GLOBALPLATFORM®
THE STANDARD FOR SECURE DIGITAL SERVICES AND DEVICES

Certificate of Security Evaluation

Upteq NFC422 v1.0

Certification Number:	GP-SE-2019/02	**Product Name:**	Upteq NFC422 v1.0
Issuance Date:	Sept. 9th 2019	**Configurations:**	---
Sponsor:	Gemalto (Thales Group)	**Platform / Developer:**	Upteq NFC422 v1.0 / Gemalto (Thales Group)
		IC / Developer:	S3NSEN4 Rev. 1 / Samsung
Protection Profile:	GSM Association SGP.25 - Embedded UICC for Consumer Devices Protection Profile, version 1.0	**Product Type:**	☑ eUICC ☐ embedded LPA ☑ device LPA
PP-Modules:	☐ LPAe		
Certification Type:	☑ Unrestricted ☐ Restricted	**Evaluation Type:**	☑ Full ☐ Delta ☐ Fast-track ☐ Reassessment
Certification Report:	GP-SE-2019/02-CR	**Security Evaluation Lab:**	UL

This GlobalPlatform Security Evaluation Product Certificate ("Certificate") remains valid only while the version of the product specified above is posted on the GlobalPlatform website, and means only that such product version has demonstrated sufficient conformance with applicable Security Requirements, determined by a GlobalPlatform-accredited third-party laboratory evaluation. This Certificate applies only to the product version specified, does not constitute an endorsement or warranty by GlobalPlatform, and is subject to the additional terms, conditions and restrictions set forth in the attached GlobalPlatform Security Evaluation Secretariat Certification Report.

GlobalPlatform, Inc.

Kevin Gillick, Executive Director

GLOBALPLATFORM®
CERTIFIED SE

544 Hillside Road | Redwood City, CA 94062 | secretariat@globalplatform.org | www.globalplatform.org

GLOBALPLATFORM®
THE STANDARD FOR SECURE DIGITAL SERVICES AND DEVICES

GlobalPlatform Security Evaluation Secretariat
Certification Report
GP-SE-2019/02-CR v1.0

Issue date:	2019.09.09
Product:	Upteq NFC422 v1.0
Sponsor:	Gemalto (Thales Group) La Vigie, Avenue du Jujubier, ZI Athelia IV, FRANCE
Developers:	Gemalto (Thales Group) Samsung Electronics Co., Ltd.
Laboratory:	UL Unit 2 Horizon, Wade Road, Kingsland Business Park Basingstoke, Hampshire, RG24 8AH, England
Conformance:	GSM Association SGP.25 - Embedded UICC for Consumer Devices Protection Profile, version 1.0 05-June-2018, BSI-CC-PP-0100 ☐ LPAe PP-Module
Product Type:	eUICC ☐ embedded LPA ☑ device LPA
Evaluation Type:	☑ Full ☐ Delta ☐ Fast-track ☐ Reassessment
Certification Type:	☑ Unrestricted ☐ Restricted

NOTICE

GlobalPlatform, Inc. (“GlobalPlatform”) has received the request of the above listed sponsor(s) (collectively, “Sponsor”) for security certification of the above referenced product version (“Product”). After assessing such request and the security evaluation reports submitted therewith, GlobalPlatform has found reasonable evidence that the Product sufficiently conforms to the claimed eUICC Security Requirements.

GlobalPlatform therefore (a) issues this Certification Report and accompanying Product (Restricted) Certificate for the Product (collectively, the “Certification”), subject to the terms, conditions and restrictions set forth herein, and (b) agrees to include the name of the Sponsor, and name of the developer(s) above listed upon request, as well as the Product on GlobalPlatform’s website in accordance with applicable policies and procedures. Because this Certification is subject to limitations, including those specified herein and certain events of termination, Sponsor and any third parties should confirm that such Certification is current and has not been terminated by referring to the list of certified products published on the GlobalPlatform website (www.globalplatform.org).

CONDITIONS

This Certification (a) only applies to the above referenced Product version, (b) is conditioned upon all necessary agreements having been executed in accordance with GlobalPlatform policy and satisfaction of the requirements specified therein, and shall be effective only if such agreements and requirements satisfaction continue to be in full force and effect, (c) is subject to all terms, conditions and restrictions noted herein, (d) is issued solely to the submitting Sponsor and solely in connection with the Product and (d) may not be assigned, transferred or sublicensed, either directly or indirectly, by operation of law or otherwise.

Only a product with valid GlobalPlatform Certification may claim to be a ‘GlobalPlatform Certified Product’.

GlobalPlatform may revoke this Certification at any time in its sole discretion, pursuant to the terms of this Certificate Report and the GlobalPlatform SE Security Certification Process and related agreements. Accordingly, no third party should rely solely on this Certification, and continued effectiveness of this Certification should be confirmed against the applicable list of certified Products on the GlobalPlatform website. Even though GlobalPlatform has certified the Product, the Sponsor shall be responsible for compliance with all applicable specifications and Security Requirements and for all liabilities resulting from the use or sale of the Product.

In addition to GlobalPlatform’s rights to now communicate this Certification, upon the Sponsor’s authorization, you may now communicate that the Product listed above is GlobalPlatform certified (using the same or similar terms); provided, however, that (a) you also communicate all terms, conditions and restrictions set forth herein, (b) when identifying that the Product has been GlobalPlatform certified (using the same or similar terms), you provide specific details identifying the product and version that has been certified and not release a general statement implying that all of your products (or product versions that have not been certified) are certified, (c) your communication in no way suggests that by using your products that a vendor will be guaranteed by GlobalPlatform, (d) your communication in no way implies that you are a preferred product vendor of GlobalPlatform or that you or the Product are endorsed by GlobalPlatform, and (e) all written communications referring to GlobalPlatform’s certification shall contain the following legend:

"GlobalPlatform issuance of a certificate for a given product means only that the product has been evaluated in accordance and for sufficient conformance with the then current version of the claimed Security Requirements, as of the date of evaluation. GlobalPlatform's certificate is not in any way an endorsement or warranty regarding the completeness of the security evaluation process or the security, functionality, quality or performance of any particular product or service. GlobalPlatform does not warrant any products or services provided by third parties, including, but not limited to, the producer or vendor of that product and GlobalPlatform certification does not under any circumstances include or imply any product warranties from GlobalPlatform, including, without limitation, any implied warranties of merchantability, fitness for purpose, or non-infringement, all of which are expressly disclaimed by GlobalPlatform. To the extent provided at all, all representations, warranties, rights and remedies regarding products and services which have received GlobalPlatform certification shall be provided by the party providing such products or services, and not by GlobalPlatform, and GlobalPlatform accepts no liability whatsoever in connection therewith."

Contents

Tables

Figures

1 Executive Summary

This document constitutes the Certification Report for the evaluation of the eUICC Product *Upteq NFC422 v1.0*, developed by Gemalto (Thales Group), registered under number GP190006.

Upteq NFC422 v1.0 consists of Gemalto's GlobalPlatform-enabled Java Card open platform, extended with eUICC functionalities, and IC *S3NSEN4 Rev. 1* developed by Samsung Electronics Co., Ltd.

The evaluation has been performed by accredited laboratory UL in Basingstoke (UK).

The evaluation followed a composite approach by focusing on the eUICC-specific functionalities of the Product and by reusing IC's and platform's previous evaluation results. For the IC this stands for Leti's *Evaluation Technical Report (ETR for composition) - CAYUSE5,* which led to EMVCo IC certificate [ICCN0262] and Common Criteria certificate [ANSSI-CC-2019/29]. For the platform this stands for UL's *Security Evaluation Shared Evaluation Report (SER) Platform Approval*, which led to the EMVCo Platform certificate [PCN0168].

The *Evaluation Technical Report, version C [ETR]* presents the results of the evaluation of *Upteq NFC422 v1.0 based on Upteq NFC422 v1.0 eUICC Security Target, version 2.0*. The evaluation determined that:

- the Security Target is conformant with the *Embedded UICC for Consumer Devices Protection Profile* [PP] without the LPAe PP-Module;
- the Product meets the security functional requirements defined in the Security Target and resists to attackers with *high attack potential* provided the platform guidance listed in section 2.2 is applied and the operational environment meets the objectives listed in section 2.6.

The certification determined that the eUICC evaluation has been performed in conformance with the *GlobalPlatform Secure Element / eUICC Evaluation Methodology* [EM]. The certificate is valid provided all the usage restrictions defined in section 4.1 are fulfilled.

2 eUICC Product

2.1 Identification

The Product in this evaluation is *Upteq NFC422 v1.0,* a Java Card/GlobalPlatform-based eUICC developped by Gemalto (Thales Group) on top of Samsung's certified IC:

Product Identification	
Product Name	Upteq NFC422 v1.0
Developers	Gemalto (Thales Group) Samsung Electronics Co., Ltd.
Product Type	eUICC ☐ embedded LPA ☑ device LPA

The Target of Evaluation (TOE) consists of the components that are listed in the following table. The eUICC does not embed the LPA module, which is hosted by the device (LPAd).

TOE Components Identification		**Certificate**
IC reference	S3NSEN4 Rev. 1	ICCN0262 (Expiration 18 May 2020) and ANSSI-CC-2019/29
Platform reference	UpTeq NFC4.2.2 v1.0 with crypto library 1.52 v3.5.0.0	PCN0168 (Expiry Date 29 May 2020)
TOE internal identification	5A10890330234221000000000000000061512 (eUICC identifier value)	Not applicable

The TOE internal identification is accessible by using a GET DATA command on tag "5A12" after having selected the E-CASD. The identification elements are the following:

Field	**Value**	**Interpretation**
T	5A	Tag
L	10	Length
Digits 1-2	89	Telecom Industry
Digits 3-5	033	Country Code
Digits 6-8	023	Issuer Identifier
Digits 9-13	42210	Platform & OS Version
Digits 14-18	00000	Additional issuer info
Digits 19-30	000000000615	Identification number
Digits 31-32	12	Check digits

2.2 Documentation

The Security Target (ST) for this evaluation is:

- [ST] *Upteq NFC422 v1.0 eUICC Security Target, version 2.0.*

The ST is compliant with *Embedded UICC for Consumer Devices Protection Profile* [PP] without LPAe PP-Module.

The platform guidance [Platform_GUI] applies to Upteq NFC422 v1.0:

- *D1188231 Guidance for secure application development on UpTeq NFC platforms, Release A13.3b*, August 2018;
- *GPC_GUI_050 GlobalPlatform Card, Composition Model Security Guidelines for Basic Applications,* Version 2.0, November 2014.

2.3 Architecture

The Product is composed of the following elements as shown in Figure 1.:

- S3NSEN4 Rev. 1 IC;
- UpTeq NFC4.2.2 v1.0 with crypto library 1.52 v3.5.0.0 platform composed of:
  - A Java Card system, which provides APIs, handles and executes the applications, implementing [JC305];
  - A GlobalPlatform package which provides a communication interface and allows to securely manage the applications, implementing [GP23];
  - An eUICC environment for network authentication and communication, implementing [SGP21] and [SGP22].

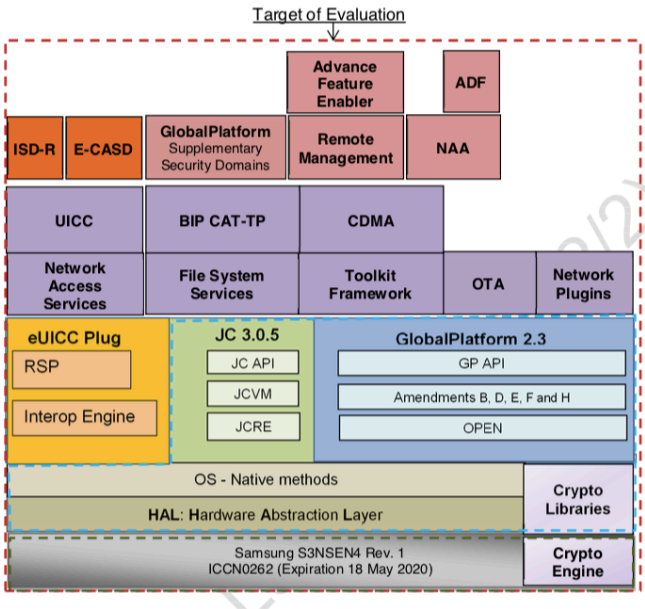

Figure 1: TOE architecture

The TOE is the dotted dark-red rectangle area that is shown in Figure 1. The evaluation reuses the evidence of the EMVCo security evaluation of the open platform (dotted light-blue rectangle area), reference PCN0168 (Expiry Date 29 May 2020), and evidence of the certified IC (dotted dark-green rectangle area), references ICCN0262 (Expiration 18 May 2020) and ANSSI-CC-2019/29.

2.4 Life cycle

The TOE's life cycle is PP-compliant. Site security (Phases a, b and c) has been assessed as part of IC and platform evaluation (cf. [IC SER] and [Platform SER]).

Life cycle phases	Activity
Phase a	Development of IC and eUICC embedded software.
Phase b	IC manufacturing and packaging
Delivery 1	Delivery of packaged IC delivery and eUICC platform to composite product integration
Phase c	Integration of the eUICC platform in the IC
Delivery 2	eUICC delivery to personalizer
Phase d	eUICC personalization (provisioning profiles and operational profiles)
Deliver 3	eUICC delivery to device manufacturer
Phase e	Operational usage (eUICC integration in the Device, registration of eUICC in a given SM-DS; remote provisioning)

2.5 Security Functionality

The eUICC Product Upteq NFC422 v1.0, implements functionalities described in [SGP21] and [SGP22] to managing multiple MNO Profiles. Each Profile is associated with an International Mobile Subscriber Identity (IMSI). The primary function of a Profile is to authenticate the validity of a Device when accessing the network. The Profile is MNO's property, and stores MNO specific information. Only one Profile can be activated at a time. The eUICC behaves as a SIM card for the activated Profile.

The security functionality of the TOE consists of the functionality offered by the underlying Java Card/GlobalPlatform open platform, which protect against logical and physical attacks, and specific functions including:

- Profile management through ISD-R (creation, enabling/disabling, deletion, etc.);
- Storage of credentials and eUICC authentication;
- Telecom Framework with algorithms ([MILENAGE], [TUAK]) used by the Network Access Applications (NAA) included in the Profiles to access the mobile networks;
- OTA communication through SCP80 or SCP81 Secure Channel Protocols.

2.6 Assumptions

The security of the TOE relies on the compliance of the TOE's operational environment with the following objectives set down in [PP]: OE.CI, OE.SM-DPlus, OE.MNO, OE.APPLICATIONS and OE.MNO-SD.

2.7 Clarification of Scope

The TOE does not include the LPA module. It provides the interfaces ES10a, ES10b and ES10c to communicate with the LPA module hosted by the device.

3 Evaluation

3.1 Evaluation Laboratory Identification

The TOE has been evaluated by UL, located Unit 2 Horizon, Wade Road, Kingsland Business Park Basingstoke, Hampshire, RG24 8AH, England.

3.2 Evaluated Configuration

The evaluation addressed one eUICC configuration, as defined in section 2.1. Any deviation from the indicated components' versions brings the TOE outside the evaluated configuration.

The testing of the TOE has been performed on samples of *Upteq NFC422 v1.0*.

3.3 Evidence for composite evaluation

Document reference	**Author, Title, Version and Issue Date**
[Platform GUI]	Gemalto (Thales Group), D1188231 Guidance for secure application development on UpTeq NFC platforms, Release A13.3b, August 2018 GlobalPlatform, GPC_GUI_050 GlobalPlatform Card, Composition Model Security Guidelines for Basic Applications, Version 2.0, November 2014
[IC GUI]	Samsung, Security Application Note for S3M2M5C/S3M2M0C/S3M1M5C/S3NSEN4/S3NSEN3, v0.4, 28 Feb
[Platform SER]	UL, EMVCo Security Evaluation Shared Evaluation Report (SER) Platform Approval, UpTeq NFC422 v1.0, 17 Jul 2019
[IC SER]	Leti, Evaluation Technical Report (ETR for composition) - CAYUSE5, 21 May 2019

3.4 Evaluation Activities

The evaluation of the TOE has been performed on the basis of the following documentation:

- [PP] *Embedded UICC for Consumer Devices Protection Profile*;
- [EM] *GlobalPlatform SE/eUICC Evaluation Methodology*;
- [JIL AM] *JIL Attack Methods for Smartcards and Similar Devices*;
- [JIL AP] *JIL Application of Attack Potential to Smartcards*.

The evaluation activities consisted of:

- Vulnerability analysis of the TOE based on public sources, on developer's documentation and on source code review of the TOE's software components;
- Conformance analysis to IC and Platform Guidance;
- Test plan development;

- Software and hardware-based TOE penetration testing.

The laboratory has also performed the following task:

- Conformity check of the Security Target [ST] against the *Embedded UICC for Consumer Devices Protection Profile* [PP].

3.5 Evaluation Results

The evaluation laboratory documented the evaluation activities and results in the following report:

- [ETR] *Evaluation Technical Report,* number 12775232JD06, *version C*.

The results from penetration testing did not reveal any weakness on the TOE.

The evaluation laboratory determined that:

- The *Upteq NFC422 v1.0 eUICC Security Target, version 2.0* [ST] is conformant with the *Embedded UICC for Consumer Devices Protection Profile* [PP] without LPA PP-Module;
- All the vulnerabilities identified during the evaluation have been fixed;
- The TOE is resistant to attacks performed by an attacker possessing high attack potential [JIL AP] provided the platform guidance is applied and the operational environment meets the objectives listed in section 2.6.

4 Certification

4.1 Usage Restrictions

The user of the certified product *Upteq NFC422 v1.0* must ensure that all the security objectives for the operational environment stipulated for the actors and applications are fulfilled (see section 2.6).

The Security Target [ST] and the platform guidance [Platform GUI] should be distributed or made available to the users of the certified product.

4.2 Conclusion

This certification report confirms that the evaluation of *Upteq NFC422 v1.0* has been performed as required by the GlobalPlatform Evaluation Methodology [EM] and that there is sufficient evidence to affirm that the product meets its Security Target [ST] and resists to attackers with high attack potential, provided all the usage restrictions defined in section 4.1 are fulfilled. Consequently, GlobalPlatform issues the unrestricted Certificate for *Upteq NFC422 v1.0* in conformity with the Certification Process [Cert Proc].

The user of the certified product should consider the results of the certification within an appropriate risk management process and define the period of time after which the re-assessment of the product is required.

5 References

Table 5-1: Evaluation and certification references

Document	Description	Ref
GP_PRO_048	GlobalPlatform Secure Element Certification Process, v1.0	[Cert Proc]
GPD_GUI_163	GlobalPlatform Technology Secure Element / eUICC Evaluation Methodology, v0.0.05	[EM]
GSMA SGP.21	Embedded UICC for Consumer Devices Protection Profile PP v1.0 05-June-2018	[PP]
	Joint Interpretation Library Attack Methods for Smartcards and Similar Devices, version 3.0, Apr 2019	[JIL AM]
	Joint Interpretation Library Application of Attack Potential to Smartcards, Version 3.0, Apr 2019	[JIL AP]
Security Target	Gemalto (Thales Group), Upteq NFC422 v1.0 eUICC Security Target, version 2.0 SHA256(ST v2.0 - Upteq NFC422 v1.0 eUICC_23.07.2019.pdf)= ec26a585235407c4de6e819dbe21476d2e9dd22a427501d632819dc37c459935	[ST]
Platform Security Guidance	Gemalto (Thales Group), D1188231 Guidance for secure application development on UpTeq NFC platforms, Release A13.3b, August 2018 GlobalPlatform, GPC_GUI_050 GlobalPlatform Card, Composition Model Security Guidelines for Basic Applications, Version 2.0, November 2014	[Platform GUI]
IC Security Guidance	Security Application Note for [S3M2M5C/S3M2M0C/S3M1M5C/S3NSEN4/S3NSEN3, v0.4, 28 Feb	[IC GUI]
Evaluation Report	UL, Evaluation Technical Report, number 12775232JD06, version C SHA256(ETR12775232JD06C.pdf)= c338a4e59039983ba8d88ad83bcdc974e2d6a48b7cdfe7a8c8caecb60b3e1d35	[ETR]
[Platform SER]	EMVCo Security Evaluation Shared Evaluation Report (SER) Platform Approval, UpTeq NFC422 v1.0, 17 Jul 2019	[Platform SER]
[IC SER]	Leti, Evaluation Technical Report (ETR for composition) - CAYUSE5, 21 May 2019	[IC SER]
EMVCo Platform Certificate	EMVCo, PCN0168 (Expiry Date 29 May 2020)	[PCN0168]
EMVCo IC Certificate	EMVCo, ICCN0262 (Expiration 18 May 2020)	[ICCN0262]

Document	Description	Ref
Common Criteria IC Certificate	Certificate ANSSI-CC-2019/29 S3NSEN4/S3NSEN3 32-bit RISC Microcontroller for Smart Card including specific IC Dedicated software (rev 1), 31 July 2019	[ANSSI-CC-2019/29]

Table 5-2: Product-related references

Document	Description	Ref
GSMA SGP.21	GSM Association Architecture Specification, version 2.2, September 2017	[SGP21]
GSMA SGP.22	GSM Association RSP Technical Specification, version 2.2, September 2017	[SGP22]
Java Card 3.0.5 Classic Edition	Java Card Platform, Classic Edition, version 3.0.5, October 2015 - Virtual Machine Specification, - Runtime Environment Specification, - Application Programming Interface	[JC305]
GlobalPlatform Card specification	GlobalPlatform Card Specification, version 2.3, October 2015 Including the following Amendments : - Remote Application Management over http, Card Specification v2.2 – Amendment B, v1.1.3 - Secure Channel Protocol '03' - Card Specification v2.2 – Amendment D, v1.1.1 - Security Upgrade for Card Content Management – Card Specification v2.3 - Amendment E, v1.1 - Secure Channel Protocol ‘11’ - Card Specification v.2.3 – Amendment F, v1.2.1 - Executable Load File Upgrade - Card Specification v2.3 – Amendment H, v1.0	[GP23]
MILENAGE	3GPP TS 35.205, 3GPP TS 35.206, 3GPP TS 35.207, 3GPP TS 35.208, 3GPP TR 35.909, release 11	[MILENAGE]
TUAK	3GPP TS 35.231, 3GPP TS 35.232, 3GPP TS 35.233, version 12.1.0, release 12	[TUAK]

6 Abbreviations

Table 6-1: Abbreviations

Term	Definition
API	Application Programming Interface
DETR	Detailed Evaluation Technical Report
E-CASD	eUICC Controlling Authority Security Domain
eUICC	embedded Universal Integrated Circuit Card
IC	Integrated Circuit
LPA	Local Profile Assistant
LPAd	LPA that is hosted by the device
LPAe	LPA that is embedded in the eUICC
NAA	Network Access Applications
MNO	Mobile Network Operator
OS	Operating System
OTA	Over-The-Air
PP	Protection Profile
SE	Secure Element
SIM	Subscriber Identity Module
SM-DS	Subscription Manager Discovery Server
ST	Security Target
TOE	Target of Evaluation

Mounji Methlouthi

Signature numérique de Mounji Methlouthi
DN : c=US, cn=Mounji Methlouthi, email=mounji.methlouthi@smart-consulting.com
Date : 2019.09.10 01:34:41 +02'00'