Bundesamt
für Sicherheit in der
Informationstechnik

Assurance Continuity Maintenance Report

BSI-DSZ-CC-0668-2010-MA-01

CardOS V4.4 with Application for QES Version 1.01

from

Atos IT Solutions and Services GmbH

Common Criteria Recognition
Arrangement
for components up to EAL4

The IT product identified in this report was assessed according to the *Assurance Continuity: CCRA Requirements,* version 1.0, February 2004 and the developers 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-0668-2010.

The change to the certified product is that it has been supplemented with a new Service Package. The change has no effect on assurance. The identification of the maintained product is indicated by a new version number compared to the certified product. Additionally, there has been an update in the guidance documents and the developers' company name has been changed.

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-0668-2010 dated 10 December 2010 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-0668-2010.

Bonn, 26 October 2011

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 [4] and the Evaluation Technical Report as outlined in [3].

The vendor for the CardOS V4.4 with Application for QES, Version 1.01, Atos IT Solutions and Services GmbH, 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 CardOS V4.4 with Application for QES, Version 1.01 was changed due to a new Service Package, an update in the guidance documents [7] – [11] and a new company name of the developer. Information about usage of test IDs was added to the guidance documents. Configuration Management procedures required a change in the product identifier. Therefore the version number changed from Version 1.00 to Version 1.01.

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-0668-2010 dated 10 December 2010 is of relevance and has to be considered when using the product.

Conclusion

The change to the TOE is at the level of a new Service Package, the guidance documentation and a new developers' name. The change has no effect on assurance. As a result of the changes the configuration list for the TOE has been updated [5].

The Security Target was editorially updated [6].

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.

Therefore, BSI agrees that the assurance as outlined in the Certification Report [3] is maintained for this version of the product.

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-0668-2010 dated 10 December 2010 is of relevance and has to be considered when using the product.

Additional 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.

The guidance has been replaced by new versions of the documents. As concerning the usage of the test IDs, the old versions are no longer valid and may not be used any more.

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

The following cryptographic algorithms are used by the TOE to enforce its security policy:

- algorithms for the encryption and decryption:
  RSA

This holds for the following security functionalities:

- SS3 SCD/SVD Pair Generation and SS4 Signature Creation

The validity period of the algorithms for the creation and verification of signatures is mentioned in the official catalogue [12]. The TOE is able to handle key lengths that are not valid according to [12].

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

References

[1] Common Criteria document CCIMB-2004-02-009 “Assurance Continuity: CCRA Requirements”, version 1.0, February 2004

[2] CardOS V4.4 (CNS) and CardOS DI V4.2C CNS Impact Analysis Report, version 1.20, Edition 07/2011,13 July 2011, Atos IT Solutions and Services GmbH (confidential document)

and

CardOS V4.4 (CNS) and CardOS DI V4.2C CNS Document Versions, version 1.00, Edition 10/2011, 7 October 2011 (part of Impact Analysis Report, confidential document)

[3] Certification Report BSI-DSZ-CC-0668-2010 for CardOS V4.4 with Application for QES from Siemens IT Solutions and Services GmbH, Bundesamt für Sicherheit in der Informationstechnik, 10 December 2010

[4] Security Target BSI-DSZ-CC-0668-2010, CardOS V4.4 with Application for QES, Version 0.50, Edition 04/2010, Siemens AG, 29.04.2010

[5] CardOS V4.4 with Application for QES Configuration List, Atos IT Solutions and Services GmbH, Version 0.30, Edition 07/2011, 13.07.2011 (confidential document)

[6] Security Target, CardOS V4.4 with Application for QES, Atos IT Solutions and Services GmbH, Version 0.70, Edition 07/2011, 13.07.2011

[7] CardOS V4.4, Administrator Guidance, Atos IT Solutions and Services GmbH, Version 0.60, Edition 07/2011, 13.07.2011 (confidential document)

[8] CardOS V4.4, User Guidance, Atos IT Solutions and Services GmbH, Version 0.60, Edition 07/2011, 13.07.2011 (confidential document)

[9] CardOS V4.4 (CNS), Sequences of the personalisation scripts and ADS scripts, Atos IT Solutions and Services GmbH, zip file “CardOS_V44_SigG_Personalization_Scripts_20110707.zip” (confidential document)

[10] CardOS V4.4 (CNS), Packages & Release Notes, Atos IT Solutions and Services GmbH, Edition 07/2011, 13.07.2011 (confidential document)

[11] CardOS 4.4 (CNS) and CardOS DI V4.2C CNS, Life-cycle support, Atos IT Solutions and Services GmbH, Version 0.50, Edition 07/2011, 13.07.2011 (confidential document)

[12] Geeignete Algorithmen zur Erfüllung der Anforderungen nach § 17 Abs. 1 bis 3 SigG in Verbindung mit Anlage 1 Abschnitt I Nr. 2 SigV, Veröffentlicht am 04. Februar 2010 im Bundesanzeiger Nr. 19, S. 426, vom 20. Mai 2011, Bundesnetzagentur für Elektrizität, Gas, Telekommunikation, Post und Eisenbahnen