Certification Report

BSI-DSZ-CC-1112-V2-2021

for

CardOS DI V5.4 QES Version 1.0

from

Atos

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-1112-V2-2021 (*)

Digital signature: Secure Signature Creation Devices (SSCD)

CardOS DI V5.4 QES Version 1.0

from	Atos
PP Conformance:	EN 419211-2:2013 (BSI-CC-PP-0059-2009-MA-02), EN 419211-4:2013 (BSI-CC-PP-0071-2012-MA-01), EN 419211-5:2013 (BSI-CC-PP-0072-2012-MA-01) (**)
Functionality:	PP conformant plus product specific extensions Common Criteria Part 2 extended
Assurance:	Common Criteria Part 3 conformant EAL 4 augmented by ALC_DVS.2 and AVA_VAN.5

SOGIS
Recognition Agreement

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 and by advice of the Certification Body for components beyond EAL 5 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 5.

(**) The IT Product identified in this certificate fulfils PP EN 419211-2:2013, PP EN 419211-4:2013 as well as PP EN 419211-5:2013 and is therefore a compliant signature creation device according to Article 30(3.(a)) ("Certification of qualified electronic signature creation devices", 3.(a)) of eIDAS Regulation (Regulation No 910/2014 OF THE EUROPEAN PARLIAMENT AND OF THE COUNCIL of 23 July 2014).

Common Criteria
Recognition Arrangement
recognition for components
up to EAL 2 and ALC_FLR
only

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

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

Bonn, 29 September 2021

For the Federal Office for Information Security

Sandro Amendola L.S.
Head of Division

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

This page is intentionally left blank.

Contents

A. Certification

1. 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.

2. 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[1]
- BSI Certification and Approval Ordinance[2]
- BSI Schedule of Costs[3]
- 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]

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

[2] 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

[3] 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

- Common Criteria for IT Security Evaluation (CC), Version 3.1[4] [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]

3. 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.

3.1. European Recognition of 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.

The basic recognition level includes Common Criteria (CC) Evaluation Assurance Levels EAL 1 to EAL 4. 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 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.sogis.eu.

The SOGIS-MRA logo printed on the certificate indicates that it 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 under SOGIS-MRA for all assurance components selected.

3.2. 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 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.

[4] Proclamation of the Bundesministerium des Innern of 12 February 2007 in the Bundesanzeiger dated 23 February 2007, p. 3730

This certificate is recognized according to the rules of CCRA-2014, i. e. up to and including CC part 3 EAL 2+ ALC_FLR components.

4. 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 CardOS DI V5.4 QES Version 1.0 has undergone the certification procedure at BSI. This is a re-certification based on BSI-DSZ-CC-1112-2020. Specific results from the evaluation process BSI-DSZ-CC-1112-2020 were re-used.

The evaluation of the product CardOS DI V5.4 QES Version 1.0 was conducted by TÜV Informationstechnik. The evaluation was completed on 14 September 2021. TÜV Informationstechnik is an evaluation facility (ITSEF)[5] recognised by the certification body of BSI.

For this certification procedure the sponsor and applicant is: Atos.

The product was developed by: Atos.

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

5. Validity of the Certification Result

This Certification Report applies only to the version of the product as indicated. The confirmed assurance package is 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 components and assurance levels please refer to CC itself. Detailed references are listed in part C of this report.

The Certificate issued confirms the assurance of the product claimed in the Security Target at the date of certification. As attack methods evolve over time, the resistance of the certified version of the product against new attack methods needs to be re-assessed. Therefore, the sponsor should apply for the certified product being monitored within the assurance continuity program of the BSI Certification Scheme (e.g. by a re-assessment or 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 would 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 29 September 2021 is valid until 28 September 2026. Validity can be re-newed by re-certification.

The owner of the certificate is obliged:

[5] Information Technology Security Evaluation Facility

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,
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.

6. Publication

The product CardOS DI V5.4 QES 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[6] of the product. The Certification Report may also be obtained in electronic form at the internet address stated above.

[6] Atos
Otto-Hahn-Ring 6
81739 München
Deutschland

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 a composite TOE named CardOS DI V5.4 QES Version 1.0 (developed by Atos Information Technology GmbH). The TOE is a smart card operating system dedicated to be used as a Secure Signature Creation Device (SSCD) and in accordance with eIDAS. It consists of the application QES, the OS 'CardOS DI V5.4', configuration scripts for initialization, personalization and AQES update, the according guidance documents and the underlying hardware platform together with the crypto library. There are two configurations available: TC-SCA-Mandatory and TC-SCA-CL-Only.

The platform comprises the integrated circuit SLE78CLFX*P (M7892 Design Steps D11 and G12) and the libraries RSA v2.07.003, EC v2.07.003, Toolbox v2.07.003, Base v2.07.003, SHA-2 v1.01 and Symmetric Crypto Library (SCL) v2.02.010 certified according to CC v3.1 under the ID BSI-DSZ-CC-0891-V4-2019.

The TOE protects the SCD (Signature Creation Data) during the whole life cycle as to be used in a signature creation process solely by its signatory.

The Security Target [6] is the basis for this certification. It is based on the certified Protection Profiles [8]. See [6] Chapter 5.2 for further information on the PP claim for the different TOE configurations:

- 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

The TOE Security Assurance Requirements (SAR) are based entirely on the assurance components defined in Part 3 of the Common Criteria (see part C or [1], Part 3 for details). The TOE meets the assurance requirements of the Evaluation Assurance Level EAL 4 augmented by ALC_DVS.2 and AVA_VAN.5.

The TOE Security Functional Requirements (SFR) relevant for the TOE are outlined in the Security Target [6], chapter 9.1. They are selected from Common Criteria Part 2 and some of them are newly defined. Thus the TOE is CC Part 2 extended.

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

TOE Security Functionality	Addressed issue
SF_HardwareCryptoLibrary	Hardware and cryptographic library
SF_UserIdentificationAuthentication	Identification and authentication of the user roles
SF_AccessControl	Regulation of access by external entities to operations of the TOE
SF_KeyManagement	Management of keys, generation of keys
SF_SignatureCreation	Signature creation
SF_Protection	Protection of TSF, TSF data and user data

Table 1: TOE Security Functionalities

For more details please refer to the Security Target [6], chapter 10.1.

The assets to be protected by the TOE are defined in the Security Target [6], chapter 6.1.1. Based on these assets the TOE Security Problem is defined in terms of Assumptions, Threats and Organisational Security Policies. This is outlined in the Security Target [6], chapter 6.

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:

CardOS DI V5.4 QES Version 1.0

The following table outlines the TOE deliverables:

TOE deliverables provided to the chip manufacturer				
1.	SW	Combined OS Software and InitData	Version 1.0	The operating system software is delivered from the developer to Infineon to be manufactured on the certified hardware. The data is encrypted and a secure upload mechanism by Infineon is used. After upload the consistency of deliverables is verified by the developer before production starts.
TOE deliverables provided to the Trust Center				
1.	HW	SLE78CLFX*P* (M7892 D11/G12)	M7892 D11/ G12	IC package The composite TOE is delivered from Infineon to Trust Center (customer). The delivery procedures that were in the scope of the platform certification are used. The SW components are loaded in protected part of NVM and the flash loader is blocked before delivery.
2.	SW (Atos)	CardOS DI V5.4 for 404kByte flash	“C904”	
3.	SW (Infineon)	RSA library	2.07.003	
4.		EC library	2.07.003	
5.		Toolbox	2.07.003	
6.		Base	2.07.003	
7.		SHA-2 library	1.01	
8.		Symmetric Crypto Library	2.02.010	
9.	DOC	*User’s Manual ‘CardOS V5.4’*	2020-02	As PDF via signed and encrypted mail.
10.		*User Guidance ’CardOS DI V5.4 QES Version 1.0’*	1.30R	

TOE deliverables provided to the chip manufacturer				
11.		*Application QES Description ‘CardOS DI V5.4 QES, Version 1.0’*	1.50R	
12.		*Administrator Guidance ‘CardOS DI V5.4 QES, Version 1.0’*	1.30R	
13.		*CardOS DI V5.4 Packages & Release Notes*	2020-03	
14.	DATA	StartKey_1 (included in command sequence in the csf files)	For the detailed list of scripts for these variants please refer to [11] chapter 5.3.	Data files
15.		Initialization script for RSA or EC based QES packet, ConfigApp_Init.csf		
16.		Personalization script for RSA or EC based QES packet, ConfigApp_Person.csf		
17.		Initialization constants script for QES packet, ConfigData_Init.csf		
18.		Personalization variables script for QES packet, ConfigData_Person.csf		
19.		File System Checksum Package, V54DI_verifyfschecksum_Package.csf		
20.		Service Package, V54DI_ServicePack_Package.csf		

Table 2: Deliverables of the TOE

The composite TOE consists of the application QES, the OS ‘CardOS DI V5.4’, configuration scripts for initialization, personalization and AQES update, the underlying hardware platform (integrated circuit SLE78CLFX*P (M7892 Design Steps D11 and G12) and the libraries RSA v2.07.003, EC v2.07.003, Toolbox v2.07.003, Base v2.07.003, SHA-2 v1.01 and Symmetric Crypto Library (SCL) v2.02.010) as well as guidance documentation.

First, the software developer Atos delivers the operating system, which is later placed in the TOE hardware ROM, and the initialization data (InitData), which is later stored in the TOE hardware EEPROM, in one file of a specific format to the chip manufacturer. The produced chips with the OS are then sent from the chip manufacturer to the Trust Center. The produced chips may be sent directly from the chip manufacturer to the Trust Center or e.g. via logistic centres or distributors. This is possible since the TOE protects itself during delivery and standard procedures for packing, storage and distribution can be applied.

The Trust Center is provided with the guidance and initialisation/personalisation scripts (also for implementation of the service package), from Atos.

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:

- Cryptographic Support
- User Data Protection
- Identification and Authentication
- Security Management

- Protection of the TSF
- Trusted Path/Channels

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.SVD_Auth	(Authenticity of the SVD)
OE.CGA_Qcert	(Generation of qualified certificates)
OE.HID_VAD	(Protection of the VAD)
OE.DTBS_Intend	(SCA sends data intended to be signed)
OE.DTBS_Protect	(SCA protects the data intended to be signed)
OE.Signatory	(Security obligation of the signatory)
OE.Dev_Prov_Service provisioning	(Authentic SSCD provided by SSCD-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.HID_TC_VAD_Exp	(Trusted channel of HID for VAD export)
OE.SCA_TC_DTBS_Exp	(Trusted channel of SCA for DTBS export)
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 [6], chapter 7.2.

5. Architectural Information

The composite TOE CardOS DI V5.4 QES is a smart card operating system based on a certified hardware platform together with the crypto library. The TOE comprises ten subsystems, listed with a short description in the following itemization:

- Startup: Performs action needed at startup only and not further used after entry into user commands processing loop.
- Command Manager: Provides the main interface between the chip-card and the host system. The subsystem receives APDU commands, checks access rights and if access is permitted the implementation is called and results are returned.
- Protocol Manger: Protocol Manager monitors the correctness of the data transmission. Its main functionality consists of sending bytes and receiving data to and from the IFD over the UART of the hardware (CPU Core).
- Command Layer: Implements the 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, 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: AES and SHA implementations, wrapper modules for IFX libraries 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: This subsystem retrieves the results of performed routines.

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

7.1. Developer's Test according to ATE_FUN

The developer’s testing effort is summarised as follows:

TOE configurations tested:

The tests were performed with the composite smartcard product CardOS DI V5.4 QES on the IC Infineon M7892 Design Steps D11 and G12. The developer tested the following configurations:

- MassSig_brain512
- MassSig_nist256
- MultipleSig_brain384
- MultipleSig_nist384
- SingleSig_brain256
- SingleSig_nist521
- MassSig_3072
- MultipleSig_2048

- SingleSig_3072
- “None”

The additional Configuration “None” is a special test configuration needed for test cases where the TOE shall be in the MANUFACTURING card life cycle before delivery. The tested configurations take into account the configurable options of the TOE as e.g. the use of elliptic curves or RSA, different key lengths, use of Brainpool or NIST elliptic curves, different mandatory use of a trusted channel, contact and contactless interface, and other options related to PIN secrets and QES.

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.

Testing Approach:

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 to allow signature creation.

Additional test cases that could not be performed on a real smartcard (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 ST 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.

7.2. Evaluator Tests - Independent Testing according to ATE_IND

The evaluator’s testing effort is described as follows, outlining the testing approach, configuration, depth and results.

Approach for independent testing:

- 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 iterations of developer’s tests.
- Independent testing was performed by the evaluator in Essen using developer’s and evaluator’s test equipment.

TOE test configurations:

- Tests with all different IC platform types (M7892 D11 and G12).
- Tests were done in different life-cycle phases (personalisation / operational).
- Different configurations (RSA/EC-based cryptography, options on QES application, trusted channel and PIN/PUK mechanism) and different key lengths were tested.

Subset size chosen:

- During sample testing the evaluator chose to sample the developer functional tests at the Evaluation Body for IT Security in Essen. Emulator tests with similar test focus were omitted.
- During independent testing the evaluator focussed on the main security functionality as described in the ST. 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.

7.3. Evaluator Tests - Penetration Testing according to AVA_VAN

Overview:

The penetration testing was performed at the site of the evaluation body TÜV Informationstechnik 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 parametrized 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 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 ST and guidance documentation. The samples were identified using the method as described by the developer in its guidance documentation. TOEs were 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 initialisation/personalisation. For testing, the different variants of the IC platform (as described in the Security Target [6], chapter 4.3.) 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.

Attack scenarios having been tested:

- DFA/LFI
- Side Channel Attacks
- Timing Analysis (PIN)
- Changing the predefined sequence of invocation of components / Using a component in an unexpected context or for an unexpected purpose
- Executing commands not intended to be executable, or making it executable
- Command input buffers overflow
- Direct Protocol Attacks on authentication mechanisms
- Replay Attacks on authentication mechanisms / Potential insecure behaviour of the TOE after an interception
- Padding Oracle attack on Secure Messaging

Verdict for the sub-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 the Security Target [6] provided that all measures required by the developer are applied.

7.4. Summary of Test Results and Effectiveness Analysis

The test results yielded that no deviations were found between the expected and the actual test results. No attack scenario with the attack potential high was actually successful in the TOE’s operational environment as defined in the Security Target [6] provided that all measures required by the developer are applied.

8. Evaluated Configuration

This certification covers the following configurations of the TOE:

There are two configurations of the TOE: TC-SCA-Mandatory and TC-SCA_CL-Only.

Details can be found in the Security Target [6], chapter 4.3.

9. Results of the Evaluation

9.1. CC specific results

The Evaluation Technical Report (ETR) [7] was provided by the ITSEF according to the Common Criteria [1], the Methodology [2], the requirements of the Scheme [3] and all interpretations and guidelines of the Scheme (AIS) [4] as relevant for the TOE.

The Evaluation Methodology CEM [2] was used for those components up to EAL 5 extended by advice of the Certification Body for components beyond EAL 5.

The following guidance specific for the technology was used:

(i) Terminologie und Vorbereitung von Smartcard-Evaluierungen (see [4], AIS 37)

(ii) Informationen zur Evaluierung von kryptographischen Algorithmen und ergänzende Hinweise für die Evaluierung von Zufallszahlengeneratoren (see [4], AIS 46)

For smart card specific methodology the scheme interpretations AIS 25, AIS 26 and AIS 36 were used (see [4]). For RNG assessment the scheme interpretations AIS 31 and AIS 20 were used (see [4]).

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

- All components of the EAL 4 package including the class ASE as defined in the CC (see also part C of this report)
- The components ALC_DVS.2 and AVA_VAN.5 augmented for this TOE evaluation.

As the evaluation work performed for this certification procedure was carried out as a re-evaluation based on the certificate BSI-DSZ-CC-1112-2020, re-use of specific evaluation tasks was possible. The focus of this re-evaluation was on AVA.

The evaluation has confirmed:

- PP Conformance: Protection profiles for secure signature creation device - Part 2: Device with key generation, 18 May 2013, BSI-CC-PP-0059-2009-MA-02,

  Protection profiles for secure signature creation device - Part 4: Extension for device with key generation and trusted channel to certificate generation application, CEN / ISSS - Information Society Standardization System, 12 October 2013, BSI-CC-PP-0071-2012-MA-01,

  Protection profiles for secure signature creation device - Part 5: Extension for device with key generation and trusted channel to signature creation application, CEN / ISSS - Information Society Standardization System, 12 October 2013, BSI-CC-PP-0072-2012-MA-01 [8]
- for the Functionality: PP conformant plus product specific extensions
  Common Criteria Part 2 extended
- for the Assurance: Common Criteria Part 3 conformant
  EAL 4 augmented by ALC_DVS.2 and AVA_VAN.5

- See [6] Chapter 5.2 for further information on the PP claim for the different TOE configurations
- For specific evaluation results regarding the development and production environment see annex B in part D of this report.
- The results of the evaluation are only applicable to the TOE as defined in chapter 2 and the configuration as outlined in chapter 8 above.
- The evaluation was performed as a composite evaluation according to AIS 36 and therefore relies on the platform certification of the used IC (certification ID BSI-DSZ-CC-0891-V4-2019) [9], [10].

9.2. Results of cryptographic assessment

The table presented in appendix A of the Security Target gives an overview of the cryptographic functionalities inside the TOE to enforce the security policy and outlines the standard of application where its specific appropriateness is stated.

The strength of the these cryptographic algorithms was not rated in the course of this certification procedure (see BSIG Section 9, Para. 4, Clause 2).

10. Obligations and Notes for the Usage of the TOE

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

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

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

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. Regulation specific aspects (eIDAS, QES)

The IT Product identified in this certificate fulfils

- PP EN 419211-2:2013 (Protection profiles for secure signature creation device - Part 2: Device with key generation (BSI-CC-PP-0059-2009-MA-02))

This Protection Profile is taken from the list of standards identified in COMMISSION IMPLEMENTING DECISION (EU) 2016/650 of 25 April 2016, Annex, for the security assessment of qualified signature and seal creation devices pursuant to Articles 30(3) and 39(2) of Regulation (EU) No 910/2014 of the European Parliament and of the Council on electronic identification and trust services for electronic transactions in the internal market.

Therefore, the IT-product certified is technically suitable to be a compliant signature creation device according to Article 30(3) and a compliant seal creation device according to Article 39(2) of Regulation (EU) No 910/2014 of the European Parliament and of the Council of 23 July 2014 and to fulfil the requirements laid down in Article 29(1), Article 39(1) and Annex II provided that the following operational conditions are followed:

- The obligations and notes for the usage of the TOE have to be followed as outlined in chapter 10 of this report.
- The trust service provider has to follow the operational requirements from the regulation as relevant for a compliant signature creation device and a compliant seal creation device as well as to follow all related obligations from its supervisory body.
- For the creation of qualified electronic signatures or qualified electronic seals the product has to use the cryptographic algorithms in accordance with the SOG-IS Crypto Evaluation Scheme - Agreed Cryptographic Mechanisms [13] which are depicted in Table 3.
- The trust service provider shall consider the results of the certification and the operational conditions listed above within the system risk management process for the product usage. Specifically, the evolution of limitations of cryptographic algorithms and parameters[7] as well as the evolution of attack methods related to the product or to the type of product has to be considered e.g. by a regular re-assessment of the TOE assurance.

No.	Cryptographic Mechanism	Key Size in Bits	Acceptability Deadline according to [13] as of today
1	RSA PKCS#1 v1.5 [14, 15, 16]	Modulus length = 2048	31. December 2025
2	RSA PKCS#1 v1.5 [14, 15, 16]	Modulus length = 3072	31. December 2027+[8]
3	RSA PSS (PKCS#1 v2.1) [14, 15, 16]	Modulus length = 2048	31. December 2025
4	RSA PSS (PKCS#1 v2.1) [14, 15, 16]	Modulus length = 3072	None
5	ECDSA [17, 18]	ECC Key sizes corresponding to the used elliptic curve brainpoolP{256, 384, 512}r1 [19] secp{256, 384, 521}r1 [17, Appendix D.1.2]	None
6	SHA-2, hash length (bits) = 224 [20, 21]	-	31. December 2025
7	SHA-2, hash length (bits) = 256, 384, 512 [20, 21]	-	None

Table 3: Cryptographic algorithms of the TOE in accordance with [13]

[7] Future updates of the catalogue [13] may shorten or extend the acceptance time frame. This may need actions for the usage of the product to be taken.

[8] According to [13] the validity period of the algorithm may be extended in future versions of the document.

Out of this, the compliance of the QSCD / QSealCD is confirmed under the conditions mentioned above within the following categories:

- Components and procedures for the generation of signature resp. seal creation data
- Components and procedures for the storage of signature resp. seal creation data
- Components and procedures for the processing of signature resp. seal creation data

13. Definitions

13.1. Acronyms

AES	Advanced Encryption Standard
AIS	Application Notes and Interpretations of the Scheme
APDU	Application Protocol Data Unit
AQES	Application Qualified Electronic Signature
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
CL	Contactless
cPP	Collaborative Protection Profile
CPU	Central Processing Unit
CRC	Cyclic Redundancy Check
EAL	Evaluation Assurance Level
EEPROM	Electrically Erasable Programmable Read Only Memory
eIDAS	electronic IDentification, Authentication and trust Services
ETR	Evaluation Technical Report
IFD	Interface Device
ISSS	Information Society Standardisation System
IT	Information Technology
ITSEF	Information Technology Security Evaluation Facility
NIST	National Institute Of Standards And Technology
PIN	Personal Identification Number
PP	Protection Profile
PUK	Personal Unblocking Key
QES	Qualified Electronic Signature

ROM	Read Only Memory
SAR	Security Assurance Requirement
SCA	Signature Creation Application
SCL	Symmetric Crypto 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
SVD	Signature Validation 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

[1] 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

[2] Common Methodology for Information Technology Security Evaluation (CEM), Evaluation Methodology, Version 3.1, Rev. 5, April 2017, https://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 BSI-DSZ-CC-1112-V2-2021, Revision 1.61R, 2020-04-17, Security Target 'CardOS DI V5.4 QES V1.0', Atos Information Technology GmbH (sanitised public document)

[7] Evaluation Technical Report, Version 1, 2021-09-09, EVALUATION TECHNICAL REPORT SUMMARY (ETR SUMMARY), TÜV Informationstechnik GmbH, (confidential document)

[8] 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

[9] specifically

- 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 36, Version 5, Kompositionsevaluierung including JIL Document and CC Supporting Document
- AIS 37, Version 3, Terminologie und Vorbereitung von Smartcard-Evaluierungen
- AIS 46, Version 3, Informationen zur Evaluierung von kryptographischen Algorithmen und ergänzende Hinweise für die Evaluierung von Zufallszahlengeneratoren

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

[9] Certification Report, BSI-DSZ-CC-0891-V4-2019 for Infineon Security Controller M7892 Design Steps D11 and G12, with specific IC dedicated firmware and optional software from Infineon Technologies AG, 19.12.2019, Bundesamt für Sicherheit in der Informationstechnik (BSI)

[10] ETR for composite evaluation (according to AIS 36) for BSI-DSZ-CC-0891-V4-2019, Version 2, 2019-12-16, “Evaluation Technical Report for Conmposite Evaluation (ETR Comp)”, TÜV Informationstechnik GmbH (confidential document)

[11] Configuration list for the TOE, Revision 1.30, 2020-05-08, Configuration List ’CardOS DI V5.4 QES Version 1.0’ (confidential document)

[12] Guidance documentation for the TOE:

User’s Manual ‘CardOS V5.4’, –, 2020-02, Atos Information Technology GmbH

User Guidance ’CardOS DI V5.4 QES Version 1.0’, Version 1.30R, 2020-04-17, Atos Information Technology GmbH

Administrator Guidance ‘CardOS DI V5.4 QES Version 1.0’, Version 1.30R, 2020-04-17, Atos Information Technology GmbH

Application QES Description ‘CardOS DI V5.4 QES Version 1.0’, Version 1.50R, 2020-04-17, Atos Information Technology GmbH

[13] SOG-IS Crypto Evaluation Scheme Agreed Cryptographic Mechanisms, Version 1.2, January 2020

[14] J. Jonsson and B. Kaliski. Public-Key Cryptography Standard (PKCS) #1: RSA Cryptography Specifications Version 2.1. 2003.

[15] RSA Laboratories. PKCS #1 v2.2: RSA Cryptography Standard. 2012.

[16] ISO/IEC. ISO/IEC 9796-2:2010 – Information technology – Security techniques – Digital signature schemes giving message recovery – Part 2: Integer factorization based mechanisms. 2010.

[17] National Institute of Standards and Technology. FIPS PUB 186-4: Digital Signature Standard (DSS). 2013.

[18] ISO/IEC. ISO/IEC 14888-3:2006 – Information technology – Security techniques – Digital signatures with appendix – Part 3: Discrete logarithm based mechanisms. 2006.

[19] M. Lochter and J. Merkle. Elliptic Curve Cryptography (ECC) Brainpool Standard Curves and Curve Generation. 2010.

[20] National Institute of Standards and Technology. FIPS PUB 180-4: Secure Hash Standard (SHS). 2012.

[21] ISO/IEC. ISO/IEC 10118-3:2004 – Information technology – Security techniques – Hash-functions – Part 3: Dedicated hash-functions. 2004.

C. Excerpts from the Criteria

For the meaning of the assurance components and levels the following references to the Common Criteria can be followed:

- On conformance claim definitions and descriptions refer to CC part 1 chapter 10.5
- On the concept of assurance classes, families and components refer to CC Part 3 chapter 7.1
- On the concept and definition of pre-defined assurance packages (EAL) refer to CC Part 3 chapters 7.2 and 8
- On the assurance class ASE for Security Target evaluation refer to CC Part 3 chapter 12
- On the detailled definitions of the assurance components for the TOE evaluation refer to CC Part 3 chapters 13 to 17
- The table in CC part 3 , Annex E summarizes the relationship between the evaluation assurance levels (EAL) and the assurance classes, families and components.

The CC are published at https://www.commoncriteriaportal.org/cc/

D. Annexes

List of annexes of this certification report

Annex A: Security Target provided within a separate document.

Annex B: Evaluation results regarding development
and production environment

Annex B of Certification Report BSI-DSZ-CC-1112-V2-2021

Evaluation results regarding development and production environment

The IT product CardOS DI V5.4 QES Version 1.0 (Target of Evaluation, TOE) has been evaluated at an approved evaluation facility using the Common Methodology for IT Security Evaluation (CEM), Version 3.1 extended by Scheme Interpretations and by advice of the Certification Body for components beyond EAL 5 and CC Supporting Documents for conformance to the Common Criteria for IT Security Evaluation (CC), Version 3.1.

As a result of the TOE certification, dated 29 September 2021, the following results regarding the development and production environment apply. The Common Criteria assurance requirements ALC – Life cycle support (i.e. ALC_CMC.4, ALC_CMS.4, ALC_DEL.1, ALC_DVS.2, ALC_LCD.1, ALC_TAT.1)

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

a) Atos Information Technology GmbH, Otto-Hahn-Ring 6, 81739 Munich, Germany (SW Development)

b) Atos Information Technology GmbH, Wuerzburger Str. 121, 90766 Fuerth, Germany (SW Development)

c) Atos IT Solutions and Services d.o.o, Matice Hrvatske 15, 21000 Split, Croatia (SW Development)

d) See [9] for the development and production sites of the hardware platform.

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

Note: End of Report