



Assurance Continuity Maintenance Report

BSI-DSZ-CC-0525-2010-MA-01

SmartCase™ KB SCR eSIG, S26381-K529-Vxxx
HOS:01

der

Fujitsu Technology Solutions GmbH



Common Criteria Recognition
Arrangement
für Komponenten bis EAL 4



Das in diesem Report genannte IT-Produkt wurde entsprechend der Anforderungen aus *Assurance Continuity: CCRA Requirements*, Version 1.0, Februar 2004 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-0525-2010 zertifizierten Produkts.

Die Änderung im Vergleich zum zertifizierten Produkt wurde auf der Ebene von Code-Anteilen außerhalb der TSF vorgenommen, eine Änderung, die keine Auswirkungen auf die Vertrauenswürdigkeit hat. Die Identifizierung des geänderten Produkts erfolgt, verglichen mit dem zertifizierten Produkt, durch eine neue Firmware-Versionsnummer.

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 Grund ist die Vertrauenswürdigkeitsaussage im Zertifizierungsreport BSI-DSZ-CC-0525-2010 bei der Verwendung des Produktes heranzuziehen. Nähere Informationen finden sich auf den nächsten Seiten.

Dieser Report ist ein Anhang zum Zertifizierungsreport BSI-DSZ-CC-0525-2010.

Bonn, 4. Februar 2011



für Komponenten bis EAL 4

Beurteilung

Das in diesem Report genannte IT-Produkt wurde entsprechend der Anforderungen aus *Assurance Continuity: CCRA Requirements* [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 [4] und der technische Evaluierungsbericht, wie in [3] angegeben.

Der Vertreiber für SmartCase™ KB SCR eSIG, S26381-K529-Vxxx HOS:01, Fujitsu Technology Solutions GmbH, legte dem BSI einen IAR [2] zur Entscheidung vor. Der IAR dient der Erfüllung der in dem Dokument *Assurance Continuity: CCRA Requirements* [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.

Das SmartCase™ KB SCR eSIG, S26381-K529-Vxxx HOS:01 wurde aufgrund der Behebung eines Implementierungsfehlers in einem Schnittstellenmodul der Firmware geändert. Die Änderung ist aus Sicherheitssicht nicht signifikant, die Konfigurationsmanagement-Prozeduren jedoch erfordern eine Änderung der Versionsnummer der Firmware von 1.20 auf 1.21.

Ergebnis

Die Änderung des EVG wurde auf der Ebene von Code-Anteilen außerhalb der TSF vorgenommen, eine Änderung, die keine Auswirkungen auf die Vertrauenswürdigkeit hat. Die Untersuchung der Herstellernachweise zeigt, dass die durchgeführten Änderungen auf die redaktionelle Bearbeitung der Benutzerdokumentation und der Konfigurationsliste, sowie der Aktualisierung des SHA-256 Hashwertes für die Anwendung¹ zum Auslesen der Firmware-Version und die Fehlerbehebung von Code-Anteilen außerhalb der TSF begrenzt sind. Die Sicherheitsvorgaben wurden für die geänderte Produktversion redaktionell überarbeitet [7]. 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.

Daher stimmt das BSI der Ausdehnung der im Zertifizierungsreport [3] angegebenen Vertrauenswürdigkeit auf die Firmware-Version 1.21 des Produktes zu.

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.

¹ „FWCheck_KBSCReSIG_V121.exe“ mit dem folgenden SHA256-Hashwert:
E45265F8 F0EEAF28 F54A642A A1862C32 1EDF4548 F0DF6DFF D19E9980 40948520

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 zu begegnen, sollte der Kunde eine Zeitspanne definieren, ab der eine Neubewertung des EVGs erforderlich ist und daher vom Sponsor des Zertifikats verlangt werden wird.

Dieser Report ist ein Anhang zum Zertifizierungsreport [3].

Referenzen

- [1] Common Criteria Dokument CCIMB-2004-02-009 "Assurance Continuity: CCRA Requirements", Version 1.0, February 2004
- [2] Common-Criteria-Dokument Auswirkungsanalyse Firmwareänderung V1.20 auf V1.21, Version 1.01, 10.11.2010, ZF Electronics GmbH (Vertrauliches Dokument)
- [3] Zertifizierungsreport BSI-DSZ-CC-0525-2010 zu SmartCase KB SCR eSIG (S26381-K529-Vxxx) Hardware-Version HOS:01, Firmware-Version 1.20, Bundesamt für Sicherheit in der Informationstechnik, 11.01.2010
- [4] Sicherheitsvorgaben BSI-DSZ-0525-2010, Version 1.16, 09.09.2009, Common-Criteria-Dokument Sicherheitsvorgaben EAL3+, Fujitsu Technology Solutions GmbH
- [5] Common-Criteria-Dokument Konfigurationsliste, Version 1.01, 06.12.2010, Fujitsu Technology Solutions GmbH (vertrauliches Dokument)
- [6] Dokumentation für den EVG, Ausgabe November 2010, „USB-Security-Tastatur KB SCR eSIG Betriebsanleitung“
- [7] Sicherheitsvorgaben BSI-DSZ-0525-2010-MA01, Version 1.17, 10.11.2010, Common-Criteria-Dokument Sicherheitsvorgaben EAL3+, Fujitsu Technology Solutions GmbH