Bundesamt
für Sicherheit in der
Informationstechnik

Assurance Continuity Maintenance Report

BSI-DSZ-CC-0603-2010-MA-01
MICARDO V3.5 R1.0 eHC V1.2 QES V1.0
from
Morpho e-Documents Division

Common Criteria Recognition
Arrangement
for components up to EAL4

Common Criteria

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-0603-2010.

The change to the certified product is at the level of the file system of the product due to the updated Gematik specification. The change has no effect on assurance. The identification of the maintained product is indicated by an extension of the product name.

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-0603-2010 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-0603-2010.

Bonn, 30 May 2011

SOGIS
IT SECURITY CERTIFIED
INFORMATION TECHNOLOGY SECURITY
MUTUAL RECOGNITION AGREEMENT

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

The vendor for the MICARDO V3.5 R1.0 eHC V1.2 QES V1.0, Morpho e-Documents Division, 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 MICARDO V3.5 R1.0 eHC V1.2 QES V1.0 was changed due to the updated Gematik specification. The changes to the application layout (file system) of the product fulfil the requirements of the updated Gematik specification [12], [13] and the updated PP version [11]. An additional change has been made to some access rules to clarify some ambiguity in the Gematik specification as well as to introduce an improvement of the Image Versioning Scheme. Configuration Management procedures required a change in the product identifier. Therefore the TOE name was changed to MICARDO V3.5 R1.0 eHC V1.2 QES V1.0.

Please note that the chip platform certificate has changed from BSI-DSZ-CC-0410-2007 to BSI-DSZ-CC-0680-2010 [8], [9], [10]. Please be aware that this is only possible for a Maintenance procedure because the actual chip has not changed. The reason for the chip re-certification was the inclusion of an additional site and the re-assessment of the chip.

Conclusion

The change to the TOE is at the level of the file system of the product due to the updated Gematik specification. The change has no effect on assurance. As a result of the changes the configuration list for the TOE has been updated [6].

The Security Target [4], the Security Target Lite [5], the Data Sheet [7] and the Configuration List [6] were updated.

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-0603-2010 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.

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).

In addition to the baseline certificate BSI notes that cryptographic functionalities with a security level of 80 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 CCIMB-2004-02-009 “Assurance Continuity: CCRA Requirements”, version 1.0, February 2004

[2] Impact Analysis Report MICARDO v3.5 R1.0 eHC v1.2 QES v1.0, version V1.01, 26.05.2011 (confidential document)

[3] Certification Report BSI-DSZ-CC-0603-2010 for MICARDO V3.5 R1.0 eHC V1.0 (QES), 11.06.2010, Bundesamt für Sicherheit in der Informationstechnik (BSI)

[4] Security Target – MICARDO V3.5 R1.0 eHC V1.2 QES V1.0, Version V1.01, Sagem ORGA GmbH (Morpho e-Documents) (confidential document)

[5] Security Target Lite – MICARDO V3.5 R1.0 eHC V1.2 QES V1.0, Version V1.00, Sagem ORGA GmbH (Morpho e-Documents)

[6] Configuration List – MICARDO V3.5 R1.0 eHC V1.2 QES V1.0, Version V1.01, Sagem ORGA GmbH (Morpho e-Documents)

[7] Data Sheet – MICARDO V3.5 R1.0 eHC V1.2 QES V1.0, Version V2.00, Sagem ORGA GmbH (Morpho e-Documents)

[8] Certification Report for NXP Secure Smart Card Controller P5CD080V0B, P5CC080V0B, P5CN080V0B and P5CC073V0B each with specific IC Dedicated Software, BSI-DSZ-CC-0680-2010, 03.11.2010, Bundesamt für Sicherheit in der Informationstechnik (BSI)

[9] ETR for composition, NXP P5CD080V0B Secure 8-bit Smart Card Controller, BSI-DSZ-CC-0680, T-Systems GEI GmbH, Version 1.36, 29.10.2010 (confidential document)

[10] Security Target Lite – P5CC080V0B, BSI-DSZ-CC-0680-2010, Revision 1.9, 14.07.2010, NXP Semiconductors GmbH

[11] Protection Profile – electronic Health Card (eHC) – elektronische Gesundheitskarte (eGK), BSI-CC-PP-0020-V2-2007-MA-03, Version 2.61, 19.04.2011, Bundesamt für Sicherheit in der Informationstechnik (BSI)

[12] Spezifikation der elektronischen Gesundheitskarte, Teil 1: Spezifikation der elektrischen Schnittstelle, Version 2.2.0, 20.03.2008, including SRQ supplements 1070, 1069, 1067, 1066, 1065, 1064, 1047, 0959, 0842, 0841, 0840, 0838, 0837, 0836, 0835, 0834, 0833, 0832, 0831, 0829, 0828, 0827, 0826, 0825, 0824, 0823, 0822, 0821, 0820, 0819, 0818, 0817, 0816, 0815, 0814, 0810, 0809, 1154, 1153, 1094 (as specified in "Dokumentenlandkarte Releasestand 0.5.3 – Rollout eGK Festlegung der Versionsstände", gematik, Version: 1.0.0, 11.04.2011), Gematik

[13] Spezifikation der elektronischen Gesundheitskarte, Teil 2: Grundlegende Applikationen, Version 2.2.0, 25.03.2008, including SRQ supplements 1030, 950, 949, 948, 947, 946, 945, 944, 890, 889, 888, 887, 886, 885, 884, 883, 882, 881, 1085 (as specified in "Dokumentenlandkarte Releasestand 0.5.3 – Rollout eGK Festlegung der Versionsstände", gematik, Version: 1.0.0, 11.04.2011), Gematik