Bundesamt
für Sicherheit in der
Informationstechnik

Assurance Continuity Maintenance Report

BSI-DSZ-CC-0833-2013-MA-01

CardOS V5.0 with Application for QES, V1.0

from

Atos IT Solutions and Services GmbH

SOGIS
Recognition Agreement

The IT product identified in this report was assessed according to the *Assurance Continuity: CCRA Requirements,* version 2.1, June 2012 and the developer's 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-0833-2013.

The certified product itself did not change. The changes are related to an updated assessment of appropriateness of cryptographic functions.

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 using the CC assurance class AVA has not been re-assessed in the course of this maintenance process. Therefore, the overall assurance statement as outlined in the Certification Report BSI-DSZ-CC-0833-2013 dated 26 July 2013 is of relevance and has to be considered by the user's risk assessment and when using the product. Details can be found on the following pages.

This report is an addendum to the Certification Report BSI-DSZ-CC-0833-2013.

Common Criteria
Recognition Arrangement
for components up to
EAL 4

Bonn, 7 July 2017

The Federal Office for Information Security

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

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 V5.0 with Application for QES, V1.0, 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 changes on how to use the product and outlines the security impact of the changes.

The certified product CardOS V5.0 with Application for QES, V1.0 itself did not change.

The changes are related to the scope and method on how to use the product, specifically as a qualified electronic signature creation device according to EU Regulation [8], [9] or related to national regulations (e.g. German digital signature act [6], [7]).

The product was certified in 2013 stating that the Protection Profile certified under BSI-CC-PP-0059-2009 has been used as a baseline, but with specific deviations / additions. Specific configurations of the product can be used in order to fulfil the requirements of the laws on digital signatures in Germany and Switzerland. For details, refer to the Certification Report [3]. In the meantime this PP certified under BSI-CC-PP-0059-2009 was editorially adapted to the PP-version listed in the EU regulation [9] (see [10]). However, these changes in [10] do not affect the relationship between the product and the PP described above.

When using the product as a qualified electronic signature creation device the guidance documentation as listed in the certification report [3] has to be used, whereby the following constraints have to be taken into account:

- For RSA keys generated on chip only the key length 3072 and 3584 have a security level above 100 bit. When using the product with on chip generated RSA keys and in accordance e.g. to the German catalogue of appropriate algorithms [7] only these key length values provide the required level of security of at least 100 bit.
  If other key length values for RSA keys generated by the product are being used, a specific assessment on the appropriateness supported by Atos and Infineon has to be made within the context of the specific application. The certification service provider has to take appropriate measures to ensure that key length values providing the right level of security are used.
- Constraints on cryptographic algorithms and parameters, e.g. when using the product according to the German catalogue of appropriate algorithms [7], have to be considered. These constraints cover in particular RSA, hash algorithms, random number generation.

Conclusion

The change to the certificate are at the level of limiting the scope and method on how to use the product in addition to the user guidance documentation. The Security Target [4] is still valid for the TOE, but the extended notes on how to use the product need to be considered. Consideration of the nature of the change leads to the conclusion 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 when considering the extended notes listed above.

The resistance to attacks using the CC assurance class AVA has not been re-assessed in the course of this maintenance process. Therefore, the overall assurance statement as outlined in the Certification Report BSI-DSZ-CC-0833-2013 dated 26 July 2013 is of relevance and has to be considered by the user's risk assessment and when using the product.

The IT product identified in the certificate and in this maintenance report is conformant to protection profile EN 419211-2:2013 (see [10]) and is therefore a compliant signature creation device according to Article 30(3.(a)) of Regulation No 910/2014 of the European Parliament and of the Council of 23 July 2014 [8] in combination with the Commissions implementation decision [9].

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.

In addition to the baseline certificate and the items outlined above BSI notes that cryptographic functionalities with a security level of 100 bits or lower can no longer be regarded as secure against attacks with high attack potential without considering the application context. Therefore for this functionality it shall be checked whether the related crypto operations are appropriate for the intended system. Some further hints and guidelines can be derived from the 'Technische Richtlinie BSI TR-02102' (https://www.bsi.bund.de).

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

References

[1] Common Criteria document “Assurance Continuity: CCRA Requirements”, version 2.1, June 2012

[2] Impact Analysis Report, V1.00, 21 June 2017, CardOS V5.0 with Application for QES, V1.0 and CardOS V5.3 QES, V1.0 (confidential document)

[3] Certification Report BSI-DSZ-CC-0833-2013 for CardOS V5.0 with Application for QES, V1.0 from Atos IT Solutions and Services GmbH, V1.0, 26 July 2013, Bundesamt für Sicherheit in der Informationstechnik

[4] Security Target BSI-DSZ-CC-0833-2013, Rev. 2.00, 27 March 2013, Security Target 'CardOS V5.0 with Application for QES V1.0', Atos IT Solutions and Services GmbH

[5] Gesetz über die Rahmenbedingungen für elektronische Signaturen (Signaturgesetz - SigG) in der Fassung vom 16. Mai 2001 (BGBl. Jahrgang 2001 Teil I Nr. 22) zuletzt geändert durch Artikel 4 Absatz 106 des Gesetzes vom 18. Juli 2016 (BGBl. I S. 1666)

[6] Verordnung zur elektronischen Signatur (Signaturverordnung - SigV) in der Fassung vom 16. November 2001 (BGBl. Jahrgang 2001 Teil I Nr. 59) zuletzt geändert durch Artikel 4 Absatz 106 des Gesetzes vom 18. Juli 2016 (BGBl. I S. 1666)

[7] Bekanntmachung zur elektronischen Signatur nach dem Signaturgesetz und der Signaturverordnung (Übersicht über geeignete Algorithmen) vom 7. Dezember 2016, Bundesnetzagentur für Elektrizität, Gas, Telekommunikation, Post und Eisenbahnen

[8] REGULATION (EU) No 910/2014 OF THE EUROPEAN PARLIAMENT AND OF THE COUNCIL of 23 July 2014 on electronic identification and trust services for electronic transactions in the internal market and repealing Directive 1999/93/EC

[9] COMMISSION IMPLEMENTING DECISION (EU) 2016/650 of 25 April 2016, laying down standards for the security assessment of qualified signature and seal creation devices pursuant to Articles 30(3) and 39(2) of Regulation (EU) No 910/2014 of the European Parliament and of the Council on electronic identification and trust services for electronic transactions in the internal market

[10] BSI-CC-PP-0059-2009-MA-02, Common Criteria Protection Profile: EN 419211-2:2013 - Protection profiles for secure signature creation device - Part 2: Device with key generation, CEN/ISSS - Information Society Standardization System, 18 May 2013

The standard is available at the Technical Bodies of the European Committee for Standardization (CEN): https://standards.cen.eu/
For Germany, it can be obtained at Beuth Verlag, DIN's publishing house: http://www.beuth.de/

[11] PKCS #1 v2.2: RSA Cryptography Standard, 27 October 2012, http://www.emc.com/emc-plus/rsa-labs/pkcs/files/h11300-wp-pkcs-1v2-2-rsa-cryptography-standard.pdf

End of document