Federal Office
for Information Security

Certification Report

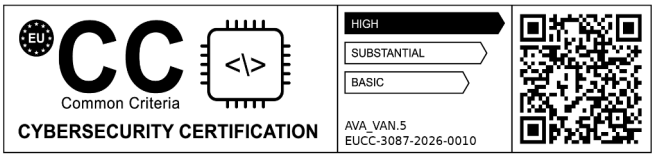
EUCC-3087-2026-0010
Administration ID
BSI-DSZ-CC-1162-V4-2026

for

CardOS V6.0 ID R1.2

from

Eviden Germany 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 9582-11

Contents

A. Certification

1. Preliminary Remarks

The Implementing Regulation (EU) 2024/482 of the European Parliament and of the Council of 31 January 2024 [EUCC-VO] establishes a Union-wide cybersecurity certification scheme for TOEs and Protection Profiles for conformity assessments using the requirements of Common Criteria.

By implementing the Cybersecurity Act[1], certification activities at assurance level ‘high’ and in duly justified cases at assurance level ‘substantial’ are reserved to the National Cybersecurity Certification Agency of a Member State.

In accordance to BSIG[2] Act, the Federal Office for Information Security (BSI) issues certificates for information technology products.

Certification of a product is carried out at the request of a developer, vendor or a distributor, hereinafter called the applicant.

A part of the procedure is the technical examination (evaluation) of the product according to the security criteria referenced in the above mentioned Implementing Regulation (EU) 2024/482 as well as relevant application notes and interpretations published by the certification body of the BSI.

Evaluation facilities notified by the German National Cybersecurity Certification Authority carry out the evaluation.

This Certification Report is the result of the certification activities carried out by the certification body of the BSI in conclusion of the technical evaluation. 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.

2. Specifications of the Certification Procedure

The certification body carries out its activities according to the criteria laid down in the following:

- Implementing Regulation (EU) 2024/482 of the European Parliament and of the Council of 31 January 2024 laying down rules for the application of Regulation (EU) 2019/881 of the European Parliament and of the Council as regards the adoption of the European Common Criteria-based cybersecurity certification scheme (EUCC) [EUCC-VO]
- EUCC state-of-the-art documents of relevance to the TOE [EUCC_SOTA]
- Act on the Federal Office for Information Security[2]

[1] Regulation (EU) 2019/881 of the European Parliament and of the Council of 17 April 2019 on ENISA (the European Union Agency for Cybersecurity) and on information and communications technology cybersecurity certification and repealing Regulation (EU) No 526/2013 (Cybersecurity Act)

[2] Act on the Federal Office for Information Security (BSI-Gesetz - BSIG) of 2 December 2025, BGBl. 2025 Nr. 301, S. 2

- BSI Certification and Approval Ordinance[3]
- BMI Regulations on Ex-parte Costs[4]
- Special decrees issued by the Bundesministerium des Innern (Federal Ministry of the Interior and Community)
- ISO/IEC 15408 (Common Criteria for IT Security Evaluation (CC), Version 3.1 R5) [CC]
- ISO/IEC 18045 (Common Methodology for IT Security Evaluation (CEM), Version 3.1 R5) [CEM]
- DIN EN ISO/IEC 17065 standard
- EUCC programme: Scheme documentation describing the certification process (EUCC) [EUCC_PROG]
- BSI certification: Application Notes and Interpretation of the Scheme (AIS) [AIS]

3. Recognition Agreements

In order to avoid multiple certifications 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.

3.1. 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 current list of signatory nations and approved certification schemes can be seen on the website: https://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 related bodies of the signatory nations. A disclaimer beneath the logo indicates the specific scope of recognition.

This certificate is recognized according to the rules of CCRA-2014, i. e. up to and including CC part 5 EAL 2 and ALC_FLR components.

4. Performance of Evaluation and Certification

- The certification body monitors each individual evaluation to ensure a uniform application and interpretation of the criteria as well as uniform ratings.

[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 02 December 2025, Bundesgesetzblatt 2025, no. 301

[4] BMI Regulations on Ex-parte Costs - Besondere Gebührenverordnung des BMI für individuell zurechenbare öffentliche Leistungen in dessen Zuständigkeitsbereich (BMIBGebV), Abschnitt 7 (BSI-Gesetz) - dated 2 September 2019, Bundesgesetzblatt I p. 1365

- The TOE CardOS V6.0 ID R1.2 has been certified by the certification body of the Federal Office for Information Security (BSI) based on administration ID BSI-DSZ-CC-1162-V3-2024. Specific results from the evaluation process were re-used.
- The evaluation of the product CardOS V6.0 ID R1.2 was carried out by TÜV Informationstechnik GmbH, located at Am TÜV 1, 45307 Essen, Germany.
- The evaluation was completed on 1 June 2026. TÜV Informationstechnik GmbH is a notified evaluation facility (ITSEF).
- This certification was applied for: Eviden Germany GmbH.
- The assessed TOE was developed by: Eviden Germany GmbH.
- The certification activities are concluded with the comparability check and the production of this Certification Report. This work was completed by the certification body of the BSI.

This Certification Report applies only to the version of the TOE as identified in this document. The confirmed assurance package is valid on the condition that

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

For the meaning of the assurance components and assurance levels please refer to CC [CC] itself.

The issued Certificate confirms the assurance of the product claimed in the Security Target [ST] on certificate’s issuance day. 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 holder of the Certificate should involve the assurance continuity program of the EUCC Certification Scheme (e.g. by a re-assessment or re-certification) in its obligations to monitor the certified product. Specifically, if certification results should be 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 prevent an indefinite certificate usage where evolving attack methods justify a recent re-assessment of the product’s resistance, the maximum validity period of the certificate is limited. The certificate issued on 23 June 2026 is valid until 22 June 2031 and its validity can be renewed by certifying the TOE again.

The holder of this certificate is obliged:

- to meet the obligations from the Implementing Regulation (EU) 2024/482, in particular but not exclusively to respect the rules for certificate usage, to monitor the conformity of the certified TOE, to inform the certification body about subsequently detected vulnerabilities or irregularities with relevance to the security of the TOE and to maintain vulnerability management and disclosure procedures.

Should changes be introduced into the certified version of the TOE, the validity period of its related certificate can be extended in order to cover the changed TOE, provided the holder of the certificate applies for measures under EUCC scheme’s assurance continuity (i.e. re-certification or maintenance) and the changed TOE then meets the assurance requirements.

5. Publication

The TOE CardOS V6.0 ID R1.2 has been notified to ENISA for publication on the website on European cybersecurity certification schemes and has also been included in BSI's list of certified products, which is published regularly (see [EUCC_CERT]). Further information can be obtained from BSI-Infoline +49 228 9582-111.

This holder of the certificate[5] has to publish on its website this Certification Report and supplementary information. The Certification Report may also be obtained in electronic form at the internet address stated above.

[5] Eviden Germany GmbH
Otto-Hahn-Ring 6
81739 München
Germany

B. Certification Results

The following chapters summarise the assessment results of

- the applicant’s Security Target specified for the Target of Evaluation,
- the relevant evaluation results from the evaluation facility, and
- complementary notes, statements and indications from the certification body.

1. Executive Summary

The Target of Evaluation (TOE) is named CardOS V6.0 ID R1.2 and developed by Eviden Germany GmbH. The TOE is a smart card operating system on an IC with at least one application. Applications covered by this TOE comprise an electronic passport (ePass) application and/or a signature (eSign) application.

The IC platform comprises the integrated circuit SLC52GDA448* (IFX_CCI_000005 Design Step H13) and the cryptographic libraries RSA v2.08.007, EC v2.08.007, Toolbox v2.08.007, Base v2.08.007, HCL (Hash Cryptographic Library) v1.12.001, SCL (Symmetric Cryptographic Library) v2.04.002 and HSL (Hardware Support Library) v03.12.8812 from Infineon Technologies AG certified under ID BSI-DSZ-CC-1110-V8-2025 as relevant for the present TOE.

Three major configurations of the TOE are defined which differ in the description of the file system:

- ePassport: User data are stored in an ICAO-compliant ePass Application protected by PACE and EAC1. Here, EAC1 is used only for data groups 3 and 4.
- SSCD: User data are stored in an eSign Application conformant to “Protection profiles for secure signature creation device – Part 2: Device with key generation” ([PP]).
- eID: User data are contained in an ICAO-compliant ePass Application, in an eSign Application conformant to “Protection profiles for secure signature creation device – Part 2: Device with key generation“ ([PP]), and optional eID applications.

The product CardOS V6.0 ID R1.2 has been certified under the EUCC scheme in accordance to the provisions of the Implementing Regulation (EU) 2024/482. This is a certification based on BSI administration ID BSI-DSZ-CC-1162-V3-2024. Specific results from the evaluation process BSI-DSZ-CC-1162-V3-2024 were re-used. The TOE deliverables are listed in table 1.

The evaluation of the product CardOS V6.0 ID R1.2 was conducted by TÜV Informationstechnik GmbH. The evaluation was completed on 1 June 2026. TÜV Informationstechnik GmbH is a notified evaluation facility (ITSEF).

The Evaluation Technical Report (ETR) [ETR] was provided by the ITSEF according to the Common Criteria [CC], the Methodology [CEM], the requirements of the Scheme [EUCC-VO] and [EUCC_PROG].

The evaluation has confirmed:

- CC Version and Release: see [CC] and [CEM]
- PP Conformance: Protection profiles for secure signature creation device – Part 2: Device with key generation, CEN/ISSS, EN 419211-2:2013, 2016-06-30, BSI-CC-PP-0059-2009-MA-02 [PP]

  Protection profiles for secure signature creation device – Part 4: Extension for device with key generation and trusted communication with certificate generation application, CEN/ISSS, EN 419211-4:2013, 2016-06-30, BSI-CC-PP-0071-2012-MA-01 [PP]

	Protection profiles for secure signature creation device – Part 5: Extension for device with key generation and trusted communication with signature creation application, CEN/ISSS, EN 419211-5:2013, 2016-06-30, BSI-CC-PP-0072-2012-MA-01 [PP] Machine Readable Travel Document with "ICAO Application" Extended Access Control with PACE, Version 1.3.2, 5 December 2012, BSI-CC-PP-0056-V2-2012-MA-02 [PP] Common Criteria Protection Profile Machine Readable Travel Document using Standard Inspection Procedure with PACE (PACE_PP), Version 1.01, 22 July 2014, BSI-CC-PP-0068-V2-2011-MA-01 [PP]
• Assurance Level:	EUCC High with component AVA_VAN.5
• Assurance Package:	EAL 4
• Augmentation:	ALC_DVS.2, ATE_DPT.2 and AVA_VAN.5

The Security Target [ST] is the basis for this certification. It is based on the certified Protection Profiles [PP].

A detailed description of the security functionality, addressed threats, organisational security policies and the operational environment can be found in the Security Target [ST].

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

The vulnerability assessment results stated in this certificate do not express an appraisal of the strength and suitability of the cryptographic algorithms implemented in the TOE (see BSIG Section 52, Para. 4, Clause 2).

The certification results apply only to the version of the product indicated in the certificate and on the condition that all the statements and indications are kept as detailed in this Certification Report. Neither the BSI nor any other organisation that recognises or gives effect to this certificate implicitly or explicitly guarantee or endorse the certified TOE.

2. Identification of the TOE

The Information and communications technology (ICT) product is identified as follows:

CardOS V6.0 ID R1.2

Holder of the certificate: Eviden Germany GmbH
Otto-Hahn-Ring 6
81739 München
Germany
https://www.cryptovision.com/en/product-security/

The following table outlines the TOE deliverables:

No.	Type	Identifier	Release	Form of Delivery
1	HW	Infineon / IFX SLC52GDA448*	IFX_CCI_000005 Design Step H13	Wafer, module or a packaged component.
2	SW	CardOS V6.0 ID R1.2	V6.0 / R1.2	
3	SW	RSA Cryptographic Library	v2.08.007	

No.	Type	Identifier	Release	Form of Delivery
4	(Infineon)	EC Cryptographic Library	v2.08.007	
5		Toolbox Library	v2.08.007	
6		Base Library	v2.08.007	
7		Hash Cryptographic Library (HCL)	v1.12.001	
8		Symmetric Cryptographic Library (SCL)	v2.04.002	
9		Hardware Support Library (HSL)	v03.12.8812	
10	DOC [Guides]	CardOS V6.0 User's Manual	06/2023	As PDF via signed and encrypted e-mail.
11		User Guidance 'CardOS V6.0 ID R1.2' and 'CardOS V6.0 ID R1.2 (BAC)'	1.60R	
12		Administrator Guidance 'CardOS V6.0 ID R1.2' and 'CardOS V6.0 ID R1.2 (BAC)'	1.70R	
13		Application Base Guidance 'CardOS V6.0 ID R1.2' and 'CardOS V6.0 ID R1.2 (BAC)'	1.60R	
14		Application ePassport Guidance 'CardOS V6.0 ID R1.2' and 'CardOS V6.0 ID R1.2 (BAC)'	1.60R	
15		Application eSign Guidance 'CardOS V6.0 ID R1.2' and 'CardOS V6.0 ID R1.2 (BAC)'	1.60R	
16		Packages & Release Notes, CardOS V6.0	11/2024	
17	DATA	Configuration Scripts for initialization and personalization	R1.20 CL54655	As file via signed and encrypted e-mail.
18		StartKey for initialization	-	

Table 1: Deliverables of the TOE

Components no. 1 to no. 9 are actually delivered as one item, namely the IC platform containing the software mask.

Item no. 17 represents the configuration files for initialization and personalization. These represent possible configurations and changes on values and parameters to be applied as outlined in the scripts themselves and according to the guidance documents.

The OS software pre-loaded on the IC hardware is sent directly from the chip manufacturer to the Trust Center or via logistic centers or distributors. This is possible since the TOE protects itself during delivery and standard procedures for packaging, storage and distribution can be applied. Only with knowledge of the StartKey it is possible to continue the process of setting up the TOE. The Trust Center is also provided with the guidance and initialization / personalization scripts from the developer Eviden Germany GmbH. All data and documents are sent signed and encrypted by mail.

The TOE can be identified in accordance with the described processes in the Administrator Guidance, chapter 5.1, User Guidance, chapter 4.2 and Application Base Guidance, chapter 4.1 [Guides]. After the delivery the TOE can be identified by the command response sequence as outlined in the Administrator Guidance, chapter 5.1 and Application

Base Guidance, chapter 4.1 [Guides], verifying the OS version, product name, version and year, chip identification and loaded packages (see version information in Packages & Release Notes, CardOS V6.0, chapter 2 [Guides]).

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:

- Security Audit
- Cryptographic Support
- User Data Protection
- Identification and Authentication
- Security Management
- Protection of the TSF
- Trusted Path/Channels

The TOE implements physical and logical security functionality in order to protect user data and TSF data stored and operated on the smart card when used in a hostile environment. Hence the TOE maintains integrity and confidentiality of code and data stored in its memories and the different CPU modes with the related capabilities for configuration and memory access and for integrity, the correct operation and the confidentiality of security functionality provided by the TOE. Therefore the TOE's overall policy is to protect against malfunction, leakage, physical manipulation and probing. Besides, the TOE's life cycle is supported as well as the user Identification whereas the abuse of functionality is prevented. Furthermore, specific cryptographic services including random number generation and key management functionality are being provided to be securely used by the smart card embedded software.

Specific details concerning the above mentioned security policies can be found in the Security Target [ST], chapter 7.6.

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 uncovered aspects need to be provided by specific security objectives that have to be met by the TOE environment. The following topics are of relevance:

- OE.Legislative_Compliance (Issuing of the travel document)
- OE.Passive_Auth_Sign (Authentication of travel document by Signature)
- OE.Personalisation (Personalisation of travel document)
- OE.Terminal (Terminal operating)
- OE.Travel_Document_Holder (Travel document holder Obligations)
- OE.Auth_Key_Travel_Document (Travel document Authentication Key)
- OE.AA_Key_Travel_Document (Travel document Authentication Key)
- OE.Authoriz_Sens_Data (Authorization for Use of Sensitive Biometric Reference Data)

- OE.Exam_Travel_Document (Examination of the physical part of the travel document)
- OE.Prot_Logical_Travel_Document (Protection of data from the logical travel document)
- OE.Ext_Insp_Systems (Authorization of Extended Inspection Systems)
- OE.SVD_Auth (Authenticity of the SVD)
- OE.CGA_QCert (Generation of qualified certificates)
- OE.SSCD_Prov_Service (Authentic SSCD provided by SSCD-provisioning service)
- OE.HID_VAD (Protection of the VAD)
- OE.HID_TC_VAD_Exp (Trusted channel of HID for VAD export)
- OE.DTBS_Intend (SCA sends data intended to be signed)
- OE.DTBS_Protect (SCA protects the data intended to be signed)
- OE.SCA_TC_DTBS_Exp (Trusted channel of SCA for DTBS export)
- OE.Signatory (Security obligation of the signatory)
- OE.Dev_Prov_Service (Authentic SSCD provided by SSCD Provisioning Service)
- OE.CGA_SSCD_Auth (Pre-initialization of the TOE for SSCD authentication)
- OE.CGA_TC_SVD_Imp (CGA trusted channel for SVD import)
- OE.Env_Admin (Administrator works in trusted environment)
- OE.Env_Mass_Signature (Mass signatures are generated in trusted environment only)

Details can be found in the Security Target [ST], chapter 5.2.

5. Architectural Information

The composite TOE CardOS V6.0 ID R1.2 is a smart card product consisting of the operating system, a certified Infineon hardware platform with its cryptographic libraries (refer to [CertRep IC]) and the file system that defines its applications. The TOE comprises the following subsystems as listed with a short description in the following itemization:

- Startup: Performs actions needed at startup only and not further used after entry into user commands processing loop.
- Command Manager: The main loop within the Command Manager is the most central part of CardOS.
- Protocol Manager: Takes care of command reception and transmission of response data.
- Command Layer: Implements the APDU command set, enables secure access to data and allows for package download.
- Security: Selects appropriate rules and the corresponding evaluation, manages the administration of access rights, provides secure messaging processing, evaluates an entities' life cycle when influencing access rules, protects the TOE against attacks using the underlying hardware security features.
- Entities: Provides the mediation of access to the application and its objects, provides file system administration, performs the setting of authorization flags, provides

PIN/PUK blocking functionality, handles private keys for signature generation with appropriate parameters, handles SCP functionality, provides integrity mechanisms (CRC), checks file status and provides countermeasures against fault induction attacks.

- Cryptography: Provides wrapper modules for IFX platform libraries, padding routines and generic management of cryptography.
- CBIOS: Provides interface functionality to the hardware peripherals (UART, CRC generator) and provides utility functions (memory management, transaction management, interrupt service routines).
- IC: Represents the parts of the underlying hardware platform of the composite TOE, which interacts with the operating system.
- Retrieval Functions: Retrieves the results of performed routines.

6. Supplementary Cybersecurity Information

The evaluated documentation as outlined in table 1 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 [ST].

The developer's website as stated in chapter 2 provides the following supplementary information:

- the period during which support is offered (especially security related updates)
- contact information of the manufacturer or provider and accepted methods for receiving vulnerability information from end users and security researchers
- a reference to online repositories listing publicly disclosed vulnerabilities related to the TOE/ICT, ICT service or ICT process and to any relevant cybersecurity advisories

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

All tests have been carried out by the ITSEF

TÜV Informationstechnik GmbH
Am TÜV 1
D-45307 Essen

under the responsibility of the certification body

Bundesamt für Sicherheit in der Informationstechnik
Godesberger Allee 87
Postfach 20 03 63
D-53175 Bonn

Please refer to chapter 1 of this report for details on assurance levels or packages involved into testing.

For the state-of-the-art documents and supporting documents applied please refer to chapter 9.1 of this report.

Please refer to chapter 8 for complete and precise information on settings and configuration of the TOE during the evaluation, including relevant operational notes and observations.

Developer's Tests according to ATE_FUN

Testing approach:

The evaluation activities were performed on the composite smart card product. A wide spectrum of configurations and configuration parameters, basically categorized as follows, was tested:

- Configuration variants with ECC ePassport application
- Configuration variants with RSA ePassport application
- Configuration variants with ECC eSign application
- Configuration variants with RSA eSign application
- Configuration variants with eSign and ePassport applications:
  - Both ECC-based
  - Both RSA-based
  - One ECC-based and one RSA-based
  - A 4th configuration with ECC and RSA vice versa

A special test configuration was used for test cases where the TOE shall be in the MANUFACTURING card life-cycle state before delivery. The tested configurations take into account the configurable options of the TOE as e.g. the use of ECC or RSA, different key lengths, use of Brainpool or NIST elliptic curves, contact-based and contactless interface, and other options related to PIN secrets or Active Authentication.

All configurations were tested appropriately with a similar amount of tests. The tests were performed in all life cycle phases that are in scope after TOE delivery within the according operation environment.

Originating from the behaviour defined in the SFRs of the ST, the developer specified test cases for all SFRs in order to cover the TSF. ATE_COV and ATE_DPT were taken into account and mapped to these test cases. The main test focus was laid upon the access right management and commands that are used in the operational usage phase for authentication, file access, key generation and signature creation. Tests using multiple application DFs to verify their separation were performed.

Additional test cases that could not be performed on a real smart card (e.g., memory faults and manipulation) were performed on an emulator.

Verdict for the activity:

The testing approach covers all TSFI as described in the functional specification and all subsystems of the TOE design adequately. All configuration options as described in the Security Target are covered, and a well-defined approach of possible combinations of options was applied. All test results collected in the test reports are as expected and in accordance with the TOE design and the desired TOE functionality.

Independent Testing according to ATE_IND

Approach for independent testing:

The testing approach covers:

- Examination of developer's testing amount, depth and coverage analysis and of the developer's test goals and plan for identification of gaps.
- Examination whether the TOE in its intended environment is operating as specified using repetition of developer's tests.
- Independent testing was performed by the evaluator at the ITSEF using developer's and evaluator's test equipment.

TOE test configurations:

Tests were done in different life-cycle phases (personalization / operational).

eSign and ePassport application, combinations of both applications and multiple instances were considered in the configurations.

Different options of application parameters were tested, e.g. RSA or EC-based cryptography (Brainpool and NIST curves), different key lengths or PIN/PUK options.

Subset size chosen:

During sample testing the evaluator chose to sample the developer functional tests at the ITSEF. Emulator tests with similar test focus were omitted.

During independent testing the evaluator focussed on the main security functionality as described in the Security Target. Access control and user authentication was mainly in focus.

Penetration tests as outcome of the vulnerability analysis were performed to cover potential vulnerabilities. Fuzzy tests, laser fault injections and side-channel analysis were conducted during testing.

Developer tests performed:

The developer performed tests of all TSF and interfaces with script-based tests and emulator test cases.

The evaluator selected a set of functional tests of the developer's testing documentation for sampling. Test cases with similar test focus were omitted.

Verdict for the activity:

During the evaluator's TSF subset testing the TOE operated as specified.

The evaluator verified the developer's test results by executing a sample of the developer's tests and verifying the test results for successful execution.

Penetration testing according to AVA_VAN

Overview:

The penetration testing was performed at the site of the ITSEF in the evaluator's test environment with the evaluator's test equipment. The samples were provided by the sponsor and developer. The test samples were configured and parameterized by the evaluator according to the guidance documentation. Different configurations of the TOE being intended to be covered by the current evaluation were tested using a distribution of configuration parameters to achieve a well-defined and wide coverage. The overall result is that no deviations were found between the expected result and the actual result of the tests. Moreover, no attack scenario with an attack potential of High was actually successful.

Penetration testing approach:

Based on the list of potential vulnerabilities applicable to the TOE in its operational environment created within the vulnerability analysis evaluation report, the evaluator created attack scenarios for the penetration tests, where the evaluator is of the opinion that the vulnerabilities could be exploitable. While doing so, the evaluator also considered all aspects of the security architecture of the TOE being not covered by the functional developer tests.

The source code reviews of the provided implementation representation accompanied the development of test cases and were used to find test input. The code inspection supported the testing activity by enabling the evaluator to verify implementation aspects that could hardly be covered by test cases.

The primary focus for devising penetration tests was to cover all potential vulnerabilities identified as applicable in the TOE's operational environment for which an appropriate test set was devised.

TOE test configurations:

The evaluators used TOE samples for testing that were configured according to the Security Target and guidance documentation. The samples were identified using the method as described by the developer in its guidance documentation. The TOE was configured with a reasonable coverage for different support of cryptographic algorithms and key sizes. Both, contactless and contact-based interface were covered during testing.

Test configurations were used that allow to reset the TOE in its initial state before initialization / personalization. For testing, the different variants of the IC platform were used. Whenever possible, the TOE as a whole (embedded software on IC) was used. For some test scenarios however, an emulator was used that would allow to directly view and manipulate the memory of the TOE.

Verdict for the activity:

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 [ST] provided that all measures required by the developer are applied.

8. Evaluated Configuration

The TOE named CardOS V6.0 ID R1.2 is a smart card product consisting of an operating system on an Infineon IC together with an application layer. Applications covered by this TOE comprise an electronic passport (ePass) application and/or a signature (eSign) application.

The IC platform comprises the integrated circuit SLC52GDA448* (IFX_CCI_000005 Design Step H13) and the cryptographic libraries RSA v2.08.007, EC v2.08.007, Toolbox v2.08.007, Base v2.08.007, HCL (Hash Cryptographic Library) v1.12.001, SCL (Symmetric Cryptographic Library) v2.04.002 and HSL (Hardware Support Library) v03.12.8812 from Infineon Technologies AG certified under ID BSI-DSZ-CC-1110-V8-2025 as relevant for the present TOE.

Three major configurations of the TOE are defined which differ in the description of the file system:

- ePassport: User data are stored in an ICAO-compliant ePass Application protected by PACE and EAC1. Here, EAC1 is used only for data groups 3 and 4.

- SSCD: User data are stored in an eSign Application conformant to “Protection profiles for secure signature creation device – Part 2: Device with key generation” ([PP]).
- eID: User data are contained in an ICAO-compliant ePass Application, in an eSign Application conformant to “Protection profiles for secure signature creation device – Part 2: Device with key generation“ ([PP]), and optional eID applications.

9. Results of the Evaluation

9.1. CC specific results

The ITSEF produced and provided the Evaluation Technical Report (ETR) [ETR] according to the requirements of the Scheme [EUCC-VO], [EUCC_PROG], the Common Criteria [CC], the Common Evaluation Methodology [CEM], and all relevant interpretations and guidelines of the Scheme (AIS) [AIS].

For the evaluation the following state-of-the-art documents and supporting documents specific for the technology were applied:

- EUCC Scheme State-of-the-Art document - Composite product evaluation for Smart Cards and similar devices for CC 3.1, Version 2, December 2024, ENISA
- EUCC Scheme State-of-the-Art document - Security Architecture requirements (ADV_ARC) for smart cards and similar devices extended to Secure Sub Systems in SoCs, Version 1.1, October 2023, ENISA
- EUCC Scheme State-of-the-Art document - Application of Attack Potential to smartcards and similar devices, Version 2, February 2025, ENISA
- Attack Methods for Smartcards and Similar Devices, Version 2.5, 2022-05, Joint Interpretation Working Group (confidential)
- EUCC Scheme State-of-the-Art document - Application of CC to integrated circuits, Version 2, December 2024, ENISA
- EUCC Scheme State-of-the-Art document - Minimum Site Security Requirements, Version 2, February 2025, ENISA
- EUCC Scheme State-of-the-Art document - STAR methodology, Version 1, February 2025, ENISA
- EUCC Scheme State-of-the-Art document - Security Evaluation and Certification of Qualified Electronic Signature/Seal Creation Devices according to eIDAS Regulation (EU) 910/2014, as amended by Regulation (EU) 2024/1183, Version 1, February 2025, ENISA
- EUCC Scheme State-of-the-Art document - Minimum ITSEF requirements for security evaluations of smart cards and similar devices, Version 1.1, October 2023, ENISA
- Functionality classes and evaluation methodology of physical and deterministic random number generators (AIS 20 and AIS 31, see [AIS])
- Guidance for smartcard evaluation (AIS 37, see [AIS])
- Information on cryptographic evaluation (AIS 46, see [AIS])
- Reuse of evaluation results (AIS 38, see [AIS])
- Test validity (AIS 25, see [AIS])

- Evaluation Methodology for CC Assurance Classes for EAL5+ and EAL6 (AIS 34, see [AIS])
- CC and CEM interpretations (AIS 32, see [AIS])
- Site Audits (AIS 1, see [AIS])

A document ETR for composite evaluation according to the State-of-the-Art document has not been provided in the course of this certification procedure. It could be provided by the ITSEF and submitted to the certification body for approval subsequently.

The assurance refinements outlined in the Protection Profiles [PP] were followed in the course of the evaluation of the TOE.

As a result of the evaluation, the verdict PASS is confirmed for the assurance components that are identified in chapter 1 of this report and claimed by the Security Target [ST] for the corresponding TOE identified in chapter 1 and 2 of this report.

The certificate

- is uniquely identified by: EUCC-3087-2026-0010, administration ID BSI-DSZ-CC-1162-V4-2026
- was issued on: 23 June 2026
- is valid until: 22 June 2031

The results of the evaluation are only applicable to the TOE as defined in chapter 1 and 2 and the configuration as outlined in chapter 8 above.

9.2. Results of cryptographic assessment

The table A.1 presented in the Security Target [ST], chapter A gives an overview of the cryptographic functionalities inside the TOE to enforce the security policy.

The strength of these cryptographic algorithms was not rated in the course of this certification procedure (see BSIG Section 52, Para. 4, Clause 2).

For the TOE's cryptographic functionalities, table A.1 in the Security Target outlines - where applicable - the standard of application where their specific appropriateness is stated. According to the referenced standards these algorithms are suitable for authentication, key agreement, authenticity, integrity, confidentiality and trusted channel. An explicit validity period is not given at this point.

For the rows no. 1, 2, 8 and 9 in table A.1 of the Security Target that address RSA and ECC based signature generation and key generation as regards the TOE's signature functionality, the security level of these algorithms as a kind of rating from cryptographic point of view is of relevance. Note that the security level refers to the pure cryptographic (mathematical) strength only, and does not take into account whatever exploitable weaknesses induced by side-channel leakage, physical attacks, or implementation flaws of any kind. Cryptographic functionalities with a security level of lower than 120 bits can no longer be regarded as secure without considering the application context. Therefore, for these functionalities it shall be checked whether the related cryptographic operations are appropriate for the intended system. Further hints and guidelines on the respective security level and validity period of the cryptographic algorithms can be derived from the document 'Technische Richtlinie BSI TR-02102-1' (refer to https://www.bsi.bund.de) and as well from the crypto catalogue [ACM].

The cryptographic algorithms and protocols as outlined in table A.1 of the Security Target are implemented in the card operating system and hereby make use of the

SLC52GDA448* (IFX_CCI_000005 Design Step H13) secure dual-interface controller and its related cryptographic libraries RSA v2.08.007, EC v2.08.007, Toolbox v2.08.007, Base v2.08.007, HCL (Hash Cryptographic Library) v1.12.001, SCL (Symmetric Cryptographic Library) v2.04.002 and HSL (Hardware Support Library) v03.12.8812 from Infineon Technologies AG certified under ID BSI-DSZ-CC-1110-V8-2025 as relevant for the present TOE. In particular, the core routines for RSA (signature generation and verification, key generation) and ECC (ECDSA signature generation and verification, ECDH, key generation), the SHA hash calculation and the symmetric cryptographic algorithms are taken from the cryptographic libraries. For random number generation and its DRG.4 the TOE uses the PTG.2 provided by the IC. The security evaluation of these cryptographic algorithms was performed in the framework of the certification of the IC with its related cryptographic libraries (refer to [CertRep IC]). The TOE relies on the correct (i.e. standard-conform) and secure implementation of these cryptographic algorithms. The remaining cryptographic implementation was analysed in the framework of the present composite evaluation of the TOE.

10. Obligations and Notes for the Usage of the TOE

Table 1 outlines the documents that contain necessary information on the intended use of the TOE including all security related information, conditions and instructions to be taken into account by the user. In addition, all aspects of Assumptions, Threats and OSPs as outlined in the Security Target and not covered by the TOE itself need to be met by the operational environment of the TOE.

Specific attention should be paid on the TOE functionality RSA key generation provided by the TOE command GENERATE ASYMMETRIC KEY PAIR that does not claim for side channel resistance and should therefore be carried out only within a trustworthy environment as outlined and specified by the Security Target [ST] and TOE guidance documentation [Guides].

The customer or user of the TOE shall take the statements of this certificate into account in its system risk management process. The user should define measures in its risk management that respond to emerging and new attack methods and techniques to the TOE until the TOE has been re-assessed.

The user also has to consider in its risk management the limited validity for the usage of cryptographic algorithms as outlined in chapter 9.

11. Security Target

For the purpose of publishing, the Security Target [ST] of the TOE / Information and communications technology (ICT) product is provided within a separate document as Annex A of this report.

12. Regulation specific aspects (eIDAS, QES)

Conformity of the IT Product identified in this certificate with the Regulation (EU) No 910/2014 and Amendment Regulation (EU) 2024/1183 as well as the related scope and restrictions are stated in a separate document [eIDAS Rep].

13. Definitions

13.1. Acronyms

AES	Advanced Encryption Standard
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
CEN	European Committee for Standardisation
cPP	Collaborative Protection Profile
CPU	Central Processing Unit
CRC	Cyclic Redundancy Check
DF	Dedicated File
DRG	Deterministic Random Number Generator
EAC	Extended Access Control
EAL	Evaluation Assurance Level
EC	Elliptic Curve
ECC	Elliptic Curve Cryptography
EEPROM	Electrically Erasable Programmable Read Only Memory
eIDAS	electronic IDentification, Authentication and trust Services
ETR	Evaluation Technical Report
HCL	Hash Cryptographic Library
HSL	Hardware Support Library
IFD	Interface Device
ISSS	Information Society Standardisation System
ICAO	International Civil Aviation Organization
ICT	Information and communications technology
IT	Information Technology
ITSEF	Information Technology Security Evaluation Facility
NIST	National Institute of Standards and Technology
PACE	Password Authenticated Connection Establishment
PIN	Personal Identification Number
PP	Protection Profile

PTG	Physical Ture Random Number Generator
PUK	Personal Unblocking Key
QES	Qualified Electronic Signature
ROM	Read Only Memory
RSA	Rivest Shamir Adleman
SAR	Security Assurance Requirement
SCA	Signature Creation Application
SCL	Symmetric Cryptographic Library
SCP	Smart Card Platform
SFP	Security Function Policy
SFR	Security Functional Requirement
SHA	Secure Hash Algorithm
SSCD	Secure Signature Creation Device
ST	Security Target
STAR	Site Technical Audit Report
SVD	Signature Verification Data
TC	Trusted Channel
TOE	Target of Evaluation
TSF	TOE Security Functionality
TSFI	TSF Interface
UART	Universal Asynchronous Receiver Transmitter
VAD	Verification Authentication Data

13.2. 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.

14. Bibliography

[EUCC-VO] Implementing Regulation (EU) 2024/482 of the European Parliament and of the Council of 31 January 2024 laying down rules for the application of Regulation (EU) 2019/881 of the European Parliament and of the Council as regards the adoption of the European Common Criteria-based cybersecurity certification scheme (EUCC)

and

Implementation Regulation (EU) 2025/2462 of 8 December 2025 amending Implementing Regulation (EU) 2024/482 as regards definitions, ICT product series certification, assurance continuity and state-of-the-art document

[CC] Common Criteria for Information Technology Security Evaluation, Version 3.1,
Part 1: Introduction and general model, Revision 5, April 2017
Part 2: Security functional components, Revision 5, April 2017
Part 3: Security assurance components, Revision 5, April 2017

https://www.commoncriteriaportal.org

[CEM] Common Methodology for Information Technology Security Evaluation (CEM), Evaluation Methodology, Version 3.1, Revision 5, April 2017

https://www.commoncriteriaportal.org

[EUCC_SOTA] EUCC state-of-the-art documents:

https://certification.enisa.europa.eu/publications/eucc-state-art-documents_en

[EUCC_PROG] EUCC program of the BSI: Scheme documentation describing the certification process (EUCC)

https://www.bsi.bund.de/zertifizierung

[EUCC_CERT] EUCC Certificates, periodically updated list published on ENISA's website on European cybersecurity certification schemes (https://certification.enisa.europa.eu/), but also on BSI's website (https://www.bsi.bund.de/zertifizierungsreporte)

[AIS] Application Notes and Interpretations of the Scheme (AIS) as relevant for the TOE[6]

[6]specifically

- AIS 1, Version 14, Durchführung der Ortsbesichtigung in der Entwicklungsumgebung des Herstellers

https://www.bsi.bund.de/AIS

[ST] Security Target for BSI-DSZ-CC-1162-V4-2026, Security Target 'CardOS V6.0 ID R1.2', Revision 2.50R, 2026-05-04, Eviden Germany GmbH

[PP] Protection Profiles:

Protection profiles for secure signature creation device – Part 2: Device with key generation, CEN/ISSS, EN 419211-2:2013, 2016-06-30, BSI-CC-PP-0059-2009-MA-02

Protection profiles for secure signature creation device – Part 4: Extension for device with key generation and trusted communication with certificate generation application, CEN/ISSS, EN 419211-4:2013, 2016-06-30, BSI-CC-PP-0071-2012-MA-01

Protection profiles for secure signature creation device – Part 5: Extension for device with key generation and trusted communication with signature creation application, CEN/ISSS, EN 419211-5:2013, 2016-06-30, BSI-CC-PP-0072-2012-MA-01

Machine Readable Travel Document with "ICAO Application" Extended Access Control with PACE, Version 1.3.2, 5 December 2012, BSI-CC-PP-0056-V2-2012-MA-02

Common Criteria Protection Profile Machine Readable Travel Document using Standard Inspection Procedure with PACE (PACE_PP), Version 1.01, 22 July 2014, BSI-CC-PP-0068-V2-2011-MA-01

[ETR] Evaluation Technical Report for BSI-DSZ-CC-1162-V4-2026, Evaluation Technical Report Summary (ETR Summary), Version 2, 2026-05-29, TÜV Informationstechnik GmbH (confidential document)

- AIS 14, Version 7, Anforderungen an Aufbau und Inhalt der ETR-Teile (Evaluation Technical Report) für Evaluationen nach CC (Common Criteria)
- AIS 19, Version 9, Anforderungen an Aufbau und Inhalt der Zusammenfassung des ETR (Evaluation Technical Report) für Evaluationen nach CC (Common Criteria) und ITSEC
- AIS 20, Version 3, Funktionalitätsklassen und Evaluationsmethodologie für deterministische Zufallszahlengeneratoren
- AIS 25, Version 9, Anwendung der CC auf Integrierte Schaltungen including JIL Document and CC Supporting Document
- AIS 26, Version 10, Evaluationsmethodologie für in Hardware integrierte Schaltungen including JIL Document and CC Supporting Document
- AIS 31, Version 3, Funktionalitätsklassen und Evaluationsmethodologie für physikalische Zufallszahlengeneratoren
- AIS 32, Version 7, CC-Interpretationen im deutschen Zertifizierungsschema
- AIS 34, Version 3, Evaluation Methodology for CC Assurance Classes for EAL 5+ (CCv2.3 & CCv3.1) and EAL 6 (CCv3.1)
- AIS 37, Version 3, Terminologie und Vorbereitung von Smartcard-Evaluierungen
- AIS 38, Version 2, Reuse of evaluation results
- AIS 46, Version 3, Informationen zur Evaluierung von kryptographischen Algorithmen und ergänzende Hinweise für die Evaluierung von Zufallszahlengeneratoren

[ConfList] Configuration List for BSI-DSZ-CC-1162-V4-2026, Configuration List ’CardOS V6.0 ID R1.2’ and ’CardOS V6.0 ID R1.2 (BAC)’, Version 1.46, 2026-05-04, Eviden Germany GmbH (confidential document)

[Guides] Guidance documentation for the TOE (confidential documents):

CardOS V6.0 User’s Manual, 06/2023, Eviden Germany GmbH

User Guidance ’CardOS V6.0 ID R1.2’ and ’CardOS V6.0 ID R1.2 (BAC)’, Revision 1.60R, 2024-11-13, Eviden Germany GmbH

Administrator Guidance ’CardOS V6.0 ID R1.2’ and ’CardOS V6.0 ID R1.2 (BAC)’, Revision 1.70R, 2024-11-13, Eviden Germany GmbH

Application Base Guidance ’CardOS V6.0 ID R1.2’ and ’CardOS V6.0 ID R1.2 (BAC)’, Revision 1.60R, 2024-10-31, Eviden Germany GmbH

Application ePassport Guidance ’CardOS V6.0 ID R1.2’ and ’CardOS V6.0 ID R1.2 (BAC)’, Revision 1.60R, 2024-10-31, Eviden Germany GmbH

Application eSign Guidance ’CardOS V6.0 ID R1.2’ and ’CardOS V6.0 ID R1.2 (BAC)’, Revision 1.60R, 2024-11-20, Eviden Germany GmbH

Packages & Release Notes, CardOS V6.0, 11/2024, Eviden Germany GmbH

[ST IC] Security Target of the underlying hardware platform, Security Target IFX_CCI_000003h, IFX_CCI_000005h, IFX_CCI_000008h, IFX_CCI_00000Ch, IFX_CCI_000013h, IFX_CCI_000014h, IFX_CCI_000015h, IFX_CCI_00001Ch, IFX_CCI_00001Dh, IFX_CCI_000021h, IFX_CCI_000022h design step H13, Version 6.2, 26 June 2025, Infineon Technologies AG, BSI-DSZ-CC-1110-V8-2025 (confidential document)

Security Target Lite of the underlying hardware platform, Security Target IFX_CCI_000003h, IFX_CCI_000005h, IFX_CCI_000008h, IFX_CCI_00000Ch, IFX_CCI_000013h, IFX_CCI_000014h, IFX_CCI_000015h, IFX_CCI_00001Ch, IFX_CCI_00001Dh, IFX_CCI_000021h, IFX_CCI_000022h design step H13, Version 6.2, 26 June 2025, Infineon Technologies AG, BSI-DSZ-CC-1110-V8-2025 (sanitised public document)

[CertRep IC] Certification Report BSI-DSZ-CC-1110-V8-2025 for Infineon Security Controller IFX_CCI_000003h, IFX_CCI_000005h, IFX_CCI_000008h, IFX_CCI_00000Ch, IFX_CCI_000013h, IFX_CCI_000014h, IFX_CCI_000015h, IFX_CCI_00001Ch, IFX_CCI_00001Dh, IFX_CCI_000021h, IFX_CCI_000022h in the design step H13 and including optional software libraries and dedicated firmware in several versions from Infineon Technologies AG, 5 August 2025, Bundesamt für Sicherheit in der Informationstechnik (BSI)

[ETRfComp IC] ETR for Composite Evaluation of the underlying hardware platform Infineon Security Controller IFX_CCI_000003h, IFX_CCI_000005h, IFX_CCI_000008h, IFX_CCI_00000Ch, IFX_CCI_000013h, IFX_CCI_000014h, IFX_CCI_000015h, IFX_CCI_00001Ch, IFX_CCI_00001Dh, IFX_CCI_000021h, IFX_CCI_000022h design step

H13 from certification procedure BSI-DSZ-CC-1110-V8-2025, Version 2, 25 July 2025, TÜV Informationstechnik GmbH (confidential document)

[STAR] STAR Reports (confidential documents, refer to BSI-DSZ-CC-1162-V2-MA-01):

Site Technical Audit Report (STAR) – Munich, Version 1, 15 July 2024, TÜV Informationstechnik GmbH

Site Technical Audit Report (STAR) – Fuerth, Version 1, 15 July 2024, TÜV Informationstechnik GmbH

Site Technical Audit Report (STAR) – Split, Version 1, 15 July 2024, TÜV Informationstechnik GmbH

[eIDAS Rep] Certificate of Conformity pursuant to Article 29 (1), 39 (1) and Annex II of the Regulation (EU) No 910/2014 and Amendment Regulation (EU) 2024/1183 for CardOS V6.0 ID R1.2, Bundesamt für Sicherheit in der Informationstechnik (BSI), Version 1.0, June 2026

[ACM] EUCC Agreed Cryptographic Mechanisms, Version 2.0, April 2025, European Cybersecurity Certification Group, Sub-group on Cryptography

https://certification.enisa.europa.eu/publications/eucc-guidelines-cryptography_en

C. 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

Annex B of Certification Report BSI-DSZ-CC-1162-V4-2026

Evaluation results regarding development and production environment

The IT product CardOS V6.0 ID R1.2 (Target of Evaluation, TOE, also named as ICT product) has been evaluated at an approved evaluation facility using the Common Methodology for IT Security Evaluation (CEM) [CEM].

As a result of the TOE certification, dated 23 June 2026, the following results regarding the development and production environment apply. The Common Criteria assurance requirements ALC – Life cycle support as claimed by the ST [ST] and that are stated in chapter 1 of this report are fulfilled for the development and production sites of the TOE listed below:

a) Eviden Germany GmbH, Otto-Hahn-Ring 6, 81739 Munich, Germany (SW Development)

b) Eviden Germany GmbH, Wuerzburger Str. 121, 90766 Fuerth, Germany (SW Development)

c) Eviden d.o.o, Matice Hrvatske 15, 21000 Split, Croatia (SW Development)

d) For development and production sites regarding the underlying IC platform please refer to the Certification Report BSI-DSZ-CC-1110-V8 [CertRep IC].

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

Note: End of report