Federal Office
for Information Security

Certification Report

BSI-DSZ-CC-1060-2020

for

de.fac2 - FIDO U2F Authenticator Applet v1.34

from

Federal Office for Information Security (BSI)

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-1060-2020 (*)

de.fac2 - FIDO U2F Authenticator Applet
v1.34

from	Federal Office for Information Security (BSI)
PP Conformance:	FIDO Universal Second Factor (U2F) Authenticator Version 3, 5 November 2018, BSI-CC-PP-0096-V3-2018
Functionality:	PP conformant plus product specific extensions Common Criteria Part 2 extended
Assurance:	Common Criteria Part 3 conformant EAL 4 augmented by AVA_VAN.5

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 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 5.

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, 8 May 2020

For the Federal Office for Information Security

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

Sandro Amendola L.S.
Head of Division

Bundesamt für Sicherheit in der Informationstechnik
Godesberger Allee 185-189 - D-53175 Bonn - Postfach 20 03 63 - D-53133 Bonn
Phone +49 (0)228 99 9582-0 - Fax +49 (0)228 9582-5477 - Infoline +49 (0)228 99 9582-111

This page is intentionally left blank.

Contents

A. Certification....6

1. Preliminary Remarks....6
2. Specifications of the Certification Procedure....6
3. Recognition Agreements....7
4. Performance of Evaluation and Certification....8
5. Validity of the Certification Result....8
6. Publication....9

B. Certification Results....10

1. Executive Summary....11
2. Identification of the TOE....12
3. Security Policy....13
4. Assumptions and Clarification of Scope....13
5. Architectural Information....13
6. Documentation....14
7. IT Product Testing....14
8. Evaluated Configuration....16
9. Results of the Evaluation....16
10. Obligations and Notes for the Usage of the TOE....19
11. Security Target....19
12. Regulation specific aspects (eIDAS, QES)....19
13. Definitions....19
14. Bibliography....20

C. Excerpts from the Criteria....23

D. Annexes....24

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 3 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 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.

This certificate is recognized according to the rules of CCRA-2014, i. e. up to and including CC part 3 EAL 2 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 de.fac2 - FIDO U2F Authenticator Applet, v1.34 has undergone the certification procedure at BSI.

The evaluation of the product de.fac2 - FIDO U2F Authenticator Applet, v1.34 was conducted by TÜV Informationstechnik GmbH. The evaluation was completed on March 23rd 2020. TÜV Informationstechnik GmbH is an evaluation facility (ITSEF)[5] recognised by the certification body of BSI.

For this certification procedure the sponsor and applicant is: Federal Office for Information Security (BSI).

The product was developed by: Federal Office for Information Security (BSI).

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 8 May 2020 is valid until 7 May 2025. Validity can be re-newed by re-certification.

The owner of the certificate is obliged:

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

[5] Information Technology Security Evaluation Facility

2. to inform the Certification Body at BSI immediately about vulnerabilities of the product that have been identified by the developer or any third party after issuance of the certificate,
3. to inform the Certification Body at BSI immediately in the case that security relevant changes in the evaluated life cycle, e.g. related to development and production sites or processes, occur, or the confidentiality of documentation and information related to the Target of Evaluation (TOE) or resulting from the evaluation and certification procedure where the certification of the product has assumed this confidentiality being maintained, is not given any longer. In particular, prior to the dissemination of confidential documentation and information related to the TOE or resulting from the evaluation and certification procedure that do not belong to the deliverables according to the Certification Report part B, or for those where no dissemination rules have been agreed on, to third parties, the Certification Body at BSI has to be informed.
4. to take care that the product “de.fac2“ will not be produced, as it is intended to be a pilot project for FIDO U2F Authenticator Applets in general.

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 applicant Federal Office for Information Security (BSI) decided the certification results not to be published on the BSI-Website and in [5]. Further copies of this Certification Report can be requested from the developer[6] of the product.

[6] Federal Office for Information Security (BSI)
Referat TK 11
Godesberger Allee 185-189
53175 Bonn

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 the de.fac2 – FIDO U2F Authenticator Applet 1.34 intended for FIDO Universal Second Factor (U2F) authentication with a specific implementation of the U2F token. The authenticator is physically implemented as a security chip with an application and is used to securely access online services. The authenticator, also referred to as a “U2F token” (or just “token”), communicates with an external server controlled by a relying party (RP) that supports the standardised FIDO U2F protocol. The TOE is a dual-interface secure chip including all IC dedicated software, embedded in an arbitrary housing with embedded software including the operating system and an application for FIDO U2F authentication. The TOE comprises the hardware platform IFX M5073 G11 (Certificate: BSI-DSZ-CC-0951-2015 [15], including re-assessment BSI-DSZ-CC-0951-2015-RA-01 [16]), the Sm@rtCafé® Expert 7.0 C3 Operating System by Gieseke+Devrient including the Giesecke+Devrient crypto library (certification ID BSI-DSZ-CC-1028-2017-MA-01 [12] based on BSI-DSZ-CC-1028-201 [11]) and the applet for FIDO U2F authentication and its documentation.

The Security Target [6] is the basis for this certification. It is based on the certified Protection Profile FIDO Universal Second Factor (U2F) Authenticator Version 3, 5 November 2018, BSI-CC-PP-0096-V3-2018 [8].

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

The TOE Security Functional Requirements (SFR) relevant for the TOE are outlined in the Security Target [6], chapter 5.1. 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_StrongAuthentication	This security function defines and controls the processes relevant for FIDO protocol and the underlying cryptographic support.
SF_Unlinkability	This security function provides unlinkability by ensuring that unique key pairs for each relying party and account are generated.
SF_Privacy	This security function ensures that no subject is able to determine the real user name bound the user.
SF_UserPresence	This security function provides a physical test of user presence.
SF_TSF-Protection	This security function provides protection of the TSF and is covered by the underlying platform. This includes resistance against physical attacks.

Table 1: TOE Security Functionalities

For more details please refer to the Security Target [6], chapter 6.1.

The assets to be protected by the TOE are defined in the Security Target [6], chapter 3.1.1. 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], chapters 3.2 - 3.4.

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:

de.fac2 - FIDO U2F Authenticator Applet, v1.34

The following table outlines the TOE deliverables:

No	Type	Identifier	Release	Form of Delivery
1	HW & SW	*de.fac2 - FIDO U2F Authenticator Applet* on platform SmartCafe Expert 7.0 C3 (IC, JCOS, and applet)	1.34	The delivery process is included in the evaluation of the underlying smartcard OS
2	DOC	*Developer Documentation AGD– User Guidance*	1.1	Download as PDF

Table 2: Deliverables of the TOE

According to the [6, ch. 1.2.4] the life cycle of the TOE consists of 3 stages:

- Stage 1: Development
  - Step 1 – IC Development (ICPP Phase 2),
  - Step 2a – Security IC Embedded Software Development (ICPP Phase 1),
  - Step 2b – Applet Development (ICPP Phase 1),
- Stage 2: Manufacturing
  - Step 3 – IC Manufacturing (ICPP Phase 3),
  - Step 4 – IC Packaging (ICPP Phase 4),
  - Step 5 – Composite product integration (ICPP Phase 5),
  - Step 6 – Personalisation (ICPP Phase 6),
- Stage 3: Operational Use
  - Step 7 – Operational Use (ICPP Phase 7).

The composite TOE comprising IC, JCOS and applet is delivered in the sense of CC after Step 5. Since there are no personalisation steps for the current TOE, the TOE is ready for

use after Step 5. The delivery process is included in the evaluation of the underlying smartcard OS.

The guidance of the composite TOE can be downloaded as a PDF from the BSI website. The user shall verify the SHA-512 checksum of the guidance with the reference value stated here:

0fea3736c0598f37b51e1fac05e06f9bb124a28459dd6b7b2c3b5978340cc1e86c86cdddd9
64c3916e872de148f1c2b21282e24b657e6189f60add6d5b417b07

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:

- Strong Authentication [6, ch. 6.1.1],
- Unlinkability [6, ch. 6.1.2],
- Privacy [6, ch. 6.1.3],
- User Presence Check [6, ch. 6.1.4], and
- TSF Protection [6, ch. 6.1.5].

Specific details concerning the above mentioned security policies can be found in chapters 5.1 and 6.1 of the Security Target (ST).

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.RespectSecurityBoundaries: Ensure that registrations and key material as a shared system resource is appropriately protected according to the operating environment privilege boundaries in place on the FIDO user agent.
- OE.Attestation: The Attestation certificate as well as the attestation key material is generated with high cryptographic security in a secure environment. The attestation keys are securely imported by the manufacturer and stored in the TOE. For privacy reasons a large amount of FIDO Token shares the same attestation key.

Details can be found in the Security Target [6], chapter 3.6.

5. Architectural Information

The composite TOE, de.fac2 – FIDO U2F Authenticator Applet, is a Java Card applet based on a certified Java Card platform and comprises the following subsystems, listed with a short description in the following itemization:

- JavaCard Platform: This subsystem represents the parts of the underlying platform consisting of the hardware and the JavaCard Runtime Environment which includes the implementation of the Java Card Virtual Machine, the Java Card API classes, and runtime support services.

- Control & Communication Subsystem: This subsystem contains all modules which handle the input and output data which are transmitted via TSFI.
- Crypto Subsystem: This subsystem provides the cryptographic functions like key initialization, key derivation and MAC calculation using the underlying platform functionality.

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

According to the ST, the TOE can have only one configuration, namely the CFG_DEFAULT. To allow a complete test run, the developer chose to introduce the additional configuration CFG_DEACTIVATED_USER_PRESENCE_CHECK which deactivates the “user presence check”. Also, the TOE is available with either contactless or contact based interface. Both of these interfaces were tested with both of the available test configurations.

7.1. Developer's Test according to ATE_FUN

Testing was performed by the developer using the external interfaces of the TOE, i.e. via ISO7816 APDU protocol using both contactless and contact-based interface. The test scenarios cover all defined external interfaces.

The developer testing was carried out using the TOE configuration as defined in the Security Target. Additionally, testing was performed with a modified TOE, using deactivated user presence check.

The test cases defined by the developer are based on the test described in the Basic U2F NFC Test Harness provided by the FIDO alliance. Additional test cases were created to test the reset function which is not part of the FIDO U2F standard.

All test scenarios were found to be well described and repeatable by stating all its ordering dependencies and preconditions to be fulfilled. Expected results in form of status words were found to be unambiguously and correctly defined with regard to its expected behaviour.

All actual results were consistent to its expected results. Thus, the developer’s testing showed that the TOE matches its defined and expected behaviour and security functionality.

7.2. Evaluator Tests

Independent Testing according to ATE_IND

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 at the Evaluation Body with the TOE developer test environment and additional Evaluation Body test equipment using test scripts.

TOE test configurations:

- Tests were performed with different TOE configurations, i.e. via different interfaces and with user presence check activated/deactivated.

The test samples provided by the developer were set-up following to the guidance descriptions such to create a valid TOE. Different life-cycle states for the TOE do not exist. After delivery, the TOE is always in an operational state (READY_FOR_USE) or was verified to be not usable at all.

Subset size chosen:

- During sample testing the evaluator chose to repeat the developer functional tests at the Evaluation Body for IT Security in Essen. All developer tests were repeated.
- During independent testing the evaluator used test scripts to invoke and test functionality given by the TSFI. Further penetration testing was done for AVA_VAN aspects. This includes the penetration with laser fault injection attacks, card tearing and fuzzy testing.

Interfaces tested:

- All TSFI were tested in the course of independent testing. The TOE provides only limited functionality and interfaces such that all TSFI were covered by testing.

Verdict for the activity:

- During the evaluator's TSF subset testing the TOE was operated as specified.
- No unexpected behaviour was observed.

The evaluator verified the developer's test results by executing all of the developer's tests and verifying the test log files for successful execution.

Penetration Testing according to AVA_VAN

Overview:

- The penetration testing was performed at the site of the evaluation body TÜViT in the evaluator's test environment with the evaluator's test equipment. The samples were provided by the developer. The test samples were configured and parameterized by the evaluator according to the guidance documentation. The one configuration of the TOE being intended to be covered by the current evaluation was tested.
- 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 the 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 penetration tests, where the evaluator is of the opinion that the vulnerabilities could be exploitable. While doing this, the evaluator also

considered all aspects of the security architecture of the TOE, being not covered by the functional developer tests.

- The source code review of the provided implementation representation accompanied the development of test cases and was 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 tests were performed with the one configuration of the TOE as defined in the Security Target.

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 ST [6] provided that all measures required by the developer are applied.

7.3. 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 ST [6] provided that all measures required by the developer are applied.

8. Evaluated Configuration

The Security Target has identified solely one configuration of the TOE, namely the CFG_DEFAULT. No other applications are allowed on the same authenticator to support the TOE security functions Unlinkability and Privacy.

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 and guidance specific for the technology of the product [4] (AIS 34).

The following guidance specific for the technology was used:

(i) Composite product evaluation for Smart Cards and similar devices (see AIS 36). According to this concept the relevant guidance documents of the underlying platform and the documents ETR for Composition from the platform evaluations (i.e. on OS [11, 12, 13, 14] and on IC [15, 16, 17]) have been applied in the TOE evaluation.

(ii) Guidance for Smartcard Evaluation

(iii) Application of Attack Potential to Smartcards (see AIS 26)

For RNG assessment the scheme interpretations AIS 20 was 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 AVA_VAN.5 augmented for this TOE evaluation.

The evaluation has confirmed:

- PP Conformance: FIDO Universal Second Factor (U2F) Authenticator Version 3, 5 November 2018, BSI-CC-PP-0096-V3-2018 [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 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

The table presented in chapter 6.3 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).

According to [18] and [19] the algorithms are suitable for key generation and derivation, random number generation and authentication functions. An explicit validity period is not given.

9.3. Additional Evaluation Results

Impact Assessment of IC Platform Update

At the time of initial creation of the ETR (first version of the ETR) the ETR for Composition of the underlying IC [17] which was used in the current evaluation as part of the underlying JCOS platform was older than 18 months. However, the IC that is the basis of the underlying JCOS platform and the current composite TOE has been recertified. The certification body agreed that within the context of this evaluation the ETR is accepted although the ETR for Composition of the IC is older than 18 months, if the composite TOE consisting of the applet, the JCOS and the IC also fulfils the requirements imposed in the latest IC recertification. The current composite evaluation is based on the JCOS which was certified under ID BSI-DSZ-CC-1028-2017-MA-01 which bases on the IC certified under ID BSI-DSZ-CC-0951-2015 (including BSI-DSZ-CC-0951-2015-RA-01). The IC certified

under ID BSI-DSZ-CC-0951-2015 (including BSI-DSZ-CC-0951-2015-RA-01) was recertified under IDs BSI-DSZ-CC-0951-V2-2017 and BSI-DSZ-CC-0951-V3-2018.

None of the security functionalities of the current composite TOE relies on functionalities that were changed in the course of the IC recertification. The current composite TOE fulfils also the requirements of the IC certification with ID BSI-DSZ-CC-0951-V3-2018.

Impact Assessment of Java Card Platform Update

At the time of initial creation of the ETR (first version of the ETR) the ETR for Composition of the underlying JCOS [13] (Smartcafe Expert v7.0 C3) was slightly older than 18 months. From a technical perspective the evaluation body does not have any concerns because of this expiration:

The composite TOE takes care of the recommendations and requirements imposed by the guidance documentation and ETR for composition of the underlying platform to be resistant against attackers with attack potential high.

In the meantime, a re-evaluation of the Java Card Platform (Smartcafe Expert v7.0 C4) was performed and finished under the certification ID BSI-DSZ-CC-1084-2019. The updated JCOS platform comprised another, but very similar IC (M7893 B11), a different configuration of interfaces, a few bugfixes, the removal of some EC key lengths and an update of the operational user guidance. None of the updates and changes have a negative impact on the present TOE and it still fulfills all guidance requirements of the latest re-evaluation.

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)

None

13. Definitions

13.1. Acronyms

AIS	Application Notes and Interpretations of the Scheme
BSI	Bundesamt für Sicherheit in der Informationstechnik / Federal Office for Information Security, Bonn, Germany
BSIG	BSI-Gesetz / Act on the Federal Office for Information Security
CCRA	Common Criteria Recognition Arrangement
CC	Common Criteria for IT Security Evaluation
CEM	Common Methodology for Information Technology Security Evaluation
cPP	Collaborative Protection Profile
EAL	Evaluation Assurance Level
ETR	Evaluation Technical Report
FIDO	Fast IDentification Online
FIDO U2F	Fast IDentification Online Universal Second Factor
IT	Information Technology
ITSEF	Information Technology Security Evaluation Facility
PP	Protection Profile
SAR	Security Assurance Requirement

SFP	Security Function Policy
SFR	Security Functional Requirement
ST	Security Target
TOE	Target of Evaluation
TSF	TOE Security Functionality

13.2. Glossary

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

Computing Environment The user's computer that is interacting with the FIDO Token.

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.

FIDO User Device The computing device where the FIDO Client operates, and from which the user initiates an action that utilizes FIDO.

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[7] 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-1060-2020, Version 1.24, December 16th, 2019, Common Criteria Security Target de.fac2 – FIDO U2F Authenticator Applet v 1.34, Bundesamt für Sicherheit in der Informationstechnik

[7] Evaluation Technical Report, Version 4, March 9th, 2020, Evaluation Technical Report Summary for de.fac2 – FIDO U2F Authenticator Applet 1.34, TÜV Informationstechnik GmbH, (confidential document)

[8] Common Criteria Protection Profile FIDO Universal Second Factor (U2F) Authenticator Version 3, 5 November 2018, BSI-CC-PP-0096-V3-2018

[9] Configuration list for the TOE, Version 1.5, March 2nd, 2020, Developer Documentation - Configuration Item List

[10] Guidance documentation for the TOE, Version 1.3, December 16th, 2019, Developer Documentation AGD – User Guidance

[7] specifically

- AIS 1, Version 14, Durchführung der Ortsbesichtigung in der Entwicklungsumgebung des Herstellers
- AIS 14, Version 7, Anforderungen an Aufbau und Inhalt der ETR-Teile (Evaluation Technical Report) für Evaluationen nach CC
- AIS 19, Version 9, Anforderungen an Aufbau und Inhalt der Zusammenfassung des ETR (Evaluation Technical Report) für Evaluationen nach CC (Common Criteria) und ITSEC
- AIS 20, Version 3, Funktionalitätsklassen und Evaluationsmethodologie für deterministische Zufallszahlengeneratoren
- AIS 23, Version 4, Zusammentragen von Nachweisen der Entwickler
- 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 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 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, Wiederverwendung von Evaluationsergebnissen
- AIS 46, Version 3, Info zur Evaluierung von Krypto und RNG

[11] Certification Report BSI-DSZ-CC-1028-2017 for Sm@rtCafé Expert 7.0 C3 from Veridos GmbH – Identity Solutions by G&D BDR, September 8th, 2017, including latest reassessments, Bundesamt für Sicherheit in der Informationstechnik

[12] Assurance Continuity Maintenance Report BSI-DSZ-CC-1028-2017-MA-01 Sm@rtCafé Expert 7.0 C3 from Giesecke+Devrient Mobile Security GmbH, October 4th, 2018, Bundesamt für Sicherheit in der Informationstechnik

[13] Evaluation Technical Report for Composite Evaluation, Sm@rtCafé® Expert 7.0 C3, BSI-DSZ-CC-1028, Version 3, 2017-08-16, including latest reassessments, TÜV Informationstechnik GmbH

[14] Evaluation Technical Report for Composite Evaluation Addendum for Sm@rtCafé® Expert 7.0 C3, BSI-DSZ-CC-1028-2017-MA-01, Version 1, 2018-07-18, TÜV Informationstechnik GmbH

[15] Certification Report – BSI-DSZ-CC-0951-2015 for Infineon Security Controller M5073 G11 with optional RSA2048/4096 v2.03.008, EC v2.03.008, SHA-2 v1.01 and Toolbox v2.03.008 libraries and with specific IC dedicated software (firmware) from Infineon Technologies AG, November 11th, 2015, including latest reassessments, Bundesamt für Sicherheit in der Informationstechnik

[16] Assurance Continuity Reassessment Report, BSI-DSZ-CC-0951-2015-RA-01, Infineon Security Controller M5073 G11 with optional RSA2048/4096 v2.03.008, EC v2.03.008, SHA-2 v1.01 and Toolbox v2.03.008 libraries and with specific IC dedicated software (firmware) from Infineon Technologies AG, May 31st, 2017, Bundesamt für Sicherheit in der Informationstechnik

[17] Evaluation Technical Report for Composite Evaluation, M5073 G11, BSI-DSZ-CC-0951, Version 4, May 18th, 2017, including latest reassessments, TÜV Informationstechnik GmbH

[18] FIDO Alliance Universal 2nd Factor 1.1 Specifications, September 15th, 2016, FIDO Alliance

[19] FIDO Authenticator Allowed Cryptography List, May 24th, 2017, FIDO Alliance

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-1060-2020

Evaluation results regarding development and production environment

The IT product de.fac2 - FIDO U2F Authenticator Applet, v1.34 (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 8 May 2020, 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.1, ALC_LCD.1, ALC_TAT.1)

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

a) Bundesamt für Sicherheit in der Informationstechnik, Heinemannstr 11-13, 53175 Bonn, Germany (Application development)

b) The development and production sites of the underlying platform are listed in [13].

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