Bundesamt
für Sicherheit in der
Informationstechnik

Assurance Continuity Maintenance Report

BSI-DSZ-CC-0632-2011-MA-01

SLE88CFX4001P / m8835 including optional RSA2048 and SHA-2 Library

from

Infineon Technologies AG

Common Criteria

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 2.1, June 2012 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-0632-2011 updated by a re-assessment on 16 December 2013.

The certified product itself did not change. The changes are related to an update of the user guidance.

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-0632-2011 dated 16.12.2011 updated by a re-assessment on 16.12.2013 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-0632-2011.

Bonn, 21 February 2014

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 SLE88CFX4001P / m8835 including optional RSA2048 and SHA-2 Library, 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 changes are related to an update of the user guidance [6].

Conclusion

The change to the TOE is at the level of guidance documentation. 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 [4] is still valid for the TOE.

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-0632-2011 dated 16.12.2011 updated by a re-assessment on 16.12.2013 is of relevance and has to be considered when using the product. As a result of this re-assessment, the documents [7] and [8] are the current versions of the ETR for composite evaluation and the ETR itself.

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 [7].

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 eighteen months 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). But Cryptographic Functionalities with a security level of lower than 100 bits can no longer be regarded as secure without considering the application context. Therefore for this functionalities 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). Any Cryptographic Functionality that is marked in column '*Security Level above 100 Bits*' of the following table with '*no*' achieves a security level of lower than 100 Bits (in general context).

Purpose	Cryptographic Mechanism	Standard of Implementation	Key Size in Bits	Security Level above 100 Bits
Cryptographic Primitive	SHA-1	FIPS 180-3 (SHA)	None	no
	SHA-256	FIPS 180-3 (SHA)	None	yes
	AES	FIPS197 (AES)	k|=128	yes
	DES in ECB and CBC mode	FIPS 46-3 (DES), SP 800-38A (ECB, CBC)	|k|=56, 112	no
	TDES in ECB mode	FIPS 46-3 (DES), SP 800-38A (ECB)	|k|=168	no
	TDES in CBC mode	FIPS 46-3 (DES), SP 800-38A (CBC)	|k|=168	yes
	RSA encryption and decryption	Applied Cryptography, Second Edition, Protocols, Algorithms, and Source Code in C, Bruce	moduluslength= 512-1326	no

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

Purpose	Cryptographic Mechanism	Standard of Implementation	Key Size in Bits	Security Level above 100 Bits
		Schneier, Section 19.3 RSA (page 467). (RSA)		
	RSA encryption and decryption (RSAEP, RSADP)	PKCS#1 v2.1 (RSA)	Moduluslength= 512- 1975	no
	RSA encryption and decryption (RSAEP, RSADP)	PKCS#1 v2.1 (RSA)	moduluslength= 1976 - 2276	yes
	RSA signature gerenation (RSASP1)	PKCS#1 v2.1 (RSA)	Moduluslength= 512- 1088	no
	RSA signature verification (RSAVP1)	PKCS#1 v2.1 (RSA)	moduluslength= 512 - 1975	no
	RSA signature verification (RSAVP1)	PKCS#1 v2.1 (RSA)	moduluslength= 1976 - 2276	yes

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] IAR for M8835 B18 including optional Software Libraries RSA2048 – SHA-2 Library, version 1.0, dated 2014-01-07 (confidential document)

[3] Certification Report BSI-DSZ-CC-0632-2011 for SLE88CFX4001P/m8835b18, SLE88CFX4003/m8837b18, SLE88CFX3521P/m8857b18 and SLE88CFX2921P/m8859b18 all including optional RSA2048 and SHA-2 Library from Infineon Technologies AG, Bundesamt für Sicherheit in der Informationstechnik, 16 December 2011

[4] Security Target BSI-DSZ-CC-0632-2011, Version 2.0, 26 October 2011, SSLE88CFX4001P / m8835 includung optional RSA2048 and SHA-2 Library Security Target, Infineon Technologies AG

[5] Configuration list for the TOE, Version 1.6, 6 July 2011, SLE88CFX4001P / m8835 Configuration Management Scope (confidential document)

[6] SLE88CFXxxxxP PSL & Security Reference Manual, Dec 2013, Infineon Technologies AG

[7] ETR for composite evaluation, Infineon Smart Card IC SLE88CFX4001P/m8835, version 2.04, dated 16.12.2013, T-Systems GEI GmbH

[8] ETR, Infineon Smart Card IC SLE88CFX4001P/m8835, version 2.04, dated 16.12.2013, T-Systems GEI GmbH