Federal Office
for Information Security

Assurance Continuity Maintenance Report

BSI-DSZ-CC-1060-2020-MA-01

de.fac2 - FIDO U2F Authenticator Applet

from

BSI

The IT product identified in this report was assessed according to the *Assurance Continuity: CCRA Requirements,* version 2.1, June 2012 and the developer's Impact Analysis Report (IAR). The baseline for this assessment was the Certification Report, the Security Target and the Evaluation Technical Report of the product certified by the Federal Office for Information Security (BSI) under BSI-DSZ-CC-1060-2020.

The certified product itself did not change. The changes are related to an update of the user guidance including the Security Target.

Consideration of the nature of the change leads to the conclusion that it is classified as a minor change and that certificate maintenance is the correct path to continuity of assurance.

The resistance to attacks has not been re-assessed in the course of this maintenance process. Therefore, the assurance statement as outlined in the Certification Report BSI-DSZ-CC-1060-2020 dated 08. May. 2020 is of relevance and has to be considered when using the product. Details can be found on the following pages.

This report is an addendum to the Certification Report BSI-DSZ-CC-1060-2020.

Common Criteria

Bonn, 18 July 2022

The Federal Office for Information Security

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

Assessment

The IT product identified in this report was assessed according to the *Assurance Continuity: CCRA Requirements* [1] and the Impact Analysis Report (IAR) [2]. The baseline for this assessment was the Certification Report of the certified product (Target of Evaluation, TOE) [3], its Security Target and the Evaluation Technical Report as outlined in [3].

The vendor for the de.fac2 - FIDO U2F Authenticator Applet, BSI, submitted an IAR [2] to the BSI for approval. The IAR is intended to satisfy the requirements outlined in the document *Assurance Continuity: CCRA Requirements* [1]. In accordance with those requirements, the IAR describes (i) the changes made to the certified TOE, (ii) the evidence updated as a result of the changes and (iii) the security impact of the changes.

The certified product itself did not change. The Security Target [7] was editorially updated.

The changes are related to an update of the user guidance [6] only. A note that the user environment needs to be free of malicious software was added.

Conclusion

The maintained change is at the level of an added note in the guidance documentation and the security target. The change has no effect on product assurance, but the updated guidance documentation has to be followed.

Consideration of the nature of the change leads to the conclusion that it is classified as a minor change and that certificate maintenance is the correct path to continuity of assurance.

The resistance to attacks has <u>not</u> been re-assessed in the course of this maintenance process. Therefore, the assurance statement as outlined in the Certification Report BSI-DSZ-CC-1060-2020 dated 08. May 2020 is of relevance and has to be considered when using the product.

Obligations and notes for the usage of the product:

All aspects of assumptions, threats and policies 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 for the TOE is required and thus requested from the sponsor of the certificate.

Additional Note: The strength of the cryptographic algorithms was not rated in the course of the product certification and this maintenance procedure (see BSIG[1] Section 9, Para. 4, Clause 2).

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

For details on results of the evaluation of cryptographic aspects refer to the Certification Report [3] chapter 9.2.

This report is an addendum to the Certification Report [3].

References

[1] Common Criteria document “Assurance Continuity: CCRA Requirements”, version 2.1, June 2012

[2] Impact Analysis Report (IAR) de.fac2 - FIDO U2F Authenticator Applet BSI-DSZ-CC-1060-2020, version 0.1, 14. June 2022, BSI

[3] Certification Report BSI-DSZ-CC-1060-2020 for de.fac2 - FIDO U2F Authenticator Applet v1.34, Bundesamt für Sicherheit in der Informationstechnik, 08. May 2020

[4] 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

[5] Configuration list for the TOE, Version 1.6, 07. June 2022, Developer Documentation - Configuration Item List

[6] Guidance documentation for the TOE, Version 1.4, 14. June 2022, Developer Documentation AGD – User Guidance

[7] Security Target BSI-DSZ-CC-1060-2020, Version 1.25, 14. June 2022, Common Criteria Security Target de.fac2 – FIDO U2F Authenticator Applet v 1.34, Bundesamt für Sicherheit in der Informationstechnik