



Assurance Continuity Maintenance Report

BSI-DSZ-CC-0862-V2-2021-MA-02

POLYAS CORE, Version 2.5.4

der

Polyas GmbH



SOGIS
Recognition Agreement

Das in diesem Report genannte IT-Produkt wurde entsprechend der Anforderungen aus Assurance Continuity: CCRA Requirements, Version 2.1, Juni 2012 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-0862-V2-2021 zertifizierten Produkts aktualisiert durch BSI-DSZ-CC-0862-V2-2021-MA-01.



Die Änderung im Vergleich zum zertifizierten Produkt wurde auf der Ebene der EVG-Laufzeitumgebung vorgenommen. Die Implementierung der zertifizierten Sicherheitsleistungen des EVG ist unverändert.

Die Identifizierung des geänderten Produkts wird durch eine neue Versionsnummer im Vergleich zum zertifizierten Produkt angezeigt. Das Security Target und die Handbücher wurden entsprechend editorieell überarbeitet.

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-0862-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-0862-V2-2021.



Common Criteria
Recognition Arrangement
Anerkennung nur für
Komponenten bis EAL 2
und ALC_FLR



Bonn, 11. März 2022

Bundesamt für Sicherheit in der Informationstechnik

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 und der technische Evaluierungsbericht wie in [3] angegeben.

Der Vertreiber für POLYAS CORE, Version 2.5.4, die Polyas 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.

Die Laufzeitumgebung des EVG POLYAS CORE, Version 2.5.4 wurde zur Behebung einer Sicherheitslücke in dem Paket apache log4j geändert (Wechsel von der verwundbaren log4j Version 2.13.3 zur aktuellen Version 2.17.1).

Die Konfigurationsmanagement-Prozeduren erfordern eine Änderung der Bezeichnung des Produktes. Aus diesem Grunde wurde die Versionsnummer von Version 2.5.3 (aus BSI-DSZ-0862-V2-2021-MA-01) zu Version 2.5.4 geändert.

Die EVG-Software besteht aus fünf JAR-Dateien (Java Archiven). Jede JAR-Datei wird über die eindeutige Version des EVG, den Dateinamen und die Prüfsumme (SHA-256) der Datei eindeutig identifiziert. Da die EVG-Versionsnummer Teil der JAR-Datei ist, ändern sich die Prüfsummen der fünf JAR-Dateien:

- Urnen EVG – polyas-vote-2.5.4.jar mit SHA256-Prüfsumme:
db2b3a19091c7d9b4d1362c94093eb7fe19ef11290496cc057f91eef47e327af
- Wählerverzeichnis EVG – polyas-registry-2.5.4.jar mit SHA256-Prüfsumme:
799359111720a5f6406665273ebd76158ed73065f612355630d87c954eed113d
- Validator EVG – polyas-validator-2.5.4.jar mit SHA256-Prüfsumme:
8a36fc0f1fa84437e4f79a94383aebb20b991f620838df371b3a758efd2afc30
- Wahlvorstandsinterface EVG – polyas-management-2.5.4.jar mit SHA256-Prüfsumme:
682c45a571529b26de8d9e150ccfa6329a5463a97717bf77dff7f6effb16961f
- Gemeinsamer Bestandteil – polyas-common-2.5.4.jar mit SHA256-Prüfsumme:
594da7391f171ffc1086175b167cfd29c3b9eb1eff3bcb376febd82fe43da107

Die Sicherheitsvorgaben [5] und die Handbücher [6], [7] und [8] wurden editorieil aktualisiert.

Schlussfolgerung

Die Änderung wurde auf der Ebene der EVG-Laufzeitumgebung vorgenommen. Die Implementierung der zertifizierten Sicherheitsleistungen des EVG ist unverändert. 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-0862-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.

Dieser Report ist ein Anhang zum Zertifizierungsreport [3].

Referenzen

- [1] Common Criteria Document "Assurance Continuity: CCRA Requirements", Version 2.1, Juni 2012
- [2] Impact Analysis Report – Core 2.5.4, Version 1.1, 08.02.2022, Polyas GmbH (vertrauliches Dokument)
- [3] Zertifizierungsreport BSI-DSZ-CC-0862-V2-2021 für POLYAS CORE, Version 2.5.0, 25.06.2021, Bundesamt für Sicherheit in der Informationstechnik
Maintenance-Anhang BSI-DSZ-CC-0862-V2-2021-MA-01 für POLYAS CORE, Version 2.5.3, 24.11.2021, Bundesamt für Sicherheit in der Informationstechnik
- [4] Sicherheitsvorgaben für das Online-Wahlprodukt POLYAS CORE, Version 1.10, 27.05.2021, Polyas GmbH
- [5] Sicherheitsvorgaben für das Online-Wahlprodukt POLYAS CORE, Version 1.12, 17.01.2022, Polyas GmbH
- [6] Benutzerdokumentation Polyas 2.5.4 – Handreichung Wähler, Version 1.6, 17.01.2022, Polyas GmbH
- [7] Benutzerdokumentation Polyas 2.5.4 – Handreichung Wahlvorstand, Version 1.5, 17.01.2022, Polyas GmbH
- [8] Benutzerdokumentation Polyas 2.5.4 – Handreichung Wahlveranstalter, Version 1.9, 17.01.2022, Polyas GmbH