

Certification Report

CSP v1.0 on Upteq NFC422 v1.0 JCS

Sponsor and developer: **Thales**
6 rue de la Verrerie
Meudon Cedex
France

Evaluation facility: **Brightsight**
Brassersplein 2
2612 CT Delft
The Netherlands

Report number: **NSCIB-CC-0089911-CR**

Report version: **1**

Project number: **0089911**

Author(s): **Wouter Slegers**

Date: **10 July 2020**

Number of pages: **11**

Number of appendices: **0**

Reproduction of this report is authorized provided the report is reproduced in its entirety.

CONTENTS:

Foreword	3
Recognition of the certificate	4
International recognition	4
European recognition	4
1 Executive Summary	5
2 Certification Results	6
2.1 Identification of Target of Evaluation	6
2.2 Security Policy	6
2.3 Assumptions and Clarification of Scope	6
2.4 Architectural Information	6
2.5 Documentation	7
2.6 IT Product Testing	7
2.7 Re-used evaluation results	9
2.8 Evaluated Configuration	9
2.9 Results of the Evaluation	9
2.10 Comments/Recommendations	9
3 Security Target	10
4 Definitions	10
5 Bibliography	11

Foreword

The Netherlands Scheme for Certification in the Area of IT Security (NSCIB) provides a third-party evaluation and certification service for determining the trustworthiness of Information Technology (IT) security products. Under this NSCIB, TÜV Rheinland Nederland B.V. has the task of issuing certificates for IT security products, as well as for protection profiles and sites.

Part of the procedure is the technical examination (evaluation) of the product, protection profile or site according to the Common Criteria assessment guidelines published by the NSCIB. Evaluations are performed by an IT Security Evaluation Facility (ITSEF) under the oversight of the NSCIB Certification Body, which is operated by TÜV Rheinland Nederland B.V. in cooperation with the Ministry of the Interior and Kingdom Relations.

An ITSEF in the Netherlands is a commercial facility that has been licensed by TÜV Rheinland Nederland B.V. to perform Common Criteria evaluations; a significant requirement for such a license is accreditation to the requirements of ISO Standard 17025 “General requirements for the accreditation of calibration and testing laboratories”.

By awarding a Common Criteria certificate, TÜV Rheinland Nederland B.V. asserts that the product or site complies with the security requirements specified in the associated (site) security target, or that the protection profile (PP) complies with the requirements for PP evaluation specified in the Common Criteria for Information Security Evaluation. A (site) security target is a requirements specification document that defines the scope of the evaluation activities.

The consumer should review the (site) security target or protection profile, in addition to this certification report, in order to gain an understanding of any assumptions made during the evaluation, the IT product's intended environment, its security requirements, and the level of confidence (i.e., the evaluation assurance level) that the product or site satisfies the security requirements stated in the (site) security target.

Reproduction of this report is authorized provided the report is reproduced in its entirety.

Recognition of the certificate

Presence of the Common Criteria Recognition Arrangement and SOG-IS logos on the certificate indicates that this certificate is issued in accordance with the provisions of the CCRA and the SOG-IS agreement and will be recognised by the participating nations.

International recognition

The CCRA has been signed by the Netherlands in May 2000 and provides mutual recognition of certificates based on the CC. Starting September 2014 the CCRA has been updated to provide mutual recognition of certificates based on cPPs (exact use) or STs with evaluation assurance components up to and including EAL2+ALC_FLR. The current list of signatory nations and approved certification schemes can be found on: <http://www.commoncriteriaportal.org>.

European recognition

The European SOGIS-Mutual Recognition Agreement (SOGIS-MRA) version 3 effective from April 2010 provides mutual recognition of Common Criteria and ITSEC certificates at a basic evaluation level for all products. A higher recognition level for evaluation levels beyond EAL4 (resp. E3-basic) is provided for products related to specific technical domains. This agreement was initially signed by Finland, France, Germany, The Netherlands, Norway, Spain, Sweden and the United Kingdom. Italy joined the SOGIS-MRA in December 2010. The current list of signatory nations, approved certification schemes and the list of technical domains for which the higher recognition applies can be found on: <http://www.sogisportal.eu>.

1 Executive Summary

This Certification Report states the outcome of the Common Criteria security evaluation of the CSP v1.0 on Upteq NFC422 v1.0 JCS. The developer of the CSP v1.0 on Upteq NFC422 v1.0 JCS is Thales located in Meudon Cedex, France and they also act as the sponsor of the evaluation and certification. A Certification Report is intended to assist prospective consumers when judging the suitability of the IT security properties of the product for their particular requirements.

The Target of Evaluation (TOE) is the cryptographic service provider (CSP) package and the underlying java Card platform, Upteq NFC422 v1.0 which supports its functionality. The TOE provides cryptographic services for the protection of the confidentiality and the integrity of user data and for entity authentication addressing the consumer electronics mobile market.

The TOE has been evaluated by Brightsight B.V. located in Delft, The Netherlands. The evaluation was completed on 10 July 2020 with the approval of the ETR. The certification procedure has been conducted in accordance with the provisions of the Netherlands Scheme for Certification in the Area of IT Security [NSCIB].

The scope of the evaluation is defined by the security target [ST], which identifies assumptions made during the evaluation, the intended environment for the CSP v1.0 on Upteq NFC422 v1.0 JCS, the security requirements, and the level of confidence (evaluation assurance level) at which the product is intended to satisfy the security requirements. Consumers of the CSP v1.0 on Upteq NFC422 v1.0 JCS are advised to verify that their own environment is consistent with the security target, and to give due consideration to the comments, observations and recommendations in this certification report.

The results documented in the evaluation technical report [ETR]¹ for this product provides sufficient evidence that the TOE meets the EAL4 augmented (EAL4+) assurance requirements for the evaluated security functionality. This assurance level is augmented with ALC_DVS.2 (Sufficiency of security measures) and AVA_VAN.5 (Advanced methodical vulnerability analysis).

The evaluation was conducted using the Common Methodology for Information Technology Security Evaluation, Version 3.1 Revision 5 [CEM] for conformance to the Common Criteria for Information Technology Security Evaluation, version 3.1 Revision 5 [CC].

TÜV Rheinland Nederland B.V., as the NSCIB Certification Body, declares that the evaluation meets all the conditions for international recognition of Common Criteria Certificates and that the product will be listed on the NSCIB Certified Products list. It should be noted that the certification results only apply to the specific version of the product as evaluated.

¹ The Evaluation Technical Report contains information proprietary to the developer and/or the evaluator, and is not releasable for public review.

2 Certification Results

2.1 Identification of Target of Evaluation

The Target of Evaluation (TOE) for this evaluation is the CSP v1.0 on Upteq NFC422 v1.0 JCS from Thales located in Meudon Cedex.

The TOE is comprised of the following main components:

Delivery item type	Identifier	Version
Hardware	S3NSEN4 (part of IC certificate)	Rev 1
Software	Secure Boot Loader & System API Code (part of IC certificate)	V1.1
	DTRNG FRO M library (part of IC certificate)	V2.2
	NFC422 v1.0 JavaCard OS	Release 1.101
	CSPApi plugin	CE020100
	de.bsi.csp package	CE020002

To ensure secure usage a set of guidance documents is provided together with the CSP v1.0 on Upteq NFC422 v1.0 JCS. Details can be found in section 2.5 of this report.

For a detailed and precise description of the TOE lifecycle refer to the *[ST]*, chapter 2.4.4

2.2 Security Policy

The TOE i.e. the Java Card System is intended to transform a smart card into a platform capable of executing applications written in a subset of the Java programming language. The intended use of a Java Card platform is to provide a framework for implementing IC independent applications conceived to safely coexist and interact with other applications into a single smart card.

Applications installed on a Java Card platform can be selected for execution when the card communicates with a card reader.

2.3 Assumptions and Clarification of Scope

2.3.1 Assumptions

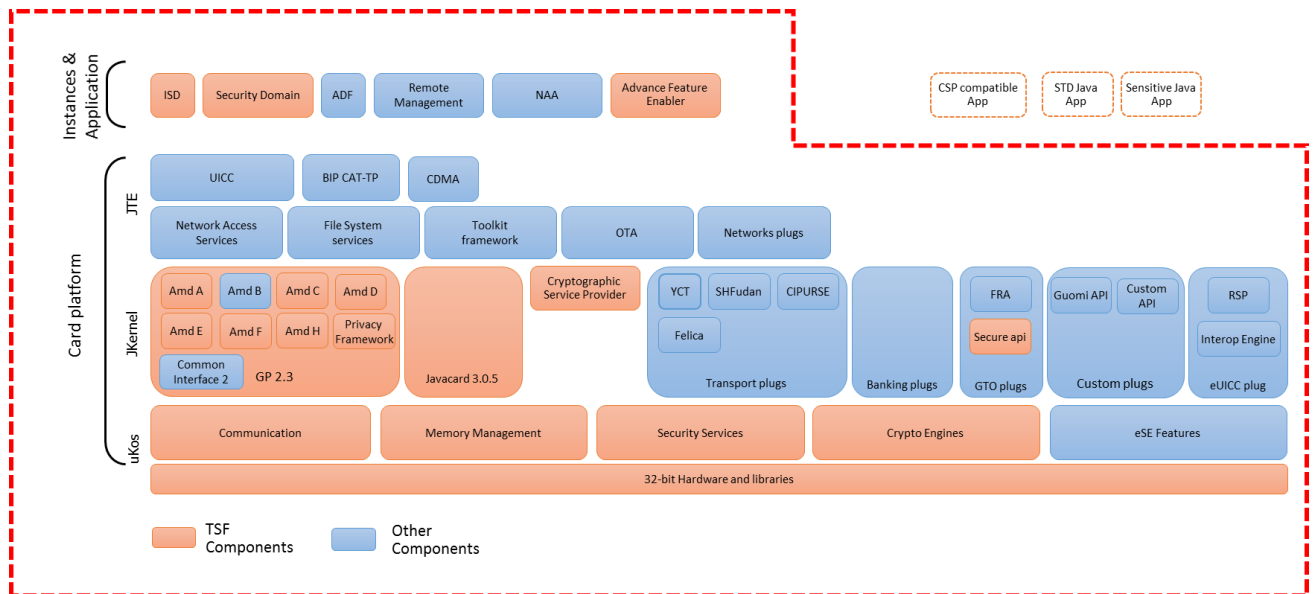
The assumptions defined in the Security Target are not covered by the TOE itself. These aspects lead to specific Security Objectives to be fulfilled by the TOE-Environment. Detailed information on these security objectives that must be fulfilled by the TOE environment can be found in section 5.2 of the *[ST]*.

2.3.2 Clarification of scope

The evaluation did not reveal any threats to the TOE that are not countered by the evaluated security functions of the product.

2.4 Architectural Information

The logical architecture, originating from the Security Target *[ST]* of the TOE can be depicted as follows:



2.5 Documentation

The following documentation is provided with the product by the developer to the customer:

Document
[AGD] Operational guidance on CC platforms With or Without CA And Optional VA, D1516184
[AGD-PRE] D1516186 v1.0 - Preparative guidance on CC platforms
[AGD-OPE] Operational guidance on CC platforms With or Without CA And Optional VA, D1516184, v1.2
[AGD-OPE-VA] D1516183 v1.0 - Operational guidance on CC platforms for VA
[Applet guidance] Guidance for Secure application development on CC platforms, D1516182, Rev 1.1
[AGD_DAP] Samsung_Security_Guide_DAP_Tech_Note_v1.1, July 2nd, 2019
[AGD-PATCH-DEV] Guidance for Patch development on Thales Embedded Secure Solutions, D1341188, Rev C03
[AGD-PATCH-ADM] Patch Loading Management for Certified Secure Elements, D1344508, Rev A01
[IDENT_CONF] Platform Identification and Configurability UpTeq NFC422 v1.0, D1484271, Rev 1.4
[AGD-APDU] NFC 4.2.2 v1.0_APDU Guide_D1518014A, Rev 1.0
[AGD-ARCH] UpTeq Card Vol1 Card Architecture Guide, D1189324A, Rev 1.0
[AGD-APP-DEV] UpTeq Card Vol4 Applet Development Guide, D1516486A, Rev 1.0
[AGD_APP-VERIF] D1258682 C01 - Application Verification for Certified Secure Elements - External Procedure

2.6 IT Product Testing

Testing (depth, coverage, functional tests, independent testing): The evaluators examined the developer's testing activities documentation and verified that the developer has met their testing responsibilities.

2.6.1 Testing approach and depth

The developer has performed extensive testing on functional specification, subsystem and module level. All parameter choices have been addressed at least once. All boundary cases identified have been tested explicitly, and additionally the near-boundary conditions have been covered probabilistically. The testing was largely automated using industry standard and proprietary test suites. Test scripts were extensively used to verify that the functions return the expected values.

The underlying hardware test results are extendable to composite evaluations, as the underlying platform is operated according to its guidance and the composite evaluation requirements are met.

For the testing performed by the evaluators, the developer has repeated tests remotely by means of a teleconference. The evaluators have thus reproduced a selection of the developer tests, as well as a small number of test cases designed by the evaluator during this testing.

2.6.2 Independent Penetration Testing

The methodical analysis performed was conducted along the following steps:

- When evaluating the evidence in the classes ASE, ADV and AGD the evaluator considers whether potential vulnerabilities can already be identified due to the TOE type and/or specified behaviour in such an early stage of the evaluation.
- For ADV_IMP a thorough implementation representation review is performed on the TOE. During this attack oriented analysis the protection of the TOE is analysed using the knowledge gained from all previous evaluation classes. This results in the identification of (additional) potential vulnerabilities. For this analysis will be performed according to the attack methods in [JIL-AP]. An important source for assurance in this step is the technical report [HW-ETRFc] of the underlying platform.
- All potential vulnerabilities are analysed using the knowledge gained from all evaluation classes and information from the public domain. A judgment was made on how to assure that these potential vulnerabilities are not exploitable. The potential vulnerabilities are addressed by penetration testing, a guidance update or in other ways that are deemed appropriate.

In total 8 perturbation attacks, 6 side-channel attacks, 4 logical attack penetration tests were performed, for a total of 24 weeks.

2.6.3 Test Configuration

The TOE was tested in the configuration as described in the [ST]. Functional testing was performed by witnessing of the developer testing. Penetration testing was performed using the lab's equipment.

2.6.4 Testing Results

The testing activities, including configurations, procedures, test cases, expected results and observed results are summarised in the [ETR], with references to the documents containing the full details.

The developer's tests and the independent functional tests produced the expected results, giving assurance that the TOE behaves as specified in its [ST] and functional specification.

No exploitable vulnerabilities were found with the independent penetration tests.

The algorithmic security level of cryptographic functionality has not been rated in this certification process, but the current consensus on the algorithmic security level in the open domain, i.e. from the current best cryptanalytic attacks published, has been taken into account.

Not all key sizes specified in the [ST] have sufficient cryptographic strength for satisfying the AVA_VAN.5 "high attack potential".

The TOE supports a wider range of key sizes (see [ST]), including those with sufficient algorithmic security level to exceed 100 bits as required for high attack potential (AVA_VAN.5).

The strength of the implementation of the cryptographic functionality has been assessed in the evaluation, as part of the AVA_VAN activities. These activities revealed that for some cryptographic functionality the security level could be reduced from an algorithmic security level above 100 bits to a practical remaining security level lower than 100 bits. As the remaining security level still exceeds 80

bits, this is considered sufficient. So no exploitable vulnerabilities were found with the independent penetration tests.

For composite evaluations, please consult the [ETRFC] for details.

2.7 Re-used evaluation results

There is no re-use of evaluation results in this certification.

There has been extensive re-use of the ALC aspects for the sites involved in the development and production of the TOE, by use of 8 Site Technical Audit Re-use report approaches.

No sites have been visited as part of this evaluation.

2.8 Evaluated Configuration

The TOE is defined uniquely by its name and version number CSP v1.0 on Upteq NFC422 v1.0 JCS.

2.9 Results of the Evaluation

The evaluation lab documented their evaluation results in the [ETR] which references an ASE Intermediate Report and other evaluator documents. To support composite evaluations according to [CCDB-2007-09-01] a derived document [ETRFC] was provided and approved. This document provides details of the TOE evaluation that have to be considered when this TOE is used as platform in a composite evaluation.

The verdict of each claimed assurance requirement is “Pass”.

Based on the above evaluation results the evaluation lab concluded the CSP v1.0 on Upteq NFC422 v1.0 JCS, to be **CC Part 2 extended, CC Part 3 conformant**, and to meet the requirements of **EAL 4** augmented with ALC_DVS.2 and AVA_VAN.5. This implies that the product satisfies the security requirements specified in Security Target [ST].

The Security Target claims 'strict' conformance to the Protection Profile [PP].

2.10 Comments/Recommendations

The user guidance as outlined in section 2.5 contains necessary information about the usage of the TOE. Certain aspects of the TOE's security functionality, in particular the countermeasures against attacks, depend on accurate conformance to the user guidance of both the software and the hardware part of the TOE.

This TOE is critically dependent on the operational environment to provide countermeasures against specific attacks as described in [Applet guidance] sections 3.4, 3.5, 3.10, 3.12, and 3.21. Please note that the documents contain relevant details with respect to the resistance against certain attacks. As such it is vital that meticulous adherence to the user guidance of both the software and the hardware part of the TOE is maintained.

In addition 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.

The strength of the cryptographic algorithms and protocols was not rated in the course of this evaluation. This specifically applies to the following proprietary or non-standard algorithms, protocols and implementations: none.

Not all key sizes specified in the [ST] have sufficient cryptographic strength for satisfying the AVA_VAN.5 “high attack potential”. In order to be protected against attackers with a “high attack potential”, appropriate cryptographic algorithms with sufficiently large cryptographic key sizes shall be used (references can be found in national and international documents and standards).

3 Security Target

The CSP on Upteq NFC422 v1.0 JCS platform Security Target, version 1.3 [ST] is included here by reference.

Please note that for the need of publication a public version [ST-lite] has been created and verified according to [ST-SAN].

4 Definitions

This list of Acronyms and the glossary of terms contains elements that are not already defined by the CC or CEM:

DFA	Differential Fault Analysis
IC	Integrated Circuit
IT	Information Technology
ITSEF	IT Security Evaluation Facility
JIL	Joint Interpretation Library
NSCIB	Netherlands Scheme for Certification in the area of IT security
PP	Protection Profile
TOE	Target of Evaluation

5 Bibliography

This section lists all referenced documentation used as source material in the compilation of this report:

- [CC] Common Criteria for Information Technology Security Evaluation, Parts I, II and III, Version 3.1 Revision 5, April 2017.
- [CEM] Common Methodology for Information Technology Security Evaluation, Version 3.1 Revision 5, April 2017.
- [ETR] Evaluation Technical Report CSP v1.0 on Upteq NFC422 v1.0 JCS, 20-RPT-144, Version 6.0, Issue 2 July 2020.
- [ETRFc] ETR for Composition Evaluation Upteq NFC422 v1.0 CSP, 20-RPT-630, Version 3.0, Issue 2 July 2020.
- [HW-CERT] Rapport de certification ANSSI-CC-2019/29, Revision 1.
- [HW-ETRFc] Evaluation Technical Report (ETR for composition) - CAYUSE5, Version 2.0.
- [HW-ST] S3NSEN4/S3NSEN3 32-bit RISC Microcontroller for Smart Card including specific IC Dedicated Software ST Lite, version 1.0.
- [JC-CERT] Certification Report Upteq NFC v1.0 JCS, NSCIB-CC-0089864-CR.
- [JC-ETRFc] ETR for Composition Evaluation Upteq NFC422 v1.0 JCS, 20-RPT-546, Version 3.0, Issue 30 June 2020.
- [JC-ST] Upteq NFC422 v1.0 JCS platform Security Target – Public version, version 1.2p
- [NSCIB] Netherlands Scheme for Certification in the Area of IT Security, Version 2.5, 28 March 2019.
- [PP] Cryptographic Service Provider Protection Profile, V0.9.8, February 2019, BSI-CC-PP-0104-2019.
- [ST] CSP on Upteq NFC422 v1.0 JCS platform Security Target, version 1.3.
- [ST-lite] CSP on Upteq NFC422 v1.0 JCS platform Security Target – Public version, version 1.3p.
- [ST-SAN] ST sanitising for publication, CC Supporting Document CCDB-2006-04-004, April 2006.

(This is the end of this report).