Bundesamt
für Sicherheit in der
Informationstechnik

Assurance Continuity Maintenance Report

BSI-DSZ-CC-0774-2011-MA-01

Renesas Cryptographic Library v5126 on Renesas RS47X smartcard integrated circuit v02

from

Renesas Electronics Europe Ltd.

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-0774-2011.

The change to the certified product is at the level of a minor change of the underlying IC platform. 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.

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-0774-2011 dated 22 September 2011 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-0774-2011.

Bonn, 8 December 2011

SOGIS IT SECURITY CERTIFIED

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 Renesas Cryptographic Library v5126 on Renesas RS47X smartcard integrated circuit v02, Renesas Electronics Europe Ltd., 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 underlying platform RS47X smartcard integrated circuit has been changed due to certain optimisations from version 01 to version 02. These changes have been accepted as a minor change and version 02 of the product has been accepted under certificate maintenance (see [7]). Since the Renesas Cryptographic Library v5126 on Renesas RS47X smartcard integrated circuit v02 is a composite product of the IC platform plus cryptographic software, configuration management procedures required a change in the product identifier. Therefore the version number changed from Renesas Cryptographic Library v5126 on Renesas RS47X security integrated circuit v01 to Renesas Cryptographic Library v5126 on Renesas RS47X smartcard integrated circuit v02.

Conclusion

The change to the TOE is at the level of the underlying platform. The change has no effect on assurance. As a result of the change the configuration list for the TOE has been updated [5].

The Security Target was editorially updated [4].

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-0774-2011 dated 22 September 2011 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.

Some security measures are partly implemented in the hardware and require additional configuration or control or measures to be implemented by the IC Dedicated Support Software or Embedded Software.

For this reason the TOE includes guidance documentation which contains guidelines for the developer of the IC Dedicated Support Software and Embedded Software on how to securely use the microcontroller chip and which measures have to be implemented in the software in order to fulfil the security requirements of the Security Target of the TOE.

In the course of the evaluation of the composite product or system it must be examined if the required measures have been correct and effectively implemented by the software. Additionally, the evaluation of the composite product or system must also consider the evaluation results as outlined in the document ETR for composite evaluation [6].

According to the scheme rules, evaluation results outlined in the document ETR for composite evaluation as listed above can usually be used for composite evaluations building on top, as long as the document ETR for composite evaluation is not older than one year and an attack assumed to be not feasible within the scope of these evaluations has not been performed successfully.

Additional Note: The strength of the cryptographic algorithms was not rated in the course of the product certification and this maintenance procedure (see BSIG[1] Section 9, Para. 4, Clause 2).

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

1 Act on the Federal Office for Information Security (BSI-Gesetz - BSIG) of 14 August 2009, Bundesgesetzblatt I p. 2821

References

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

[2] IAR for RS47X, Renesas Electronics Corporation, 16 November 2011 (confidential document)

[3] Certification Report BSI-DSZ-CC-0774-2011 for Renesas Cryptographic Library v5126 on Renesas RS47X security integrated circuit version 01 from Renesas Electronics Corporation, Bundesamt für Sicherheit in der Informationstechnik, 22 September 2011

[4] RCL on RS47X Version 02 Security Target -Public Version-, Revision 1.2, Renesas Electronics Corporation, 15 November 2011

[5] RCL on RS-4 Generic Configuration List, Version 5705, Date: 15.11.2011, Document Number D008710_ALC, Renesas Electronics Europe Ltd. (confidential document)

[6] ETR for composite evaluation according to AIS 36 for the Product Renesas Cryptographic Library v5126 running on RS47X, Version 1.0, July 22, 2011, T-Systems GEI GmbH (confidential document)

[7] Assurance Continuity Maintenance Report, BSI-DSZ-CC-0735-2011-MA-01 Renesas RS47X smartcard integrated circuit, version 02, 10 November 2011, Bundesamt fuer Sicherheit in der Informationstechnik