Federal Office
for Information Security

Certification Report

BSI-DSZ-CC-0869-V2-2019

for

Java Card Platform Implementation for Infineon on M7892 G12 (SLJ 52GxxyyyzC) V2.0

from

Oracle Corporation

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-0869-V2-2019(*)

Java Card Platform Implementation for Infineon on M7892 G12 (SLJ 52GxxyyyzC) V2.0

from Oracle Corporation

PP Conformance:	Java Card Protection Profile - Open Configuration, Version 3.0, May 2012, ANSSI-CC-PP-2010/03-M01
Functionality:	PP conformant including optional package EMG plus product specific extensions Common Criteria Part 2 extended
Assurance:	Common Criteria Part 3 conformant EAL 5 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, by advice of the Certification Body for components beyond EAL 5 and CC Supporting Documents as listed in the Certification Report for conformance to the Common Criteria for IT Security Evaluation (CC), Version 3.1. CC and CEM are also published as ISO/IEC 15408 and ISO/IEC 18045.

(*) This certificate applies only to the specific version and release of the product in its evaluated configuration and in conjunction with the complete Certification Report and Notification. For details on the validity see Certification Report part A chapter 4

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

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

Common Criteria
Recognition Arrangement
recognition for components
up to EAL 2

Bonn, 13 June 2019
For the Federal Office for Information Security

Bernd Kowalski
Head of Division

L.S.

Deutsche
Akkreditierungsstelle
D-ZE-19615-01-00

This page is intentionally left blank.

Contents

A. Certification

1. Preliminary Remarks

Under the BSIG1 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]
- Common Criteria for IT Security Evaluation (CC), Version 3.1[4] [1] also published as ISO/IEC 15408.

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

- 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 Domain 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.sogisportal.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.

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

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 Java Card Platform Implementation for Infineon on M7892 G12 (SLJ 52GxxyyyzC) V2.0 has undergone the certification procedure at BSI. This is a re-certification based on BSI-DSZ-CC-0869-2015. Specific results from the evaluation process BSI-DSZ-CC-0869-2015 were re-used.

The evaluation of the product Java Card Platform Implementation for Infineon on M7892 G12 (SLJ 52GxxyyyzC) V2.0 was conducted by TÜV Informationstechnik GmbH. The evaluation was completed on 28 May 2019. TÜV Informationstechnik GmbH is an evaluation facility (ITSEF)[5] recognised by the certification body of BSI.

For this certification procedure the applicant is: Oracle Corporation.

The product was developed by: Oracle Corporation.

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 13 June 2019 is valid until 12 June 2024. Validity can be re-newed by re-certification.

The owner of the certificate is obliged:

1. when advertising the certificate or the fact of the product's certification, to refer to the Certification Report as well as to provide the Certification Report, the Security

[5] Information Technology Security Evaluation Facility

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 Java Card Platform Implementation for Infineon on M7892 G12 (SLJ 52GxxyyyzC) V2.0 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] Oracle Corporation
500 Oracle Parkway
Redwood Shores
California 94065
U.S.A

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) Java Card Platform Implementation for Infineon on M7892 G12 (SLJ 52GxxyyyzC) V2.0 is a smart card with a Java Card operating system on the Infineon IC M7892 G12, certified under BSI-DSZ-CC-0891-V3-2018 [19]. It is a Java Card Platform in open configuration compliant with the Java Card Specification (Classic Edition) Version 3.0.1 and the GlobalPlatform Specification Version 2.2.

The TOE allows post-issuance downloading of applications that have been previously verified by an off-card trusted IT component. It constitutes a secure generic platform that supports multi-application runtime environment and provides facilities for secure loading and interoperability between different applications. The Java Card Platform is managed by the Card Manager that is a part of the TOE. The Java Card Platform is fully compliant with the Java Card Specification Version 3.0.1 excluding the optional part JCRMI which is not implemented by the TOE. No specific pre-issuance applets are in the scope of the TOE, but pre-issuance loading of applets is possible. Native code post-issuance downloading is out of scope.

The Security Target [6] is the basis for this certification. The TOE fulfills the requirements of the Common Criteria Java Card Protection Profile - Open Configuration, Version 3.0, May 2012, ANSSI-CC-PP-2010/03-M01 [8] and claims strict conformance to it. The TOE provides the ability to extend the Java Card and Global Platform functionality by offering an extensible user code area (Sandbox) that can be populated with custom code and be reachable from post-issuance Java applets via a secure, controlled mechanism. To address this, the EMG functional package of the Java Card Protection Profile [8] is used for the TOE. As JCRMI is not implemented the Remote Method Invocation (RMIG) functional package as defined in the PP is not used for the TOE.

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 5 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] and [7], chapter 6.1. 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**
Global Platform TOE Security Functionality	
SF.Card Manager	In Open Mode configuration, the Card Manager is activated and is responsible for card administration. The goal of the Card Manager is to enforce the security policies of the Card Issuer on the card by providing the following features: Card Content Management (CCM), DAP Verification, Card Management Environment, APDU Commands Dispatcher, SSD Delegated Management, Life-Cycle Management, Logical Channel Management.
SF.Secure Channels	This TOE Security Functionality provides a secure mean for the IC Manufacturer/Composite Product Integrator/Card Issuer to perform card

	management. This TSF protects the sensitive assets exchanged during that process. It relies on the Secure Channel Protocols defined in GlobalPlatform specification. This is achieved by the following features: Mutual Authentication, Message Integrity Verification, Message Confidentiality, Secure Messaging acceleration.
SF.Secure Channel Key Management	This TOE Security Functionality is intended to securely manage the keys used to establish a secure channel. These are the session keys used to open a secure channel with the CAD and the ISD keys used to open a secure channel with the IC Manufacturer/Composite Product Integrator/Card Issuer. This is achieved by Session Key/ISD Key Generation.
SF.Global PIN Management	This TOE Security Functionality controls the update of the security attributes associated with the global CVM which is restricted to the applets installed with the CVM Privilege.
Java Card TOE Security Functionality	
SF.Java Card Firewall	The Java Card firewall provides protection against the most frequently anticipated security concern: developer mistakes and design oversights that might allow sensitive data to be “leaked” to another applet. However, if the object is owned by an applet protected by its own firewall, the requesting applet must satisfy certain access rules before it can use the reference to access the object. These set of access rules controls the sharing and separation of resources between applet instantiations. The firewall also provides protection against incorrect code. If incorrect code is loaded onto a card, the firewall still protects objects from being accessed by this code.
SF.End User Authentication	This TOE Security Functionality allows applet’s user identification and authentication using the following features: PIN comparison feature.
SF.Sensitive Data Cleaner	This TOE Security Functionality ensures that sensitive information contained in data containers (APDU buffer, cryptographic buffer, local variables, bArray, static fields, class instances fields, etc.) are cleared after usage upon sensitive operations (deletion of packages/applets/objects, cryptographic operations, APDU commands, etc.).
SF.Atomic_Transactions	This TOE Security Functionality ensures the atomicity of transactions. It manages the contents of persistent storage after a stop, failure, or fatal exception during an update of a single object field or single class field or single array component. An applet might need to atomically update several different fields or array components in several different objects. Either all updates take place correctly and consistently, or else all fields or components are restored to their previous values.
SF.Security Violation	This TOE Security Functionality detects an attempt to illegally access an object belonging to another applet across the firewall boundary, on violation of fundamental language restrictions, such as attempting to invoke a private method in another class, on unavailability of data upon allocation.
SF.PIN integrity	This TOE Security Functionality ensures that the PIN value is protected in integrity. The integrity value is checked as well as its persistent attributes before any operation made on the PIN value.
SF.Key Management	This TOE Security Functionality ensures a secure on-card cryptographic keys infrastructure. Thus, providing the following security

	features: Keys Integrity Protection, Keys Confidentiality Protection, Keys Secure Generation, Keys Secure Deletion, Keys Secure Distribution, Keys Secure Agreement.
SF.Cryptographic Operations	This TOE Security Functionality enforces security means to execute the following cryptographic operations: Message Digest Generation, Signature Generation & Verification, Encryption & Decryption, Unique Hash Value, ECC basic operations, MAC calculation and verification, Random Number Generation.
SF.Extended Memory	This feature provides controlled access means to the external memory and ensures that the external memory does not address Java Card System memory (containing User Data and TSF Data) and the extended JC/GP functionality does not interfere with the TOE's memory.

Table 1: TOE Security Functionalities

For more details please refer to the Security Target [6] and [7], chapter 7.1.

The following table outlines further aspects of the TOE parts and the non-TSF parts regarding their security features:

Components		TOE parts	Non-TSF parts
SCP	Micro Controller	ISO 7816 Interface ISO 14443 A/B Interface Crypto2304T (asymmetric coprocessor) SCP (AES and TDES coprocessor) TRNG	Mifare-compatible interface
	Crypto Library	RSA EC (prime and binary) Symmetric Crypto Library	Toolbox
	IC dedicated software	Firmware parts	
Embedded Software	Protocols	SCP02, SCP03	SCP01
	Cryptographic Algorithms	ECDSA (prime and binary) ECDH (prime and binary) RSA TDES AES RSA Key generation onboard EC Key generation onboard AIS20 DRG.4 (seeded from HW-TRNG) SHA-1, SHA-2 Retail MAC, CMAC	Korean SEED MD5 RIPEMD160 MACs
	Modules	LDS Supplementary Security Domains	Match-on-Card Biometric package Templating

Table 2: Security Features of the TOE

The assets to be protected by the TOE are defined in the Security Target [6] and [7], chapter 4.1. 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] and [7], chapter 4.2 to 4.4.

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:

Java Card Platform Implementation for Infineon on M7892 G12 (SLJ 52GxxyyyzC) V2.0

The TOE developer delivers his OS image for TOE production to the Chip Manufacturer. The OS image is accompanied by related guidance documents and further tools for conducting configuration and templating with the TOE. After TOE production by the Chip Manufacturer and the Composite Product Integrator the TOE delivery takes place at the end of phase 5 of the TOE's life-cycle model as outlined in the ST, chapter 1.6. The delivery is performed by the Composite Product Integrator to the Card Issuer for personalization, issuance and the operational use thereafter. The following items are delivered to the Card Issuer:

No	Type	Identifier	Release	Form of Delivery
1	HW/SW	IC including the software part of the TOE: Java Card Platform Implementation for Infineon on M7892 G12 (SLJ 52GxxyyyzC) V2.0 [7]	Infineon M7892 G12 with Java Card Platform Implementation Version 2.0	Delivery as defined by certified IFX procedures [19]
2	DOC	Operational user guidance [11]	V2.15	
3	DOC	Data Book [12]	V2.0	

[7] The TOE in its final TOE configuration as shown in detail in the Security Target, ready for personalization:
The first x is for the available interface (can be 'C', 'L', or 'D' for the contact-based, contactless or dual interface).
The second x is for the available cryptography (can be 'A' for symmetric and asymmetric cryptography, and 'B' for only symmetric cryptography).
The number yyy is the available user memory (can be one of the following sizes: 036, 064, 080, 128, 144, 160 kB).
The last letter z is a place holder for products that will be based on the TOE (can be 'A' for ePassport, 'B' for eDriving License, 'C' for National eID Open Platform, or 'D' for National eID with applications).

No	Type	Identifier	Release	Form of Delivery
4	KEY DATA	Card Manager Keyset (Transfer keyset for embedding)	-	
5	KEY DATA	DAP Verification Authority's public key	-	

Table 3: Deliverables of the TOE

At the time of TOE delivery, all provided configuration options of the TOE and its hardware are set and cannot be further modified. The TOE can be clearly identified and its configuration can be determined as described in the following.

In order to verify that the user uses a certified TOE and certified configuration, the TOE can be identified using the means described in the Operational User Guidance [11], chapter 1.4. The TOE can be identified using the command GET DATA. It retrieves the chip and configuration data from the card. The configuration data is retrieved using GET DATA tags 0xDF10 and 0xDF11 as specified in [12], chapter 5.8. All listed items below must have the following expected value(s) after TOE delivery:

Offset	Length	Description	Expected Value
Tag 'DF10'			
66	2 bytes	Build information (major / minor version)	'0x0020'
69	1 byte	Security profile CC compliant	'C3'
88	1 byte	Dynamic reconfiguration disabled	'E1'
89	1 byte	Templating disabled	'E1'
90	1 byte	Auth. for proprietary commands by GP SCP	'D2'
91	1 byte	Reflashing disabled	'E1'
194	1 byte	If Dynamic reconfiguration disabled through dynamic configuration	'E1'
195	1 byte	If Templating disabled through dynamic configuration	'E1'
Tag 'DF11'			
32	1 byte	GP Secure Channel Protocol of ISD	'02' or '03'
33	1 byte	GP SCP implementation option of ISD - in case of SCP02 - in case of SCP03	 '15', '55', '1A' '00' or '10'
131	1 byte	ISD supports GP command format	'E1'
132	1 byte	GP configuration (GP ID or general GP)	'E1' or 'D2'

Table 4: TOE Identification Data

Further, the TOE offers a range of different configurations concerning the optional modules. A user can verify which modules are actually part of the TOE configuration and which of them are part of the TSF. Modules that are not part of the TSF do not lead to an uncertified configuration, but the use of them is not covered by this certification. Hence, the provided functionality of non-TSF modules cannot be used as certified basis for forthcoming applet evaluations.

The configuration parameters returned by the GET DATA command with tags 0xDF10 and 0xDF11 are defined in the following table (excerpt from [11], Annex B). The evaluation covers the options set in **bold text**.

Parameter	Length (in byte)	Description and Valid Options
jCOS runtime mode	1	**0xE1 - release mode** 0xD2 - debug mode
Security profile	1	**0xC3 - CC EAL5+ mode**
Maximum security violations	1	This item represents the maximum number of faults, potential security violation faults, which are tolerated before the card is put into CARD_MUTE state. Valid values are 0 through 10. The default is 3.
Enabled modules	2	16-bit mask of enabled modules: **0x0001 - EC** **0x0002 - RSA** 0x0004 - USA **0x0008 - CL (Contactless)** 0x0010 - Legacy (Korean SEED, RIPEMD, SCP01, and MD5) **0x0020 - CB (Contact Based)** **0x0040 - Advanced SSD (SCP03 and Downloadable SSD)** 0x0080 - MC (Memory Card) 0x0100 - SAND (Biometry/Regional Cryptography) **0x0200 - EXT_GP (Advanced GP)** **0x0400 - LDS Secure Messaging Accelerator (EPASSPORT)** 0x0800 – Templating **0x1000 – RSA KEYGEN** Note: unused bits 13-15 are set to 1 in the module mask
CLA encoding	1	**0xE1=JC3.0.1** 0xD2=JC2.2.1
Enable dynamic reconfiguration	1	**0xE1 - dynamic reconfiguration disabled** 0xD2 - dynamic reconfiguration enabled
Enable templating	1	**0xE1 - templating disabled** 0xD2 - load and dump enabled 0xC3 - only load enabled
Authentication for proprietary APDU commands	1	0xE1 - no secure messaging, password required **0xD2 - use configured secure messaging**
Enable flashloading	1	**0xE1 - flashloading disabled** 0xD2 - flashloading enabled

Table 5: TOE Configuration Data

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: The Security Policy of the TOE as a smart card with a Java Card operating system (OS) is to provide basic security functionalities to be used by the smart card applications thus providing an overall smart card system security.

The TOE implements physical and logical security functionality in order to protect user 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 crypto routines, 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 [6] and [7], chapter 6.1.

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.

Concerning the overall security of the TOE, constraints are imposed upon the user by the different guidance documents ([11] to[18]). Advices that are presented in the guidance have to be followed.

In particular, the security objectives for the environment have to be followed and considered. They are as follows:

- OE.APPLET: No applet loaded post-issuance shall contain native methods.
- OE.VERIFICATION: All the bytecodes shall be verified at least once, before the loading, before the installation or before the execution, depending on the card capabilities, in order to ensure that each bytecode is valid at execution time. See #.VERIFICATION in [6] and [7], chapter 3.4 for details. Additionally, the applet shall follow all the recommendations, if any, mandated in the platform guidance for maintaining the isolation property of the platform.

  Application Note: Constraints to maintain the isolation property of the platform are provided by the platform developer in application development guidance. The constraints apply to all application code loaded in the platform.
- OE.CODE-EVIDENCE: For application code loaded pre-issuance, evaluated technical measures implemented by the TOE or audited organizational measures must ensure that loaded application has not been changed since the code verifications required in OE.VERIFICATION.

  For application code loaded post-issuance and verified off-card according to the requirements of OE.VERIFICATION, the verification authority shall provide digital evidence to the TOE that the application code has not been modified after the code verification and that he is the actor who performed code verification.

  For application code loaded post-issuance and partially or entirely verified on-card, technical measures must ensure that the verification required in OE.VERIFICATION are performed. On-card bytecode verifier is out of the scope of this Protection Profile.

Application Note: For application code loaded post-issuance and verified off-card, the integrity and authenticity evidence can be achieved by electronic signature of the application code, after code verification, by the actor who performed verification.

Details can be found in the Security Target [6] and [7], chapter 5.2.

5. Architectural Information

The TOE design is defined by certain subsystems and modules. The subsystems again are logically grouped together and compose four layers of the TOE:

GlobalPlatform Layer (GP): The GlobalPlatform Layer relies on both the Java Card Platform Layer and the Operating System Layer. This layer implements the GlobalPlatform industry standard, which defines the infrastructure for development, deployment and management of smart cards. Security domains and secure channel protocols are supported in this layer.

Java Card Platform Layer (JC): The Java Card Platform Layer relies on the Operating System Layer. The Java Card Platform Layer complies with the specifications for the Java Card Platform, Version 3.0.1, Classic Edition, excluding the optional functionality for remote method invocation. This layer provides the security inherent in the Java programming language.

Operating System Layer (OS): The Operating System Layer relies on the Hardware Abstraction Layer. The OS Layer provides a memory manager, cryptography engine and input/output.

Hardware Abstraction Layer (HAL): The Hardware Abstraction Layer interacts directly with the hardware. The HAL implements CPU control, card initialization, memory operations, interruption control, and support for cryptography on the chip.

The subsystems that compose the TOE and provide its functionality are each mapped to one layer.

6. Documentation

The evaluated documentation as outlined in Table 3 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

For testing, the TOE was prepared by following the guidance documentation and using the Configurator and Templating tools. Thereby a wide range of TOE configurations was created and tested. Since the TOE provides manifold possible TOE configurations, not all of them could be tested. However, each module whether part of the TSF or not was tested appropriately. The TOE configurations did not show unexpected behavior related to their different configuration options. All behavior of different TOE configurations during testing were as expected and according to their desired configured behavior. The following sections give more detail on the TOE configurations used during testing.

Developer's Test according to ATE_FUN:

The tested configurations compose a good subset of possible TOE configurations and were chosen to cover all the functional developer tests. Additional and different configurations were tested in the course of independent testing, which show that the several configuration options have no unexpected impact on the test results.

Testing Approach: For functional testing, the developer used several test categories to cover the TOE security functionality the TOE provides. The following test categories are described in the test documentation and were found in the actual test environment:

- TCK tests: The tests in the Java Card Technology Compatibility Kit are used to verify the standard Java Card API packages, JCRE behavior and JCVM tests.
- Generic tests: The generic tests cover product requirements dealing with public specifications such as Global Platform or Java Card platform specification using API and APDU interface. Generic tests include cryptographic algorithm tests, communication protocol tests (T1 and T0) and further JCRE features such as logical channels and garbage collection.
- Secure tests: The tests referred to as Secure Tests cover security functionality involving IFX specific API and IC, GP ID configuration tests and other topics such as CVM or Sandbox feature.
- Collis tests: Some functionality related to compliance to GlobalPlatform Card Specification Version 2.2 is tested using the GP Version 2.2 UICC configuration test suite from Collis.

The tests mainly run automatically and perform all test steps including installation of test applets, test scripting, checking of results and clean-up procedures.

ATE_COV and ATE_DPT were taken into account and all mappings to interfaces and modules of the TOE are covered by the tests.

The testing approach covers all TSFI as described in the functional specification and all subsystems of the TOE design adequately. A subset of possible TOE configurations as described in the ST is covered by the approach of testing. Further configurations are tested by the evaluator during independent testing. No unexpected deviations in test results for different configurations were found. 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: (i) Examination of developer’s testing amount, depth and coverage analysis and of the developer’s test goals and plan for identification of gaps; (ii) Examination whether the TOE in its intended environment, is operating as specified using iterations of developer’s tests; (iii) Independent testing was performed at the Evaluation Body with the TOE developer test environment and additional Evaluation Body test equipment using tests applets, test scripts, simulation tools.

TOE test configurations: Tests were performed with different TOE configurations, i.e. with different optional modules activated and with different TOE interfaces (contactless, contact-based) as well as with the TOE simulator. The TOEs were generated using the Configurator Tool and the according guidance documents. Tests were done in different life-cycle phases (e.g. Global Platform life-cycle states SECURED, OP_READY, etc.). Tests were performed with TOEs that were generated with or without using Templating functionality and the Templating tools.

Subset size chosen: During sample testing the evaluator chose to sample the developer functional tests at the Evaluation Body. Most of the tests were repeated in order to yield good test coverage of the TOE functionality. During independent testing the evaluator used test applets and test scripts to invoke and test functionality given by the API and APDU interface. Further penetration testing was done for AVA_VAN aspects. This includes the penetration with laser fault injection attacks, side-channel attacks on cryptographic functions and simulated memory manipulation.

Interfaces tested: The selection criteria for the interfaces of the composed subset consider simply the security functionality that is available from these interfaces. Focus was laid upon interfaces and functionality that are in particular security sensitive for a Java Card platform, such as firewall mechanisms, atomic transactions, PIN mechanisms or key handling. The tested subset comprises the APDU and the API interfaces available to users. While the physical IC interface relies on the platform certification, the independent testing focused on the APDU interface (based on the Global Platform specification) and the API interface (which provides packages from Java Card API, Global Platform API and proprietary API).

During the evaluator's TSF subset testing the TOE operated as specified. No unexpected behavior was observed, particularly related to different TOE configurations and generation of the TOE using the Configurator and Templating tools.

Penetration Testing according to AVA_VAN:

The TOE in different configurations being intended to be covered by the current evaluation was tested.

Penetration testing approach: Based on the list of potential vulnerabilities applicable to the TOE in its operational environment the evaluators devised the attack scenarios for penetration tests when they were of the opinion, that those potential vulnerabilities could be exploited in the TOE's operational environment. The aspects of the security architecture were considered for penetration testing as well as all other evaluation evidence. 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 also supported the testing activity by enabling the evaluator to verify implementation aspects that could hardly be covered by test cases.

In addition the evaluator applied tests and performed code reviews during the composite evaluation aspects to verify the implementation of the requirements imposed by the ETR and the guidance of the underlying platform. This ensured confidence in the security of the TOE as a whole.

TOE test configurations: The evaluators used TOE samples for testing that were configured according to the ST. The configurations that were created for testing constitute a reasonable subset of possible configurations that are possible according to the modularization concept as defined in the ST. The tests were performed in different test scenarios: (i) TOE smart cards tested using specialized test tools for smart cards, Java cards, for LFI testing and analysis tools; (ii) A simulator was used for test cases, which were not possible to be performed with a real smart card TOE, e.g. memory manipulation; (iii) Different life-cycles as well as life-cycle management were tested.

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 provided that all measures required by the developer are applied.

8. Evaluated Configuration

The TOE offers a range of TOE configurations that are defined by the available optional modules and the functionality they provide. The underlying hardware platform may also vary and provides different options by its available interface (contactless, contact-based or dual), its memory sizes and co-processors. Each of them is valid for the composite TOE and is covered by the underlying hardware certification BSI-DSZ-CC-0891-V3-2018. The evaluated TOE configurations meet the definitions that are given by the TOE identification data as described above. The optional non-TSF modules were considered as part of the TOE configuration and do not introduce new vulnerabilities to circumvent the TSF. During production, the TOE configurations are set by using the so-called Configurator Tool which is delivered to the Chip Manufacturer accompanied by the according guidance documentation.

9. Results of the Evaluation

9.1. CC specific results

The Evaluation Technical Report (ETR) [9] 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 and guidance specific for the technology of the product [4] (AIS 34).

The TOE was subject to a composite evaluation according to AIS 36 [4]. The platform certificate for the Integrated Circuit (IC) Infineon Security Controller M7892 Design Steps D11 and G12 with its related crypto libraries, certification ID BSI-DSZ-CC-0891-V3-2018, was used ([19] to [25]).

The following guidance specific for the technology was used:

(i) Composite product evaluation for Smart Cards and similar devices according to AIS 36 (see [4]). On base of this concept the relevant guidance documents of the underlying IC platform (refer to the guidance documents [22] to [25]) and the document ETR for composite evaluation from the IC's evaluation ([21]) have been applied in the TOE evaluation.

(ii) Guidance for Smartcard Evaluation (AIS 37, see [4]).

(iii) Application of Attack Potential to Smartcards (AIS 26, see [4]).

(iv) The application of CC to integrated circuits (AIS 25, see [4]).

(v) Functionality classes and evaluation methodology of physical and deterministic random number generators (AIS 20 and AIS 31, see [4]).

(vi) Informationen zur Evaluierung von kryptographischen Algorithmen (AIS 46, see [4]).

For smart card specific methodology the scheme interpretations AIS 25, AIS 26, AIS 36, AIS 37 and AIS 46 (see [4]) were used. For RNG assessment the scheme interpretations AIS 20 and AIS 31 were used (see [4]).

To support composite evaluations according to AIS 36 (see [4]) the document ETR for composite evaluation [18] was provided and approved. This document provides details of this Java Card platform evaluation that have to be considered in the course of a composite evaluation on top.

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

- All components of the EAL 5 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-0869-2015, re-use of specific evaluation tasks was possible. The focus of this re-evaluation was on the adoption of the operating system (due to the change of the underlying HW platform and its related crypto libraries) and on the maintenance of the TOE implementation regarding functional and security aspects.

The evaluation has confirmed:

- PP Conformance: Java Card Protection Profile - Open Configuration, Version 3.0, May 2012, ANSSI-CC-PP-2010/03-M01 [8]
- for the Functionality: PP conformant including optional package EMG plus product specific extensions
  Common Criteria Part 2 extended
- for the Assurance: Common Criteria Part 3 conformant
  EAL 5 augmented by ALC_DVS.2 and AVA_VAN.5

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

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

9.2. Results of cryptographic assessment

For an overview and details of the cryptographic functionalities that are implemented by the TOE to enforce its security policy please refer to the two tables in the Annex ‘Crypto Disclaimer’ of the Security Target [7].

The first table in the ‘Crypto Disclaimer’ outlines the Purpose, the Cryptographic Mechanism, the Standard of Implementation, the Key Size in bits, the Standard of Application where its specific appropriateness is stated as well as related document references. An explicit validity period is not given here.

The second table in the ‘Crypto Disclaimer’ outlines the Purpose, the Cryptographic Mechanism, the Standard of Implementation, the Key Size in bits, the Security Level (rating from cryptographic point of view) as well as related document references. Any cryptographic functionality that is marked in column 'Security Level above 100 Bits' in the table with '*no*' achieves a security level of lower than 100 Bits (in general context) only.

The strength of the cryptographic algorithms was not rated in the course of this certification procedure (see BSIG Section 9, Para. 4, Clause 2). But cryptographic functionalities with a security level of lower than 100 bits can no longer be regarded as secure without considering the application context. Therefore, for these functionalities it shall be checked whether the related crypto operations are appropriate for the intended system. Some further hints and guidelines can be derived from the “Technische Richtlinie BSI TR-02102-1” (https://www.bsi.bund.de) [30].

The TOE’s cryptographic functionalities outlined in the Annex ‘Crypto Disclaimer’ of the Security Target [7] are implemented in the TOE’s operating system making use of the crypto libraries belonging to the underlying HW platform except for the SHA implementation. Hereby, the TOE relies on the correct and secure implementation of the cryptographic functionalities provided by the crypto libraries of the underlying HW platform. Deviations within the implementation of the cryptographic functionalities from the referenced standards are outlined in the Security Target [7], chapter 6.1 or in the tables of the ‘Crypto Disclaimer’ respectively, and are covered via specific guidance requirements in [11], where applicable.

10. Obligations and Notes for the Usage of the TOE

The documents as outlined in Table 3 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.

Some security measures are partly implemented in this certified TOE, but require additional configuration or control or measures to be implemented by a product layer on top using the TOE. For this reason the TOE includes guidance documentation (see Table 3) which contains obligations and guidelines for the developer of the product layer on top on how to securely use this certified TOE and which measures have to be implemented in order to fulfil the security requirements of the Security Target of the TOE. In the course of the evaluation of the composite product or system it must be examined if the required measures have been correctly and effectively implemented by the product layer on top. Additionally, the evaluation of the composite product or system must also consider the evaluation results as outlined in the document "ETR for composite evaluation" [18].

At the point in time when evaluation and certification results are reused there might be an update of the document "ETR for composite evaluation" available. Therefore, the certified products list on the BSI website has to be checked for latest information on reassessments, recertifications or maintenance result available for the product.

Since the TOE provides a variety of possible configurations, it must be stated that there are configuration options that are not part of the TSF. Their use is not covered by the certification. That is for example, a security domain may offer the deprecated SCP01 module, but must be aware that authentication and subsequent actions like content management cannot be covered any longer by the certification.

The constraints and exceptions on the usage of the TOE as pointed out above have to be followed.

Additionally, the requirements provided for TOE users/administrators in the guidance documentation [11] to [18] have to be considered. They include mandatory information on the secure usage of the TOE functionality.

11. Security Target

For the purpose of publishing, the Security Target [7] of the Target of Evaluation (TOE) is provided within a separate document as Annex A of this report. It is a sanitised version of the complete Security Target [6] used for the evaluation performed. Sanitisation was performed according to the rules as outlined in the relevant CCRA policy (see AIS 35 [4]).

12. Definitions

12.1. Acronyms

AES	Advanced Encryption Standard
AIS	Application Notes and Interpretations of the Scheme
API	Application Programming Interface
BSI	Bundesamt für Sicherheit in der Informationstechnik / Federal Office for Information Security, Bonn, Germany
BSIG	BSI-Gesetz / Act on the Federal Office for Information Security
CCRA	Common Criteria Recognition Arrangement
CC	Common Criteria for IT Security Evaluation
CEM	Common Methodology for Information Technology Security Evaluation
cPP	Collaborative Protection Profile
DAP	Data Authentication Pattern
DRNG	Deterministic Random Number Generator
EAL	Evaluation Assurance Level
EC	Elliptic Curve
ECDH	Elliptic Curve Diffie-Hellman
ECDSA	Elliptic Curve Digital Signature Algorithm
EMG	External Memory Group
ETR	Evaluation Technical Report
GP	Global Platform
IFX	Acronym for Infineon
IT	Information Technology
ITSEF	Information Technology Security Evaluation Facility
JC	Java Card
JCP	Java Card Platform
JCRE	Java Card Runtime Environment

JCRMI	Java Card Remote Method Invocation
JCS	Java Card System
JCVM	Java Card Virtual Machine
LDS	Logical Data Store
MAC	Message Authentication Code
PP	Protection Profile
RNG	Random Number Generator
RSA	Rivest, Shamir and Adleman Algorithm
SAR	Security Assurance Requirement
SCP	Smart Card Platform / Secure Channel Protocol
SFP	Security Function Policy
SFR	Security Functional Requirement
SHA	Secure Hash Algorithm
ST	Security Target
TCK	Technology Compatibility Kit, a test suite provided by the developer as part of ATE_FUN
TDES	Triple Data Encryption Standard
TOE	Target of Evaluation
TRNG	True Random Number Generator
TSF	TOE Security Functionality

12.2. Glossary

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

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

Deterministic random number generator (DRNG) - An RNG that produces random numbers by applying a deterministic algorithm to a randomly selected seed and, possibly, on additional external inputs.

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.

Random number generator (RNG) - A group of components or an algorithm that outputs sequences of discrete values (usually represented as bit strings).

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.

True random number generator (TRNG) - A device or mechanism for which the output values depend on some unpredictable source (noise source, entropy source) that produces entropy.

13. Bibliography

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

[2] Common Methodology for Information Technology Security Evaluation (CEM), Evaluation Methodology, Version 3.1, Revision 4, September 2012
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[8], 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 for BSI-DSZ-CC-0869-V2-2019: Security Target for Java Card Platform Implementation for Infineon on M7892 G12 (SLJ 52GxxyyyzC) V2.0, Version 3.6, 22 May 2019, Oracle Corporation (confidential document)

[7] Security Target Lite for BSI-DSZ-CC-0869-V2-2019: Security Target Lite for Java Card Platform Implementation for Infineon on M7892 G12 (SLJ 52GxxyyyzC) V2.0, Version 3.6, 24 May 2019, Oracle Corporation (sanitised version)

[8] specifically

- AIS 1, Version 14, Durchführung der Ortsbesichtigung in der Entwicklungsumgebung des Herstellers
- 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 9, 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 35, Version 2, Öffentliche Fassung des Security Targets (ST-Lite) including JIL Document and CC Supporting Document and CCRA policies
- AIS 36, Version 5, Kompositionsevaluierung including JIL Document and CC Supporting Document
- 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

[8] Common Criteria Java Card Protection Profile - Open Configuration, Version 3.0, May 2012, ANSSI-CC-PP-2010/03-M01

[9] Evaluation Technical Report Summary (ETR Summary) for BSI-DSZ-CC-0869-V2-2019: ETR for Java Card Platform Implementation for Infineon on M7892 G12 (SLJ 52GxxyyyzC) V2.0, Version 4, 27 May 2019, TÜV Informationstechnik GmbH (confidential document)

[10] Configuration List for BSI-DSZ-CC-0869-V2-2019: Configuration Management Scope for Java Card Platform Implementation for Infineon on M7892 G12 (SLJ 52GxxyyyzC) V2.0, Version 2.6, 24 May 2019, Oracle Corporation (confidential document)

[11] AGD_OPE for Java Card Platform Implementation for Infineon on M7892 G12 (SLJ 52GxxyyyzC) V2.0, Version 2.15, May 2019, Oracle Corporation

[12] Java Card Platform Implementation for Infineon on SLE 78 (SLJ 52GxxyyyzC), Data Book, Version 2.0, Oracle Corporation

[13] AGD_PRE Composite Product Integrator for Java Card Platform Implementation for Infineon on M7892 G12 (SLJ 52GxxyyyzC) V2.0, Version 2.6, December 2018, Oracle Corporation

[14] AGD_PRE Chip Manufacturer for Java Card Platform Implementation for Infineon on M7892 G12 (SLJ 52GxxyyyzC) V2.0, Version 2.6, December 2018, Oracle Corporation

[15] Java Card Platform Implementation for Infineon on SLE 78 (SLJ 52GxxyyyzC), Configuration Guide, Version 2.0, February 2018, Oracle Corporation

[16] Java Card Platform Implementation for Infineon on SLE 78 (SLJ 52GxxyyyzC), Configurator Tool Guide, Version 2.0, February 2018, Oracle Corporation

[17] Java Card Platform Implementation for Infineon on SLE 78 (SLJ 52GxxyyyzR), Tools Programming Guide, Version 2.0, March 2016, Oracle Corporation

[18] Evaluation Technical Report for Composite Evaluation (ETR Comp) according to AIS 36 for BSI-DSZ-CC-0869-V2-2019: ETR for Composition for Java Card Platform Implementation for Infineon on M7892 G12 (SLJ 52GxxyyyzC) V2.0, Version 4, 27 May 2019, TÜV Informationstechnik GmbH (confidential document)

[19] Certification Report BSI-DSZ-CC-0891-V3-2018 for Infineon Security Controller M7892 Design Steps D11 and G12 with specific IC dedicated firmware and optional software, 9 January 2018, Bundesamt für Sicherheit in der Informationstechnik (BSI)

[20] Security Target Lite for BSI-DSZ-CC-0891-V3-2018: Security Target Lite for Infineon Security Controller M7892 Design Steps D11 and G12 with specific IC dedicated firmware and optional software, Revision 1.2, 21 November 2017, Infineon Technologies AG

[21] Evaluation Technical Report for Composite Evaluation (ETR Comp) according to AIS 36 for BSI-DSZ-CC-0891-V3-2018: ETR for Composition for Infineon Security Controller M7892 Design Steps D11 and G12 with specific IC dedicated firmware and optional software, Version 1, 29 November 2017, TÜV Informationstechnik GmbH (confidential document)

[22] SLx 70 Family Production and Personalization User’s Manual, 1 April 2015, Infineon Technologies AG

[23] M7892 Security Guidelines, Revision 4.0, 28 June 2017, Infineon Technologies AG

[24] SCL78 Symmetric Crypto Library for SCPv3 DES / AES, Version 2.02.010, 14 October 2016, Infineon Technologies AG

[25] CL70 Asymmetric Crypto Library for Crypto@2304T RSA / ECC / Toolbox User Interface (2.07.003), 15 May 2017, Infineon Technologies AG

[26] Java Card Platform, Version 3.0.1 (May 2009), Classic Edition, Application Programming Interface, May 2009, published by Oracle Corporation

Java Card Platform, Version 3.0.1 (May 2009), Classic Edition, Runtime Environment (Java Card RE) Specification, May 2009, published by Oracle Corporation

Java Card Platform, Version 3.0.1 (May 2009), Classic Edition, Virtual Machine (Java Card VM) Specification, May 2009, published by Oracle Corporation

[27] GlobalPlatform Card Specification, Version 2.2, March 2006

[28] Confidential Card Content management – GlobalPlatform Card Specification Version 2.2 – Amendment A, Version 1.0.1, January 2011

[29] GlobalPlatform Card ID Configuration, Version 1.0, December 2011, Document Reference: GPC_GUI_039

[30] Technische Richtlinie BSI TR-02102-1, Kryptographische Verfahren: Empfehlungen und Schlüssellängen, Version 2019-01, 22 February 2019, BSI, https://ww.bsi.bund.de/TR

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 [7] provided within a separate document.
Annex B:	Evaluation results regarding development and production environment.
Annex C:	Overview and rating of cryptographic functionalities implemented in the TOE.

Annex B of Certification Report BSI-DSZ-CC-0869-V2-2019

Evaluation results regarding development and production environment

The IT product Java Card Platform Implementation for Infineon on M7892 G12 (SLJ 52GxxyyyzC) V2.0 (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, 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 13 June 2019, 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.5, ALC_DEL.1, ALC_DVS.2, ALC_LCD.1, ALC_TAT.2) are fulfilled for the development and production sites of the TOE listed below:

a) Oracle, Santa Clara (short: SCA), 4210 Network Cycle, Santa Clara California 95054, United States (Development Environment).

b) Oracle, Austin (short: ADC), 11400 N Lamar Blvd, Austin, TX 78753-2663, United States (Data Center).

c) Oracle Colorado (short: COL), 500 Eldorado Blvd, Broomfield, CO US 80021, United States (Global Security Operations Center).

d) For development and production sites regarding the underlying IC platform please refer to the certification report BSI-DSZ-CC-0891-V3-2018 [19]

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] and [7]) are fulfilled by the procedures of these sites.

Annex C of Certification Report BSI-DSZ-CC-0869-V2-2019

Overview and rating of cryptographic functionalities implemented in the TOE

For details of the cryptographic algorithms and protocols that are implemented by the TOE to enforce its security policy please refer to the tables in the Annex ‘Crypto Disclaimer’ of the Security Target [7]. These tables outline the Purpose, the Cryptographic Mechanism, the Standard of Implementation, the Key Size in bits, the Security Level and the Standard of Application respectively as well as related document references.

Note: End of report