be operated in a single configuration. It consists of all delivered parts that comprise the TOE as described in the scope of delivery. Further, the TOE shall be operated with activated lock-out mode.

The single configuration of hardware, firmware, software and user guidance is:

- The TOE device as composed of its hardware/firmware components
- Contact-based smart card NXP J2E081_M64 R3 with JCOP v2.4.2 R3 (Java Card), certified by NSCIB-CC-13-37761-CR2 (NXP)
- DIGITTRADE HS256 S3 V1.0 Java Card Applet V1.1.0 (DIGITTRADE)
- The TOE user guidance: DIGITTRADE HS256 S3 V1.0 Benutzerhandbuch / User Manual

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.

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

- All components of the EAL 2 package including the class ASE as defined in the CC (see also part C of this report).

The evaluation has confirmed:

- PP Conformance: Protection Profile for Portable Storage Media (PSMPP), Version 1.0, 31 July 2012, BSI-CC-PP-0081-2012 [8]
- for the Functionality: PP conformant
  Common Criteria Part 2 extended
- for the Assurance: Common Criteria Part 3 conformant
  EAL 2

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).

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

No.	Purpose	Cryptographic Mechanism	Standard of Implementation	Key Size in Bits	Security Level above 100 Bits	Comments
1	Key Generation (FCS_CKM.1)	AES (DRG.3)	FIPS PUB 197 [12]	512 Bit	Yes	-
2	En-/decryption of stored data (FCS_COP.1)	XTS-AES-256	NIST SP 800-38E [13] IEEE Std 1619-2007 [14]	2 × 256 Bit	Yes	-

Table 4: TOE cryptographic functionality

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 following aspects need to be fulfilled when using the TOE:

- The originality and integrity of the printed edition of the user manual is not sufficiently protected during physical delivery of the TOE. Therefore, the authorized user shall only use the electronic edition of the user manual. It is provided for download as indicated by the accompanying important notice. Before first usage of the user manual the authorized user shall verify the checksum (see chapter 2).
- The TOE shall be operated in activated lock-out mode. In order to ensure that the lock-out mode is activated, the authorized user shall monitor the corresponding status LED.
- The authorized user is responsible for the individual preparation of the TOE. Before first usage of the TOE he shall (a) change the initial smart card PIN, (b) generate the initial encryption key on the smart card, and (c) initialize the smart card on the storage device. Otherwise, the TOE shall not be used since it may not be in a secure state.
- In order to terminate the life-cycle of the encryption key and ensure that the encrypted user data definitely cannot be decrypted anymore, even when the encryption key has been copied onto several smart cards, the authorized user shall either destroy each copy of the encryption key or overwrite the entire storage area using a newly generated encryption key.
  The cryptographic keys can be deleted by either deleting the cryptographic keys by creating a new one or by entering the 8-digit PIN incorrectly 8 times.

Obligations and advices for the developer

- The security bag is apparently intended for use with different products. In order to avoid delivery of a false version of the TOE due to mistakes in the supply chain, the developer shall label the security bag with the complete TOE reference (name and version).
- When integrating further functions into the smart card, the developer shall inform its customers that any such configuration is not covered by the certificate for the TOE.

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.

12. Definitions

12.1. Acronyms

AES-XTS	Advanced Encryption Standard in XEX-based tweaked-codebook mode with ciphertext stealing
AIS	Application Notes and Interpretations of the Scheme
APDU	Application Protocol Data Unit
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
cPP	Collaborative Protection Profile
EAL	Evaluation Assurance Level
ETR	Evaluation Technical Report
FIPS	Federal Information Processing Standard
HDD	Hard Disk Drive
IEEE	Institute of Electrical and Electronics Engineers
IT	Information Technology
ITSEF	Information Technology Security Evaluation Facility
LBA	Logical Block Address
LED	Light Emitting Diode
NIST	National Institute of Standards and Technology
PP	Protection Profile
RAM	Random Access Memory
SAR	Security Assurance Requirement
SATA	Serial Advanced Technology Attachment
SFP	Security Function Policy
SFR	Security Functional Requirement
SHA	Secure Hash Algorithm
SSD	Solid State Disk
ST	Security Target
TOE	Target of Evaluation

TSF	TOE Security Functionality
USB	Universal Serial Bus

12.2. Glossary

Augmentation - The addition of one or more requirement(s) to a package.

Collaborative Protection Profile - A Protection Profile collaboratively developed by an International Technical Community endorsed by the Management Committee.

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

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.

Package - named set of either security functional or security assurance requirements

Protection Profile - A formal document defined in CC, expressing an implementation independent set of security requirements for a category of IT Products that meet specific consumer needs.

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 - An IT Product and its associated administrator and user guidance documentation that is the subject of an Evaluation.

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
http://www.commoncriteriaportal.org

[2] Common Methodology for Information Technology Security Evaluation (CEM), Evaluation Methodology, Version 3.1, Rev. 4, September 2012, http://www.commoncriteriaportal.org

[3] BSI certification: Scheme documentation describing the certification process (CC-Produkte) and Scheme documentation on requirements for the Evaluation Facility, approval and licencing (CC-Stellen), https://www.bsi.bund.de/zertifizierung

[4] Application Notes and Interpretations of the Scheme (AIS) as relevant for the TOE[9] https://www.bsi.bund.de/AIS

[5] German IT Security Certificates (BSI 7148), periodically updated list published also on the BSI Website, https://www.bsi.bund.de/zertifizierungsreporte

[6] Security Target, Version 1.10, 2017-09-18, DIGITTRADE High Security HS256 S3, (external encrypted HDD/SSD), Version 1.0, DIGITTRADE GmbH

[7] Evaluation Technical Report, Version 1.1, 2017-09-19, Evaluation DIGITTRADE HS256 S3 V1.0, DFKI GmbH, (confidential document)

[8] Protection Profile for Portable Storage Media (PSMPP), Version 1.0, 31 July 2012, BSI-CC-PP-0081-2012

[9] Configuration list for the TOE, Version 1.4, 2017-04-03, CM scope (ALC_CMS.2), (confidential document)

[10] Guidance documentation for the TOE, Version 1.07, 2017-04-03, Benutzerhandbuch / User Manual

[11] Guidance documentation for the TOE, Version 1.07, 2017-04-03, Benutzerhandbuch / User Manual - Wichtiger Hinweis / Important Notice

[12] [U.S.] National Institute of Standards and Technology (NIST): Federal Information Processing Standards (FIPS) Publication 197 – Announcing the Advanced Encryption Standard (AES), November 26, 2001.

[13] [U.S.] National Institute of Standards and Technology (NIST): Special Publication (SP) 800-38E – Recommendation for Block Cipher Modes of Operation – The XTS-AES Mode for Confidentiality on Storage Devices, January 2010.

[14] Institute of Electrical and Electronics Engineers (IEEE), Inc.: IEEE Std 1619-2007 – The XTS-AES Tweakable Block Cipher, 04/18/2008.

[15] TÜV Rheinland Nederland B.V.: NXP J3E081_M64, J3E081_M66, J2E081_M64, J3E041_M66, J3E016_M66, J3E016_M64, J3E041_M64 Secure Smart Card Controller Revision 3 [also named JCOP 2.4.2 R3] – Certification Report, NSCIB-CC-13-37761-CR2, Version 1, 25/08/2014.

[9] specifically

- AIS 32, Version 7, CC-Interpretationen im deutschen Zertifizierungsschema

This page is intentionally left blank.

C. Excerpts from the Criteria

CC Part 1:

Conformance Claim (chapter 10.4)

“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
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

Assurance Class	Assurance Components
	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.

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

“Objectives

EAL 1 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.

EAL 1 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.

EAL 1 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 EAL 1 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 (EAL 2) - structurally tested (chapter 8.4)

“Objectives

EAL 2 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.

EAL 2 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 (EAL 3) - methodically tested and checked (chapter 8.5)

“Objectives

EAL 3 permits a conscientious developer to gain maximum assurance from positive security engineering at the design stage without substantial alteration of existing sound development practises.

EAL 3 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 (EAL 4) - methodically designed, tested, and reviewed (chapter 8.6)

"Objectives

EAL 4 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. EAL 4 is the highest level at which it is likely to be economically feasible to retrofit to an existing product line.

EAL 4 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 (EAL 5) - semiformally designed and tested (chapter 8.7)

"Objectives

EAL 5 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 EAL 5 assurance. It is likely that the additional costs attributable to the EAL 5 requirements, relative to rigorous development without the application of specialised techniques, will not be large.

EAL 5 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 (EAL 6) - semiformally verified design and tested (chapter 8.8)

"Objectives

EAL 6 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.

EAL 6 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 (EAL 7) - formally verified design and tested (chapter 8.9)

"Objectives

EAL 7 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 EAL 7 is currently limited to TOEs with tightly focused security functionality that is amenable to extensive formal analysis."

Assurance Class	**Assurance Family**	**Assurance Components by Evaluation Assurance Level**						
		EAL 1	EAL 2	EAL 3	EAL 4	EAL 5	EAL 6	EAL 7
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
	ASE_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”

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.”

D. Annexes

List of annexes of this certification report

Annex A: Security Target provided within a separate document.

This page is intentionally left blank.