Bundesamt
für Sicherheit in der
Informationstechnik

Bundesamt für Sicherheit in der Informationstechnik
Postfach 20 03 63, 53133 Bonn

Bundesamt für Sicherheit in der Informationstechnik
Frau Astrid Eichler
Referat TK 11
Godesberger Allee 185-189
53175 Bonn

Gereon Killian

HAUSANSCHRIFT
Bundesamt für Sicherheit in
der Informationstechnik
Godesberger Allee 185-189
53175 Bonn

POSTANSCHRIFT
Postfach 20 03 63
53133 Bonn

TEL +49 228 99 9582-5138
FAX +49 228 99 10 9582-5138

ZertDokus@bsi.bund.de
https://www.bsi.bund.de

Betreff: Zertifizierung des Produkts de.fac2 - FIDO U2F Authenticator Applet, v1.34
Bezug: Amtliches Ersuchen auf Erteilung eines Deutschen IT-Sicherheitszertifikates durch das BSI vom 27. November 2017
Aktenzeichen: SZ 21-720-01-00
Datum: 8. Mai 2020

Anlage: Zertifizierungsurkunde BSI-DSZ-CC-1060-2020, Version 1.0 vom 8. Mai 2020,
Zertifizierungsreport BSI-DSZ-CC-1060-2020, Version 1.0

Sachstand:

Für das Produkt de.fac2 - FIDO U2F Authenticator Applet, v1.34 des Bundesamt für Sicherheit in der Informationstechnik wird das Sicherheitszertifikat BSI-DSZ-CC-1060-2020 erteilt.

Hinsichtlich der Kosten des Verfahrens ergeht ein gesonderter Kostenbescheid.

Das Zertifikat ist bis 7. Mai 2025 gültig.

Nebenbestimmungen:

Als Inhaber des Zertifikates sind Sie verpflichtet,

1. bei der Bewerbung des Zertifikates oder der Tatsache der Zertifizierung des Produktes auf den Zertifizierungsreport hinzuweisen sowie jedem Anwender des Produktes den Zertifizierungsreport und die darin referenzierten Sicherheitsvorgaben und Benutzerdokumentation für den Einsatz oder die Verwendung des zertifizieren Produktes zur Verfügung zu stellen,
2. die Zertifizierungsstelle des BSI unverzüglich über Schwachstellen des Produktes zu informieren, die nach dem Zeitpunkt der Zertifizierung durch Sie oder Dritte festgestellt wurden,

3. die Zertifizierungsstelle des BSI unverzüglich zu informieren, wenn sich sicherheitsrelevante Änderungen am geprüften Lebenszyklus, z. B. an Standorten oder Prozessen, ergeben oder die Vertraulichkeit von Unterlagen und Informationen zum Evaluierungsgegenstand oder aus dem Evaluierungs- und Zertifizierungsprozess bei denen die Zertifizierung des Produktes von der Aufrechterhaltung der Vertraulichkeit für den Bestand des Zertifikates ausgegangen ist, nicht mehr gegeben ist. Insbesondere ist vor Herausgabe von vertraulichen Unterlagen oder Informationen zum Evaluierungsgegenstand oder aus dem Evaluierungs- und Zertifizierungsprozess, die nicht zum Lieferumfang gemäß Zertifizierungsreport Teil B gehören oder für die keine Weitergaberegelung vereinbart ist, an Dritte, die Zertifizierungsstelle des BSI zu informieren.
4. dafür Sorge zu tragen, dass das Produkt „de.fac2" entsprechend seiner Bestimmung als Pilotprojekt eines FIDO U2F Authenticator Applets nicht produziert wird.

Begründung:

1. Zum fachlichen Prüfergebnis:

Mit Antrag vom 27. November 2017, hier vollständig eingegangen am 21. Dezember 2017, haben Sie für o.g. Produkt eine Zertifizierung nach der Evaluationsstufe EAL 4 mit Zusatz gemäß den Gemeinsamen Kriterien für die Prüfung und Bewertung der Sicherheit von Informationstechnik, Version 3.1 (CC) durch das BSI von Amts wegen ersucht.

Das Produkt de.fac2 - FIDO U2F Authenticator Applet, v1.34 wurde durch die vom BSI anerkannte Prüfstelle TÜV Informationstechnik GmbH bis 26. März 2020 evaluiert.

Die Evaluierung wurde durch die Zertifizierungsstelle des BSI überwacht. Das Verfahren wurde mit heutigem Datum beendet.

Das Prüfergebnis lautet:

Schutzprofilkonformität:	FIDO Universal Second Factor (U2F) Authenticator Version 3, 5 November 2018, BSI-CC-PP-0096-V3-2018
Funktionalität:	PP konform plus produktspezifische Ergänzungen Common Criteria Teil 2 erweitert
Bestätigtes Vertrauenswürdigkeitspaket:	Common Criteria Teil 3 konform EAL 4 mit Zusatz von AVA_VAN.5

Das BSI hat dieses Prüfergebnis bestätigt. Ihrem Ersuchen konnte somit hinsichtlich der Evaluationsstufe entsprochen werden. Die Ergebnisse des Zertifizierungsverfahrens sind im Detail in beiliegendem Zertifizierungsreport enthalten.

2. Zur Gültigkeitdauer:

Gemäß Zertifizierungsverordnung §12 (2) ist das Zertifikat zu befristen. Das Bundesamt hat die Gültigkeitsdauer für den jeweiligen technischen Geltungsbereich festzusetzen.

Das Zertifikat bestätigt die Vertrauenswürdigkeit des Produktes gemäß den Sicherheitsvorgaben zum Zeitpunkt der Ausstellung. Da die Verwendung des Zertifikates jedoch auch und insbesondere in die

Zukunft gerichtet ist, die mit dem Zertifikat verbundene Sicherheitsaussage angesichts des kontinuierlichen technischen Fortschritts aber nicht unbeschränkt Gültigkeit haben kann, ist es erforderlich, eine Höchstdauer der Geltung festzulegen.

Unter Abwägung der fachlichen Gesichtspunkte der Erfahrungen in der Fortentwicklung der Angriffstechnologie und einer damit begründeten kürzeren Gültigkeitsdauer einerseits, den wirtschaftlichen Interessen des Antragstellers mit Bedarf nach einer langen Gültigkeitsdauer andererseits wird das Zertifikat auf 5 Jahre unter Auflagen befristet (siehe Nebenbestimmung 4).

3. Zu Nebenbestimmung 1:

Das Zertifikat gilt nur in Zusammenhang mit dem Zertifizierungsreport und nur für die hier angegebene Version des Produktes. Das bestätigte Vertrauenswürdigkeitspaket gilt nur unter der Voraussetzung, dass alle Auflagen bzgl. Generierung, Konfiguration und Betrieb, soweit sie im Zertifizierungsreport angegeben sind, beachtet werden und das Produkt in der im Zertifizierungsreport und in den Sicherheitsvorgaben beschriebenen Einsatzumgebung betrieben wird. Daher ist der Hinweis auf den Zertifizierungsreport bei der Bewerbung des Zertifikates oder der Tatsache der Zertifizierung des Produktes wichtig, damit der Anwender in Kenntnis gesetzt wird, dass es Ergebnisdokumentation zur Zertifizierung des Produktes gibt. Der erforderliche Hinweis auf den Zertifizierungsreport bei der Bewerbung des Zertifikates oder der Tatsache der Zertifizierung kann auch durch eine Referenz auf die BSI-Internetseite www.bsi.bund.de, Rubrik Zertifizierung und Anerkennung / Zertifizierung nach Produkten/ Zertifizierung nach CC / Zertifizierte Produkte nach CC erfolgen, sofern der Veröffentlichung des Zertifikats zugestimmt wurde.

Der Zertifizierungsreport mit den Sicherheitsvorgaben als Anlage enthält Informationen zum geprüften Funktionsumfang des Produktes, zu den angewendeten Prüfvorgaben und zu den Ergebnissen des Zertifizierungsverfahrens sowie Hinweise und Auflagen für die Anwendung des Produktes in der zertifizierten Version und Konfiguration. Diese Information ist für einen Benutzer des Produktes notwendig zu kennen. Die Benutzerdokumentation zum Produkt beinhaltet ebenso Informationen zur im Sinne der zertifizierten Version des Produktes sachgerechten Konfiguration und Benutzung des Produktes. Daher sind diese Unterlagen dem Anwender zur Verfügung zu stellen.

4. Zu Nebenbestimmung 2:

Das Zertifikat wurde auf Basis der zur Verfügung gestellten Nachweise und der durchgeführten Evaluierung erteilt und der Anwender des zertifizierten Produktes verlässt sich z.B. im Rahmen seines Risikomanagements auf das Zertifizierungsergebnis im Hinblick auf die Wirksamkeit der in den Sicherheitsvorgaben beschriebenen Sicherheitseigenschaften und Schutz der Objekte. Bekannt gewordene Schwachstellen können das Zertifizierungsergebnis in Frage stellen und damit das Vertrauen des Anwenders in die zertifizierte Sicherheit des Produktes. Daher ist die Zertifizierungsstelle des BSI unverzüglich darüber zu informieren.

5. Zu Nebenbestimmung 3:

Das Zertifikat wurde unter der Maßgabe der Vertraulichkeit bestimmter Unterlagen und Informationen zum Evaluierungsgegenstand und der Aufrechterhaltung bestimmter Prozesse erteilt. Das Ergebnis der Zertifizierung und insbesondere das Ergebnis der Schwachstellenanalyse und damit auch der Bestand des Zertifikates basieren auf diesen Annahmen. Des weiteren verlässt sich der Anwender des

zertifizierten Produktes z.B. im Rahmen seines Risikomanagements auf das Zertifizierungsergebnis im Hinblick auf die Wirksamkeit der in den Sicherheitsvorgaben beschriebenen Sicherheitseigenschaften und Schutz der Objekte.

Der Antragsteller und Inhaber des Zertifikates ist für die Aufrechterhaltung der Vertraulichkeit dieser Unterlagen und damit für den Bestand dieser Annahmen verantwortlich. Veränderungen in diesem Bereich oder die geplante Weitergabe von vertraulichen Unterlagen oder Informationen zum Evaluierungsgegenstand, die nicht zur Weitergabe bestimmt waren oder für die keine Regelung vereinbart wurde, können das Zertifizierungsergebnis in Frage stellen und damit das Vertrauen des Anwenders in die zertifizierte Sicherheit des Produktes. Daher ist die Zertifizierungsstelle des BSI vorab darüber zu informieren.

6. zu Nebenbestimmung 4:

Das in diesem Zertifizierungsverfahren beschriebene FIDO U2F Authenticator Applet ist als Pilotprojekt aufgesetzt, welches nicht zur Produktion bestimmt ist. Aus diesem Grunde wurden manche Anforderungen an den produzierten TOE nur beispielhaft umgesetzt und entsprechen nicht den Anforderungen an sichere Produkte. Das Zertifikat soll lediglich dazu dienen, die Machbarkeit anhand einer beispielhaften Zertifizierung aufzuzeigen.

Hinweise:

Hinsichtlich der Bedeutung der Vertrauenswürdigkeitsstufen vgl. die Auszüge aus den technischen Regelwerken am Ende des Zertifizierungsreportes und die Erläuterungen in den Kriterien.

Dieses Zertifikat ist keine Empfehlung des IT-Produktes durch das Bundesamt für Sicherheit in der Informationstechnik oder eine andere Organisation, die dieses Zertifikat anerkennt oder darauf Einfluss hatte. Ebenfalls wird keine Gewährleistung für das IT-Produkt durch das Bundesamt für Sicherheit in der Informationstechnik oder eine andere Organisation, die dieses Zertifikat anerkennt oder darauf Einfluss hatte, übernommen.

Im Falle von Änderungen an der zertifizierten Version des Produktes kann die Gültigkeit des Zertifikats auf neue Versionen ausgedehnt werden, sofern der Antragsteller für das geänderte Produkt die Aufrechterhaltung der Aussage zur Vertrauenswürdigkeit (d.h. Re-Zertifizierung oder Maintenance) entsprechend den Vorgaben beantragt und die Prüfung keine sicherheitstechnischen Mängel ergibt.

Die Gültigkeitsdauer dieses Zertifikates kann jederzeit nach den Verfahrensregelungen des Zertifizierungsschemas auf Antrag per Re-Zertifizierung verlängert werden, sofern die damit verbundene Re-Evaluierung erfolgreich verläuft.

Da sich Angriffsmethoden im Laufe der Zeit fortentwickeln können, sollte die Widerstandsfähigkeit des zertifizierten Produktes gegen neue Angriffsmethoden auf regelmäßiger Basis neu bewertet werden. Eine solche Neubewertung erfolgt im Zertifizierungsschema des BSI im Rahmen des Programms zur Aufrechterhaltung der Vertrauenswürdigkeit als Re-Assessment oder Re-Zertifizierung, sofern der Antragsteller diese Neubewertung entsprechend den Vorgaben beantragt.

Über die Wiederverwendbarkeit der Prüfergebnisse bei auf diesem Zertifikat aufbauenden Zertifizierungen oder Zulassungen entscheidet die jeweilige damit befasste Zertifizierung- oder Zulassungsstelle.

Nach Zertifizierungsverordnung §3 (2) sind Sie verpflichtet, die Nachweise zum Zertifizierungsverfahren für die Dauer der Gültigkeit des Zertifikates plus 3 Jahren zu archivieren und in diesem Zeitraum dem BSI jederzeit auf Anfrage kostenlos zur Verfügung zu stellen, um die zu Grunde liegende Entscheidung und die technische Entscheidungsgrundlage weiterhin nachvollziehen und überprüfen zu können. Zu den Nachweisen gehören: die in diesem Zertifizierungsverfahren evaluierten und für Tests verwendeten Bestandteile des Produktes (Evaluationsgegenstandes, EVG) und die im Evaluierungsbericht (ETR) bzw. in der Konfigurationsliste genannten Herstellernachweise.

Im Auftrag

Sandro Amendola

Sandro Amendola