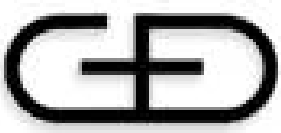
SERMA
SAFETY & SECURITY

MIFARE Security Renewal Certification Report

ARN-2017-001-R01

Product ref. : Sm@rtSIM CX Hercules Variant 14 on ST Microelectronics ST33G1M2 rev F

Developer /
Sponsor:



Giesecke+Devrient Mobile Security GmbH
C/114, 27, Polígon Pratenc
El Prat de Llobregat (Barcelona)
E-08820
SPAIN

This page is intentionally left blank

Document and project identification

Name	Value
Document title:	ARN-2017-001-R01 MIFARE Security Renewal Certification Report
Reference/version	MIFARE_ARN_2017_001_R01 / 1.0
Developer:	Giesecke+Devrient Mobile Security GmbH
Sponsor:	Giesecke+Devrient Mobile Security GmbH
Evaluation Lab:	UL Transaction Security
Certification Authority:	SERMA SAFETY & SECURITY ITSEF
Registration Number	PRN-2017-001
Approval Number	ARN-2017-001-R01

Edition

Edited by:	Renaud SQUELARD
Function:	Project Leader

Approval

Approved by:	Valérie SAULE Magali METAIS	Date: 25/07/2019
Function:	ITSEF Quality Manager	Visa: Signed original

Diffusion

Copy number	Name:	Company
1/2	Eduard MAYOR	Giesecke+Devrient Mobile Security GmbH
2/2	Renaud SQUELARD	SERMA ITSEF

Confidentiality and copyright notice

Table Of Contents

1 Introduction

1.1 Report information

1 This document is the **MIFARE Security Renewal Certification Report** of the Sm@rtSIM CX Hercules Variant 14 product developed by Giesecke+Devrient Mobile Security GmbH and masked on the integrated circuit ST33G1M2 rev F from ST Microelectronics.

2 The sponsor of this evaluation is Giesecke+Devrient Mobile Security GmbH.

3 This MIFARE Evaluation was performed by UL Transaction Security ITSEF.

4 This Certification is performed by SERMA SAFETY & SECURITY ITSEF (no sub-contracting) under the quotation 19-0240.

5 This report only concerns the objects submitted to analysis.

1.2 Product identification

6 The evaluated revision of the product components is provided in the following table:

Licensee Registration Number	PRN-2017-001
LSF date	June 17, 2019
Type of testing	Delta
Product name	Sm@rtSIM CX Hercules Variant 14
Product version	Variant 14
Product build date	-
Form factor(s)	ISO/IEC 7810 ID-1 ETSI TS 102 221 Mini-UICC
Communication protocols	Contact: T=0 and T=1 (ISO/IEC 7816-3) NFC: SWP (ETSI TS 102 613) / HCI (ETSI TS 102 622) HCI contactless: Type A or Type B (ISO/IEC 14443)
Platform name and version	Sm@rtSIM CX Hercules Variant 14
Platform build date	-
Platform PCN	PCN0090.10
PCN Issue date – Expiry date	14 July 2014 – 14 July 2019
Chip manufacturer	ST Microelectronics
Chip model and EMVCo ICCN#	ST33G1M2 rev F - ICCN0202
ICCN Issue date – Expiry date	14 July 2014 – 14 July 2020
MIFARE type	MIFARE DESFire EV1
Patch information	N.A

7 The list of documents used for this certification report is given in chapter “References“.

1.3 Contact

1.3.1 Certification Authority

8 The SERMA SAFETY & SECURITY ITSEF is a test laboratory accredited by the French Accreditation Committee (COFRAC), according to the NF EN ISO/CEI 17025 standard. This accreditation initially acquired in February 2000 (accreditation number 1-1061 for SERMA TECHNOLOGIES ITSEF) has been transferred on January 1st 2016 (accreditation number 1-6098) to SERMA SAFETY & SECURITY, fully owned by SERMA TECHNOLOGIES. This accreditation is maintained by a yearly audit. Some activities reported in this document are not under the accreditation and are identified by the symbol *.

9 The SERMA SAFETY & SECURITY ITSEF is licensed as an «Information Technology Security Evaluation Facility» by the ANSSI since July 2000 (initially for SERMA TECHNOLOGIES ITSEF then transferred on January 1st 2016). This agreement has been renewed on July 2018 (number 15741).

10 The SERMA SAFETY & SECURITY ITSEF can lead vulnerability analyses up to a high resistance level (AVA_VAN.5 according to the Common Criteria) and can provide training, consulting and evaluations associated to Common Criteria.

11 The ITSEF has been approved by MasterCard Worldwide, VISA, American Express, JCB and EMVCo for security expertises of smart cards within the CAST, VCSP, AMEX, JCB and EMVCo security evaluation programs.

12 The ITSEF has also been approved by NXP for security expertises of smart cards within the MIFARE security scheme.

13 Moreover, the ITSEF has been approved by PCI SSC for security expertises of POI and HSM within the PCI-PTS program.

14 The SERMA SAFETY & SECURITY CST Laboratory is accredited by the National Voluntary Laboratory Accreditation Program for ITST – Cryptographic and Security Testing under the code 200977-0. The SERMA SAFETY & SECURITY CST Laboratory can lead test activities on software and hardware cryptographic module compliant to FIPS 140-2 standard, up to level 4.

15 The ITSEF can also perform technical expertises outside these schemes.

SERMA ITSEF: Certification Authority Laboratory

Address:	14 rue Galilée – CS 10071 – 33608 PESSAC Cedex – FRANCE		
Contact:	Renaud SQUELARD		
Tel:	+33 5 33 20 65 15	Fax:	+33 5 57 26 08 98
e-mail:	r.squelard@serma.com		

1.3.2 Sponsor and developer

Product Developer:

Name:	Giesecke+Devrient Mobile Security GmbH		
Address:	Giesecke+Devrient Mobile Security GmbH C/114, 27, Polígon Pratenc El Prat de Llobregat (Barcelona) E-08820 SPAIN		
Contact:	Eduard MAYOR		
Tel:	-	Fax:	-
e-mail:	eduard.mayor@gi-de.com		

1.3.3 Evaluation Lab

Evaluation Laboratory:

Name:	UL Transaction Security		
Address:	Unit 2 Horizon Wade Road, Kingsland Business Park Basingstoke, RG24 8AH, UK		
Contact:	Kat ROBERTS		
Tel:	-	Fax:	+44 (0)1256 312001
e-mail:	kat.roberts@ul.com		

1.4 Work schedule and performance

1.4.1 Evaluation milestones

Milestones	Date
Scoping meeting	May 29, 2019
Test Plan review meeting	May 29, 2019
Tests campaign	June 2019
Evaluation Report Lite	July 04, 2019
Certification report	July 17, 2019

2 Evaluated configuration

2.1 Product description (from UL)

16 The Target of Evaluation (TOE), defined as Sm@rtSIM CX Hercules Variant 14, is composed of:

- **MDF-EV1**, Giesecke and Devrient GmbH's implementation of MIFARE DESFire EV1 compliant with MIFARE DESFire EV1, Rev. 3.6, 9 February 2011 134036,
- **M4Mv2**, Giesecke and Devrient GmbH's implementation of MIFARE4Mobile V2, compliant with MIFARE4Mobile V2,
- **ST33G1M2 Rev. F** hardware IC, a microcontroller known to be independently evaluated under EMVCo scheme (ICCN0202) and with a recent [SER] issued on 14 Feb 2014 and expiry date on 14 Feb 2020. Also approved under the Common Criteria Scheme with SMD_ST33G_ST_13_001 certificate,
- **Sm@rtSIM CX Hercules Variant 14** GlobalPlatform (Open configuration). The EMVCo Open Platform Sm@rtSIM CX Hercules Variant 14 is certified with PCN0090.10.
- Note that this composition model relies on the fact that **MDF-EV1** and **M4Mv2** coexist and use most of the modules from the EMVCo Open Platform **Sm@rtSIM CX Hercules Variant 14** which was fully evaluated by UL Transaction Security Lab. The EMVCo Open Platform Sm@rtSIM CX Hercules Variant 14 is certified with PCN0090.10.

2.2 Product identification

17 Evaluated product identification is provided at §1.2

2.3 Scope

18 The following elements are in the scope of this MIFARE evaluation:

- The Giesecke and Devrient GmbH implementation of MIFARE DESFire EV1, referenced MDF-EV1, and MIFARE4Mobile V2 referenced M4Mv2, with product name Sm@rtSIM CX Hercules Variant 14, is native application embedded on the hardware platform ST33G1M2 Rev. F

3 Evaluation history

3.1 Introduction

19 In the context of this MIFARE Security Evaluation Scheme, UL was selected by Giesecke+Devrient Mobile Security GmbH as the Evaluation Lab which performed the tests campaign concluded by an Evaluation Report and SERMA SAFETY & SECURITY ITSEF as the Certification authority Lab which analyzed and validated the submitted tests plan and tests results through Evaluation Report_lite received from Evaluation Lab.

3.2 Evaluation steps

20 This MIFARE Security Evaluation has consisted in the following main phases:

Milestones	Date
G&D License Submission Form to NXP (original)	January 09, 2017
NXP registration of product as: PRN-2017-001	January 11, 2017
G&D License Submission Form to NXP (for renewal)	May 14, 2019
NXP registration of approval as: ARN-2017-001-R01	June 17, 2019
G&D selection of Evaluation Lab: UL TRANSACTION SECURITY	/
G&D selection of Certification Authority Lab: SERMA SAFETY & SECURITY ITSEF	/
UL and SERMA scope of approval:	May 29, 2019
UL and SERMA penetration test plan approval	May 29, 2019
UL test campaign and test report	June 2019
UL report-lite analysis and approval by SERMA	July 04, 2019

21 No particular event occurred during those different phases.

3.3 Evaluation results

22 The test campaign, lead by UL and summarized in Report-Lite [ERL], concludes that the Sm@rtSIM CX Hercules Variant 14 product, in its evaluated configuration, is assessed resistant to 'High' attack potential according to [JIL_AP].

23 There are two tests performed on MIFARE DESFire EV1 security evaluation as it is a renewal. UL has investigated for new attack pathes and verification testing.
The Sm@rtSIM CX Hercules Variant 14 product was originally evaluated (ARN-2017-001) by UL (report referenced [ERL11627221JD01B]).

4 Evaluation summary

4.1 Evaluation reference

24 This document is the **MIFARE Security Renewal Certification Report** of the Sm@rtSIM CX Hercules Variant 14 product developed by Giesecke+Devrient Mobile Security GmbH and masked on the integrated circuit ST33G1M2 rev F from ST Microelectronics.

Registration Number	PRN-2017-001
Approval Number	ARN-2017-001-R01
Product name and version	Sm@rtSIM CX Hercules Variant 14
Platform name and version	Sm@rtSIM CX Hercules Variant 14
Platform build date	-
Platform PCN	PCN0090.10
IC name and version	ST33G1M2 rev F
ICCN	ICCN0202 issued 14 Feb 2014 and expiring 14 Feb 2020
MIFARE type	MIFARE DESFire EV1+ MIFARE4Mobile

4.2 Statement of the attack potential achieved

25 As a general conclusion, in the scope of the present evaluation, **the product is considered resistant to a "High" attack potential**, as defined by the JIL document "Application of attack potential to smart cards", [JIL_AP]**.**

4.3 Evaluation conclusion

26 Regarding the vulnerability analysis conclusions provided by UL Transaction Security (Evaluation Lab) in Evaluation Report-Lite (ERL_12793297JD01B rev B; issued on July 04, 2019) for which the Sm@rtSIM CX Hercules Variant 14 product, embedding MIFARE DESFire EV1 and MIFARE4Mobile, is assessed resistant to a "High" attack potential.

27 SERMA ITSEF (CA Lab) agrees with the conclusion provided by UL Transaction Security (Evaluation Lab) regarding the penetration tests campaign objective of Sm@rtSIM CX Hercules Variant 14 product, which did not highlight exploitable vulnerability.

28 Therefore, SERMA ITSEF (Certification Authority Lab) confirms that:

Sm@rtSIM CX Hercules Variant 14 product, embedding MIFARE DESFire EV1 and MIFARE4Mobile, 'Pass' the targeted NXP MIFARE Security Evaluation, providing the product follows the platform security guidance.

5 References

5.1 Evaluation deliverables

29 The following set of deliverables is the reference for the project:

Reference	Deliverable name	Version or delivery date	Developer reference
[LSF]	Licensee Submission Form	June 17, 2019	ARN_2017_001_R01
[PTP]	Penetration Test Plan of SkySIM CX Hercules Variant 14 from UL Transaction Lab	May 22, 2019	ERL_12793297JD01A_TestPlan
[ERL]	Evaluation Report Lite from UL Transaction Lab	July 04, 2019	ERL_12793297JD01B

5.2 Evaluation documentation

30 The following documents have been used during the MIFARE evaluation phase by the Evaluation Lab (UL):

Reference	Document	Version / Date
[SecGuide]	MIFARE Plus and DESFire, Security Evaluation Scheme,	Rev. 2.00 9 December 2016
	MIFARE DESFire EV1/EV2, Security Analysis for Evaluation Scheme	Rev. 1.03 - 05 October 2016
[IC DataSheet]	ST33G Platform ST33G1M2: Secure MCU with 32 - bit ARM SecureCore SC300 CPU - and high density Flash memory,	DS_33G1M2, v6, May 2015
[IC SecGuide]	Application note ST33G and ST33H Secure MCU platforms Security guidance.	Rev.5.0 February 2016
[SIR]	EMVCo Shared Evaluation Report for IC, project: ICCN0202, Surv2017_SER_IC	Rev. 2.0 February 22, 2017
[Platform SecGuide]	SkySIM CX Hercules Security_Guidelines.	December 20, 2016
[SER]	EMVCo Security Evaluation Shared Evaluation Report (SER) Platform Approval SkySIM CX Hercules Variant 14,	January 24, 2017
[MFD]	MIFARE DESFire EV1, Rev. 3.6 ,134036	February 9, 2011

5.3 External documentation

Reference	Document	Version
[NXP_SG]	MIFARE Plus and DESFire - Security Evaluation Scheme	Rev 2.00, December 9, 2016
[DESFire]	MIFARE DESFire EV1/EV2 - Security Analysis for Evaluation Scheme	Rev 1.03, October 5, 2016
[JIL_AP]	JIL - Application of attack potential to Smart Cards	Version 3.0, April 2019

6 Version History

Version	Nature of modifications	Author	Approval	Date
1.0	Creation	R. SQUELARD	V. SAULE	25/07/2019

Remark: the latest report version cancels and replaces the previous ones.