Certification Report

NFC422 v1.0 JCS

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

Evaluation facility: ***SGS Brightsight B.V.***
Brassersplein 2
2612 CT Delft
The Netherlands

Report number: **NSCIB-CC-0089864-CR2**

Report version: **1**

Project number: **0089864_2**

Author(s): **Jordi Mujal**

Date: **08 October 2021**

Number of pages: **12**

Number of appendices: **0**

Head Office:
Westervoortsedijk 73
NL-6827 AV Arnhem

P.O. Box 2220
NL-6802 CE Arnhem
The Netherlands

Location Leek:
Eiberkamp 10
NL-9351 VT Leek

P.O. Box 37
NL-9350 AA Leek
The Netherlands

info@nl.tuv.com
www.tuv.com/nl

Tel. +31 (0)88 888 7 888
Fax +31 (0)88 888 7 879

TÜV Rheinland Nederland B.V. is a registered company at the Netherlands Chamber of Commerce (KVK), under number 27288788.

VAT number: NL815820380B01
IBAN: NL61DEUT0265155096

CONTENTS

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 licence 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, 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.

Recognition of the Certificate

The presence of the Common Criteria Recognition Arrangement (CCRA) and the SOG-IS logos on the certificate indicates that this certificate is issued in accordance with the provisions of the CCRA and the SOG-IS Mutual Recognition Agreement (SOG-IS MRA) and will be recognised by the participating nations.

International recognition

The CCRA was signed by the Netherlands in May 2000 and provides mutual recognition of certificates based on the Common Criteria (CC). Since 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.

For details of the current list of signatory nations and approved certification schemes, see http://www.commoncriteriaportal.org.

European recognition

The SOG-IS MRA Version 3, effective since April 2010, provides mutual recognition in Europe of Common Criteria and ITSEC certificates at a basic evaluation level for all products. A higher recognition level for evaluation levels beyond EAL4 (respectively E3-basic) is provided for products related to specific technical domains. This agreement was signed initially by Finland, France, Germany, The Netherlands, Norway, Spain, Sweden and the United Kingdom. Italy joined the SOG-IS MRA in December 2010.

For details of the current list of signatory nations, approved certification schemes and the list of technical domains for which the higher recognition applies, see https://www.sogis.eu.

1 Executive Summary

This Certification Report states the outcome of the Common Criteria security evaluation of the NFC422 v1.0 JCS. The developer of the NFC422 v1.0 JCS is Thales DIS France SA 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 TOE is a combo eSE/eUICC Java Card platform product addressing the consumer electronics mobile market. The both features eSE and eUICC are isolated logically (via framework) and physically (via interface/protocol).

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. 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.

The TOE was evaluated initially by Brightsight B.V located in Delft, The Netherlands and was certified on 10 July 2020. The re-evaluation of the TOE has also been conducted by SGS Brightsight B.V. and was completed on 08 October 2021 with the approval of the ETR. The re-certification procedure has been conducted in accordance with the provisions of the Netherlands Scheme for Certification in the Area of IT Security *[NSCIB]*.

This second issue of the Certification Report is a result of a “recertification with major changes”.

The major changes are:

- New JCS TOE identification is available

- A functional patch linked to the GP Privacy Framework and SCP21 implementation, was developed.

- The underlying IC and libraries that are part of this composite TOE have been re-certified

The security evaluation reused the evaluation results of previously performed evaluations. A full, up-to-date vulnerability analysis has been made, as well as renewed testing.

The scope of the evaluation is defined by the security target *[ST]*, which identifies assumptions made during the evaluation, the intended environment for the 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 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 provide 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]* (Parts I, II and III).

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. Note that the certification results apply only 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 available for public review.

2 Certification Results

2.1 Identification of Target of Evaluation

The Target of Evaluation (TOE) for this evaluation is the NFC422 v1.0 JCS from Thales DIS France SA located in Meudon Cedex, France.

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 (OS update version value 00080000)

To ensure secure usage a set of guidance documents is provided, together with the NFC422 v1.0 JCS. For details, see section 2.5 “Documentation” of this report.

For a detailed and precise description of the TOE lifecycle, see 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

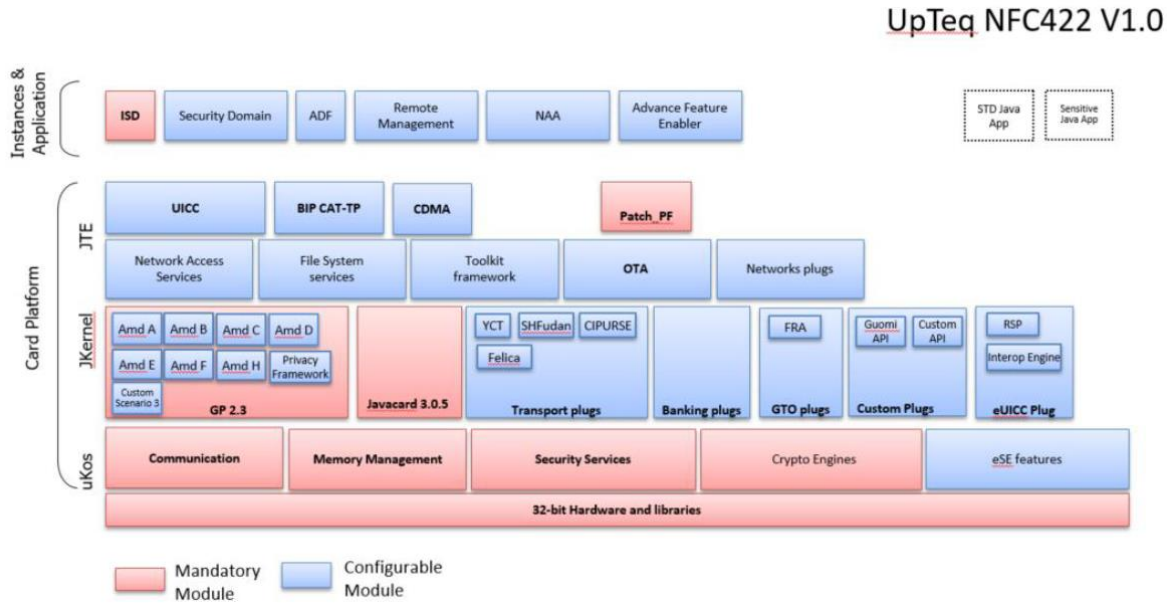
The assumptions defined in the Security Target are not covered by the TOE itself. These aspects lead to specific Security Objectives to be fulfilled by the TOE-Environment. For detailed information on the security objectives that must be fulfilled by the TOE environment, see section 6.3 of the *[ST]*.

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:

Identifier	Version
D1516186 Preparative guidance on CC platforms	v1.0
Operational guidance on CC platforms With or Without CA And Optional VA, D1516184	v1.2
D1516183 Operational guidance on CC platforms for VA	v1.0
Guidance for Secure application development on CC platforms, D1516182	Rev 1.1
Samsung_Security_Guide_DAP_Tech_Note_v1.1, July 2nd, 2019	v1.1, July 2nd, 2019
Guidance for Patch development on Thales Embedded Secure Solutions, D1341188	Rev C03
Patch Loading Management for Certified Secure Elements, D1344508	Rev A01
Platform Identification and Configurability UpTeq NFC422 v1.0, D1484271	Rev1.4
NFC 4.2.2 v1.0_APDU Guide_D1518014A	Rev 1.0
UpTeq Card Vol1 Card Architecture Guide, D1189324A	Rev 1.0
UpTeq Card Vol4 Applet Development Guide, D1516486A	Rev 1.0
D1258682 Application Verification for Certified Secure Elements - External Procedure	C01
GlobalPlatform Card Composition Model Security Guidelines for Basic Applications_v2.0, GPC_GUI_050	v2.0

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.

During the baseline evaluation, 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. These tests were performed during the baseline evaluation and all test results were as expected. The developer has added additional test cases to cover the associated changes for this recertification. New testing evidences were analysed by the Lab and the results showed that the TOE is tested on the re-certified platform and the test results were as expected.

The evaluator also analysed the changes to the TOE during this re-evaluation and determined the results of the previous testing were unaffected by the changes. Therefore, no independent functional testing was necessary as part of this re-evaluation.

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-AAPS] and [JIL-AM]*. 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.

During the baseline evaluation a total of 8 perturbation attacks, 6 side-channel attacks and 4 logical attack penetration tests were performed, for a total of 24 weeks.

During this re-evaluation, the vulnerability analysis and assurance from penetration testing were refreshed. As a result, additional penetration tests were performed. The total test effort expended by the evaluators was 4 weeks. During that test campaign, 25% of the total time was spent on Perturbation attacks and 75% on side-channel testing.

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 Test 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

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. The remaining security level still exceeds 80 bits, so this is considered sufficient. Therefore, no exploitable vulnerabilities were found with the independent penetration tests.

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

2.7 Reused Evaluation Results

This is a re-certification. Documentary evaluation results of the earlier version of the TOE have been re-used, but vulnerability analysis and penetration testing has been renewed.

There has been extensive re-use of the ALC aspects for the sites involved in the software component of the TOE. Sites involved in the development and production of the hardware platform were re-used by composition.

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 NFC422 v1.0 JCS.

2.9 Evaluation Results

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 *[COMP]* a derived document *[ETRfC]* was provided and approved. This document provides details of the TOE evaluation that must 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 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 “Documentation” 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 must 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. For the evolution of attack methods and techniques to be covered, the customer 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 to satisfy the AVA_VAN.5 “high attack potential”. 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 Upteq NFC422 v1.0 JCS platform Security Target, version 1.5, 13 September 2021 *[ST]* is included here by reference.

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

4 Definitions

This list of acronyms and definitions 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.

[Applet guidance]	Guidance for Secure application development on CC platforms, D1516182, Rev 1.1
[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
[COMP]	Joint Interpretation Library, Composite product evaluation for Smart Cards and similar devices, Version 1.5.1, May 2018
[ETR]	Evaluation Technical Report Upteq NFC422 v1.0 JCS – EAL4+, 20-RPT-143, Version 10.0, 07 October 2021.
[ETRfC]	ETR for Composition Evaluation Upteq NFC422 v1.0 JCS, 20-RPT-546, Version 7.0, 07 October 2021.
[HW-CERT]	Rapport de certification ANSSI-CC-2019/29-S01, Revision 1.
[HW-ETRfC]	LETI.CESTI.CAY5.COMPO.001, Version 3.0.
[HW-ST]	S3NSEN4/S3NSEN3 32-bit RISC Microcontroller for Smart Card including specific IC Dedicated Software ST Lite, version 1.0.
[JIL-AAPS]	JIL Application of Attack Potential to Smartcards, Version 3.1, June 2020
[JIL-AM]	Attack Methods for Smartcards and Similar Devices, Version 2.4, January 2020 (sensitive with controlled distribution)
[NSCIB]	Netherlands Scheme for Certification in the Area of IT Security, Version 2.5, 28 March 2019
[PP]	Java Card System – Open Configuration Protection Profile, version 3.0.5, registered under the reference BSI-CC-PP-0099-2017
[ST]	Upteq NFC422 v1.0 JCS platform Security Target, version 1.5, 13 September 2021
[ST-lite]	Upteq NFC422 v1.0 JCS platform Security Target, (public) version 1.5p, 13 September 2021
[ST-SAN]	ST sanitising for publication, CC Supporting Document CCDB-2006-04-004, April 2006

(This is the end of this report.)