Bundesamt
für Sicherheit in der
Informationstechnik

# Assurance Continuity Maintenance Report

## BSI-DSZ-CC-1121-V2-2021-MA-01

## Swissbit TSE SMAERS Firmware

der

## Swissbit AG

SOGIS
Recognition Agreement

Das in diesem Report genannte IT-Produkt wurde entsprechend der Anforderungen aus Assurance Continuity [1] und des Impact Analysis Report (IAR) des Herstellers beurteilt. Die Grundlage für diese Beurteilung war der Zertifizierungsreport, die Sicherheitsvorgaben und der technische Evaluierungsbericht des vom Bundesamt für Sicherheit in der Informationstechnik (BSI) unter der Zertifizierungs-ID BSI-DSZ-CC-1121-V2-2021 zertifizierten Produkts aktualisiert.

Die Änderung im Vergleich zum zertifizierten Produkt wurde auf der Ebene der Umgebung des zertifizierten Produktes vorgenommen. Hierbei ist nur die USB Konfiguration betroffen. Die Identifizierung des geänderten Produkts wird durch eine neue Versionsnummer des Endproduktes im Vergleich zum zertifizierten Produkt angezeigt.

Die Betrachtung der Art der Änderung führt zu der Entscheidung, dass die Änderung als “Minor Change“ eingestuft wird und dass das Maintenance-Verfahren für Zertifikate das sachgerechte Verfahren zur Aufrechterhaltung der Vertrauenswürdigkeit ist.

Die Widerstandsfähigkeit gegen Angriffe wurde im Rahmen dieses Maintenance-Verfahrens nicht neu bewertet. Aus diesem Grunde ist die Vertrauenswürdigkeitsaussage im Zertifizierungsreport vom BSI-DSZ-CC-1121-V2-2021 bei der Verwendung des Produktes heranzuziehen. Nähere Informationen finden sich auf den nächsten Seiten.

Dieser Report ist ein Anhang zum Zertifizierungsreport BSI-DSZ-CC-1121-V2-2021.

Common Criteria
Recognition Arrangement

Bonn, 31 March 2023

Bundesamt für Sicherheit in der Informationstechnik

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

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

# Beurteilung

Das in diesem Report genannte IT-Produkt wurde entsprechend der Anforderungen aus den Assurance Continuity [1] und des Impact Analysis Report (IAR) [2] beurteilt. Die Grundlage für diese Beurteilung war der Zertifizierungsreport des zertifizierten Produktes (Evaluierungsgegenstand, EVG) [3], die Sicherheitsvorgaben und der technische Evaluierungsbericht wie in [3] angegeben.

Der Vertreiber für Swissbit TSE SMAERS Firmware, Swissbit AG, legte dem BSI einen IAR [2] zur Entscheidung vor. Der IAR dient der Erfüllung, der in den Dokumenten Assurance Continuity [1] angegebenen Anforderungen. In Übereinstimmung mit diesen Anforderungen beschreibt der IAR (i) die am zertifizierten EVG vorgenommenen Änderungen, (ii) die aufgrund der Änderungen aktualisierten Unterlagen und (iii) die Auswirkungen der Änderungen auf die Sicherheit. Zusätzlich wurde ein Impact Analysis Survey durch die Prüfstelle MTG AG vorgelegt. [4]

Das zertifizierte Produkt selbst hat sich nicht geändert. Die technische Einsatzumgebung hat sich geringfügig verändert. Die neue ID TOE Plattform Version (HW) lautet Swissbit USB TSE PU-50n TSE Series v1.1.1. Dies betrifft nur die USB Konfiguration. Die micro SD und SD Konfigurationen bleiben unverändert.

# Schlussfolgerung

Die Änderung des EVG wurde auf der Ebene der Umgebung vorgenommen. Die Änderung hat keine Auswirkungen auf die Vertrauenswürdigkeit.

Die Betrachtung der Art der Änderung führt zu der Entscheidung, dass die Änderung als “Minor Change“ eingestuft wird und dass das Maintenance-Verfahren für Zertifikate das sachgerechte Verfahren zur Aufrechterhaltung der Vertrauenswürdigkeit ist.

Die Widerstandsfähigkeit gegen Angriffe wurde im Rahmen dieses Maintenance-Verfahrens nicht neu bewertet. Aus diesem Grunde ist die Vertrauenswürdigkeitsaussage im Zertifizierungsreport BSI-DSZ-CC-1121-V2-2021 bei der Verwendung des Produktes heranzuziehen.

### Zusätzliche Auflagen und Hinweise für die Verwendung des Produkts:

Alle in den Sicherheitsvorgaben beschriebenen Aspekte der Anforderungen, Bedrohungen und organisatorischen Sicherheitspolitiken, welche nicht vom EVG abgedeckt werden, müssen von der Einsatzumgebung erfüllt werden.

Der Kunde beziehungsweise der Benutzer des Produkts muss die Zertifizierungsergebnisse im Rahmen des bei ihm realisierten Risikomanagementprozesses individuell bewerten. Um der Weiterentwicklung von Angriffsmethoden und -techniken entgegenzutreten, sollte der Kunde eine Zeitspanne definieren, ab der eine Neubewertung des EVGs erforderlich ist und daher vom Sponsor des Zertifikats verlangt werden wird.

Ergänzender Hinweis: Die Stärke der kryptographischen Algorithmen wurde im Rahmen der Basiszertifizierung und im Rahmen dieses Maintenanceverfahrens nicht bewertet (vgl. § 9 Abs. 4 Nr. 2 BSIG[1]).

Dieser Report ist ein Anhang zum Zertifizierungsreport [3].

1 Gesetz über das Bundesamt für Sicherheit in der Informationstechnik (BSI-Gesetz – BSIG) vom 14. August 2009, Bundesgesetzblatt I S. 2821

# Referenzen

[1] Common Criteria document “Assurance Continuity: CCRA Requirements”, version 2.2, 30 September 2021

Common Criteria document “Assurance Continuity: SOG-IS Requirements”, version 1.0, November 2019

[2] Swissbit TSE SMAERS 1.1.1 – Impact Analysis Report (IAR), Version 0.0.2 (vertrauliches Dokument)

[3] Zertifizierungsreport BSI-DSZ-CC-1121-V2-2021 für (Swissbit TSE SMAERS Firmware 1.1.0), Bundesamt für Sicherheit in der Informationstechnik, (26.November 2020)

[4] Impact Anaysis Survey, Version 1.2, 28. März 2023