# Certification Report

## ProxSIM Taurus, v1.02

Sponsor and developer: ***Giesecke & Devrient GmbH***
**Prinzregentenstrasse 159**
**D-81677 Munich**
**Germany**

Evaluation facility: ***Brightsight***
**Delftechpark 1**
**2628 XJ Delft**
**The Netherlands**

| | |
|---|---|
| Report number: | **NSCIB-CC-11-32973-CR** |
| Report version: | **1** |
| Project number: | **NSCIB-CC-11-32973** |
| Authors(s): | **NLNCSA** |
| Date: | **August 4, 2011** |
| Number of pages: | **17** |
| Number of appendices: | **0** |





Head office Apeldoorn:
Boogschutterstraat 11A
P.O. Box 541
7300 AM Apeldoorn
The Netherlands
Tel. +31 (0)88 888 7 888
Fax +31 (0)88 888 7 879

Location Eindhoven:
De Rondom 1
P.O. Box 6235
5600 HE Eindhoven
The Netherlands
Tel. +31 (0)88 888 7 888
Fax +31 (0)40 265 0 302

Location Enschede:
Josink Esweg 10
P.O. Box 337
7500 AH Enschede
The Netherlands
Tel. +31 (0)88 888 7 888
Fax +31 (0)88 888 7 859

TÜV Rheinland Nederland B.V. is a registered company with the Amsterdam Chamber of Commerce under number 27288788
info@nl.tuv.com
www.tuv.com/nl

# Certificate

| | |
|---|---|
| Standard | Common Criteria for Information Technology Security Evaluation (CC), Version 3.1 Revision 3 (ISO/IEC 15408) |
| Certificate number | **C11-32973** |

TÜV Rheinland Nederland B.V. certifies:

| | |
|---|---|
| Certificate holder and developer | **Giesecke & Devrient GmbH**<br>**Located in Munich, Germany** |
| Product and assurance level | **ProxSIM Taurus, v1.02,**<br>Assurance Package:<br>▪ EAL4 augmented with ALC_DVS.2 and AVA_VAN.5<br>Protection Profile Conformance:<br>▪ ANSSI-CC-PP-2010/03: Java Card™ System Protection Profile, Open Configuration, Version 2.6, April 19th, 2010 |
| Project number | **NSCIB-CC-11-32973-CR** |
| Evaluation facility | **Brightsight BV located in Delft, the Netherlands**<br>Applying the Common Methodology for Information Technology Security Evaluation (CEM), Version 3.1 Revision 3 (ISO/IEC 18045) |

The IT product identified in this certificate has been evaluated at an accredited and licensed/approved evaluation facility using the Common Methodology for IT Security Evaluation version 3.1 Revision 3 for conformance to the Common Criteria for IT Security Evaluation version 3.1 Revision 3. This certificate applies only to the specific version and release of the product in its evaluated configuration and in conjunction with the complete certification report. The evaluation has been conducted in accordance with the provisions of the Netherlands scheme for certification in the area of IT security [NSCIB] and the conclusions of the evaluation facility in the evaluation technical report are consistent with the evidence adduced. This certificate is not an endorsement of the IT product by TÜV Rheinland Nederland B.V. or by other organisation that recognises or gives effect to this certificate, and no warranty of the IT product by TÜV Rheinland Nederland B.V. or by any other organisation that recognises or gives effect to this certificate, is either expressed or implied.

| | |
|---|---|
| Validity | Date of issue : **04-08-2011**<br>Certificate expiry : **04-08-2021** |

Registration number
Notified Body 0336

PRODUCTS
RvA C 078
Accredited by the Dutch Council for Accreditation

Managing Director
TÜV Rheinland Nederland B.V.
P.O. Box 541
7300 AM Apeldoorn
The Netherlands

www.tuv.com/nl

TÜVRheinland®
Precisely Right.

# 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.

A part of the procedure is the technical examination (evaluation) of the product 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 complies with the security requirements specified in the associated security target. A security target is a requirements specification document that defines the scope of the evaluation activities. The consumer of certified IT products should review the security target, 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 satisfies the security requirements.

## Recognition of the certificate

The Common Criteria Recognition Arrangement and SOG-IS logos are printed on the certificate to indicate that this certificate is issued in accordance with the provisions of the CCRA and the SOG-IS agreement

The CCRA has been signed by the Netherlands in May 2000 and provides mutual recognition of certificates based on the CC evaluation assurance levels up to and including EAL4. The current list of signatory nations and approved certification schemes can be found on: http://www.commoncriteriaportal.org.

The European SOGIS-Mutual Recognition Agreement (SOGIS-MRA) version 3 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 in the technical domain of Smart cards and similar Devices. 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.

# 1 Executive Summary

This Certification Report states the outcome of the Common Criteria security evaluation of the ProxSIM Taurus, v1.02. The developer of the ProxSIM Taurus is Giesecke & Devrient GmbH (G&D) located in Munich, Germany 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.

This security evaluation re-used the evaluation results of the recently performed evaluation of the "ProxSIM Taurus, v1.0". This version 1.0 of the ProxSIM Taurus was certified on May 31th, 2011 under the certification identifier NSCIB-09-26151. A number of changes were introduced by G&D to adjust the functionality of the TOE. The identification of the updated product is indicated by a new version number compared to the original product as Configuration Management procedures required a change in the version number from v1.0 into v1.02.

The updated TOE identified in this report was assessed using the developers Impact Analysis Report *[IAR]*. The IAR is intended to satisfy requirements outlined in the document Assurance Continuity: CCRA Requirements *[CCRA-AC]*. In accordance with those requirements, the IAR describes the changes made to the certified TOE, the evidence updated as a result of the changes and the security impact of the changes. The assessment indicated that the original evaluation results could be re-used and the Security Target *[ST]* and the public version of the Security Target document only needed editorially updating to include changes of the provided guidance documentation and the update of the version number.

The Target of Evaluation – TOE (i.e., the ProxSIM Taurus, v1.02) is a Java Card™ System (Java Card RE, Java Card VM and Java Card API[1]) compliant with Java Card specifications versions 2.2.2 on top of a Basic OS from G&D and embedded in an already certified Integrated Circuit (IC). The evaluation of the TOE was therefore conducted as a composite evaluation and uses the results of the CC evaluation of the underlying Samsung S3FS91J integrated circuit certified under under the French CC Scheme on 18 March 2010 (Rapport de certification ANSSI-2010/57 *[HW CERT]*). The chip is under surveillance by the French CB and the certificate validity has been confirmed by ANSSI on 23 December 2010.

The TOE allows post-issuance loading and installation of applets. Furthermore, the TOE supports RMI and the deletion of applets. The TOE supports DES, RSA and AES encryption/decryption and signature generation and verification. It also supports RSA key generation functionality. The Java Card and Global Platform functionality is supported by a Native OS developed by G&D. This native OS implements a number of services as the crypto routines, transaction management and low-level memory management.

Besides the Java Card and Global platform functionality, the TOE also implements a telecommunication application that supports USIM/SIM and OTA functionality. The TELCO part of the TOE furthermore implements a file system whereas the Java Card functionality is completely object oriented. The TOE is integrated in a mobile phone solution and provides services for SIM-based mobile NFC such as public transport ticketing, payment, loyalty and event ticketing.

For public transport, tickets or tokens are stored in the NFC application and users can request access to the transportation system by swiping their mobile. A mobile NFC payment transaction is achieved by swiping the mobile over an NFC reader at a point of sale.

The TOE provides the following interfaces to the mobile phone:

- The ISO-interface according to *[ISO7816-3]* and *[ISO7816-4]* and the
- SWP-interface according ETSI.

The major TOE security features are implemented in the Java Card System and are supported by the underlying Smart Card Platform (G&D Basic OS and the IC). The Smart Card Platform provides support in case of memory management functions, I/O functions, transaction facilities and secure (shielded, native) implementation of cryptographic functions.

[1] Please note, that the Java Card API includes the GP API.

The TOE has been re-evaluated by Brightsight B.V. located in Delft, The Netherlands and was completed on August 3rd 2011 with the final delivery of the ETR. The evaluation builds upon the EAL4+ evaluation that was completed on May 16th, 2011 as described in Certification Report NSCIB-CC-09-26151-CR.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 certification was completed on August 4th 2011 with the preparation of this Certification Report. It should be noted that the certification results only apply to the specific version of the product as evaluated.

The scope of the evaluation is defined by the security target *[ST]*, which identifies assumptions made during the evaluation, the intended environment for the ProxSIM Taurus, 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 ProxSIM Taurus 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]*[2] for this product provide sufficient evidence that it 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 3 *[CEM]*, for conformance to the Common Criteria for Information Technology Security Evaluation, version 3.1 Revision 3 *[CC]*.

TÜV Rheinland Nederland B.V., as the NSCIB Certification Body, declares that the ProxSIM Taurus, v1.02 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.

[2] 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 ProxSIM Taurus, v1.02 from Giesecke & Devrient GmbH (G&D) located in Munich, Germany.

This report pertains to the TOE which form factor that will be delivered is a mask version ready for initialization and personalization of the final smartcard for end customers. The TOE is comprised of the following main components:

| Delivery item type | Identifier | Version |
|---|---|---|
| Hardware | Samsung S3FS91J | Rev 7 |
| Software | ProxSIM Taurus Java Card OS | 1.02 |

To ensure secure usage a set of guidance documents is provided together with the ProxSIM Taurus. 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 1.9.4.

## 2.2 Security Policy

Since the security target *[ST]* for the TOE claims demonstrable conformance to the Java Card System Open Configuration considered in *[JCSPP]*, it implements Java Card Specifications version 2.2.2 (*[JCRE222]*, *[JCVM222]*, *[JCAPI222]*) and allows post issuance downloading of applications that have been previously verified by an off-card trusted IT component.

In essence the TOE provides a secure environment for the software that can be loaded onto the TOE. It provides specifically:

- Protection against physical attacks (through means of the certified IC)
- Protection against side channel attacks (platform, DES, RSA and AES)
- Protection against perturbation attacks, within limitations set by the guidance
- Domain separation between the different packages and applets loaded onto the TOE, and a secure means to load, delete and install them within limitations set by the guidance

The major TOE security features are:

- The Installer, which is responsible for:
  - Secure Loading, to download a CAP-file to the smart card.
  - Secure Linking, to speed up the execution of the application. Linking includes a resolution and a preparation step.
  - Secure Installation of the applet on the card by using an application identifier (AID).
  - Secure Deletion of applets: Applet instance deletion, applet/library package deletion and deletion of an applet package and contained instances.
- The Java Card Virtual Machine (JCVM), which is the bytecode interpreter.
- The Java Card RE, which is responsible for parts of the card resource management, communication, applet execution and applet security.
- The Java Card API, that provides classes and interfaces to the Java Card applets. It defines the calling conventions by which an applet may access the Java Card RE and native services provided by the SCP such as, I/O management functions, PIN and cryptographic specific management and the exceptions mechanism.

- The Java Card Firewall. In the Java Card platform, applet isolation is achieved through the applet firewall mechanism, which is also part of the TOE security features. However applet isolation cannot be entirely granted by the firewall mechanism if certain integrity conditions are not satisfied by the applications loaded on the card. Those conditions can be statically verified to hold by a bytecode verifier, which is off-card and is not part of the TOE security features, but part of the TOE-environment.
- The Java Card System Remote Method Invocation (JCRMI), which supports logical channels.

The following Non-TOE part is required to be used:

- The off-card byte code verifier, which has to be applied to all CAP-files that will be loaded onto the TOE.

## *2.3 Assumptions and Clarification of Scope*

### 2.3.1 Usage assumptions

There are no usage assumptions identified in the Security Target that are of relevance to the TOE.

### 2.3.2 Environmental assumptions

The following assumption about the environmental aspects defined by the Security Target has to be met (for the detailed and precise definition of the assumption refer to the *[ST]*, chapter 4.4):

- All the bytecodes are verified at least once, before the loading, before the installation or before the execution, depending on the card capabilities, in order to ensure that each bytecode is valid at execution time. This means that a package or applet that is loaded onto the TOE, is always verified using the SUN offline bytecode verifier *[SUN_BCV22]*
- Deletion of applets through the card manager is secure. The TOE is always delivered together with a Card Manager. The card manager controls the access to card management functions such as the installation, update or deletion of applets. It shall also implement the card issuer's policy on the card.
- Applets loaded post-issuance do not contain native methods.

Furthermore, the following organisational security policy relates to the environment in which the TOE shall be operated (for the detailed and precise definition of the organisational security policy refer to the *[ST]*, chapter 4.3):

- The verification policy shall ensure the consistency between the export files used in the verification and those used for installing the verified file. The policy must also ensure that no modification of the file is performed in between its verification and the signing by the verification authority.

### 2.3.3 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*

Figure 2 presents the physical scope and boundaries of the TOE. The TOE consists of the following components:

- Java Card Global Platform
- Native G&D BASIC OS
- Native Telecommunication application
- CC certified EAL 5+ IC: Samsung, S3FS91J

Logically the TOE consists of the following subsystems:

- The Java Card API subsystem provides classes and interfaces to java card applets implementing Java Card API *[JCAPI222]* and the Global platform API version 2.2 classes and interfaces.
- The Java Card Virtual Machine subsystem is the byte code interpreter as specified in the Java Card Virtual Machine specification *[JCVM222]*.
- The Java Card Runtime environment subsystem provides the central command dispatcher, and is the entry point for the card manager *[JCVM222]*.
- The G&D BASIC OS subsystem provides the low-level services.
- The Telecommunication applications subsystem (not security enforcing or –supporting). The Telco subsystem provides functionality for the mobile communication network, mainly based on ETSI and 3GPP specifications.

The Telco subsystem does not perform security activities that are claimed as SFRs in the ST. The subsystem interacts with the TSF through the TSFI but also through a number of other interfaces for low-level memory management routines, low-level I/O, memory compare and memory copy routines, crypto routines, native exception and DFA error handling. These interfaces are assessed as part of the evaluation.

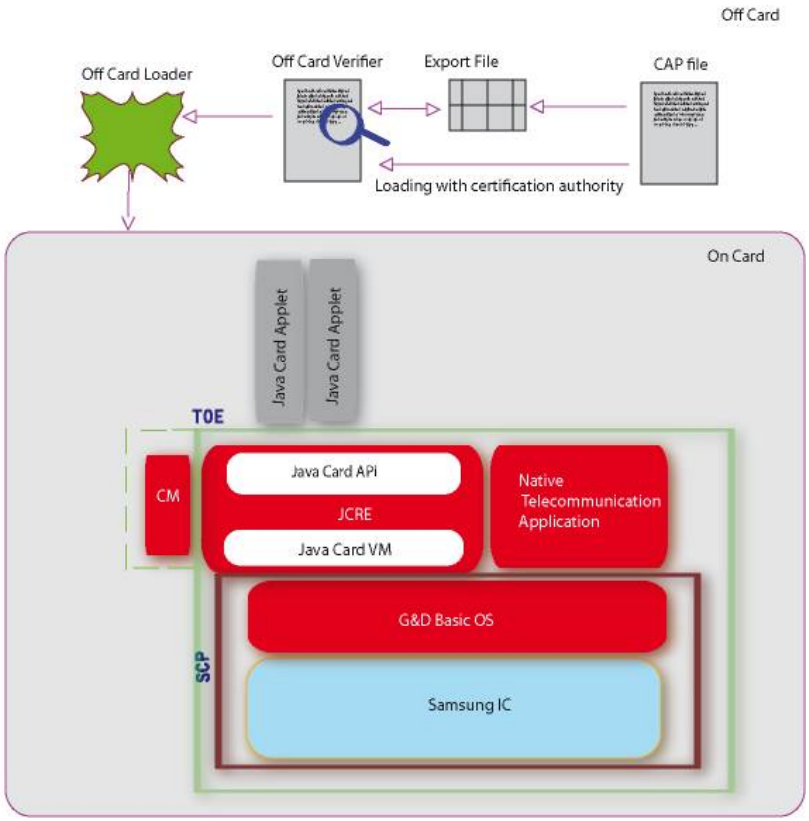


**Figure 1 – The TOE and its environment (red parts including white boxes are parts from G&D). The Card Manager is always delivered together with the TOE and marked by a dashed line.**

## 2.5 Documentation

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

| Identifier | Version |
|---|---|
| User Guidance Main Document ProxSIM Taurus | 1.4 / 20.04.2011 |

| | |
|---|---|
| User Guidance ProxSIM Taurus | 1.9 / 19.07.2011 |
| User Guidance Intialisation ProxSIMTaurus | 1.8 / 19.07.2011 |
| Application Development in User Phase ProxSIMTaurus | 1.4 / 04.04.2011 |

## *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 defined two types of tests, namely System Tests and Module Tests. Furthermore, Telco Tests are also present; these focus on the Telco native application.

Most of the requirements are directly testable, meaning that the associated tests are able to test the TOE as it is. No modifications to the configuration of the TOE are necessary to test that certain detail aspects of a security function behave as defined. This accounts for the Telco Tests and System Tests. The majority of these system tests use one or more Java Card applets that are contained in one or more Java Card packages. During testing, Java Card applets are loaded, APDU commands are send to the TOE and based on the responses, the results of the test are verified. Finally, the Java Card applets and packages are removed from the TOE. The commands for all these steps are contained in a test script. Each System Test is self contained and independent of other System Tests. The System Tests do not necessarily test one single labelled requirement per test, instead many system tests test multiple requirements within one single test, often even multiple requirements within one APDU command. This was done to keep the total amount and total size of all tests within reasonable limits as well as keeping execution times at a reasonable minimum.

Some requirements of security functions refer to internal interfaces between TOE components that are neither visible to nor accessible from the outside. Such requirements can only be tested indirectly using a modified TOE where the test is an internal part of the TOE that can be triggered from the outside and which reports its result back to the outside. These tests are called Module Tests.

The independent testing comprised of the evaluator repeating all the developer systems tests on the TOE in the context of ATE_IND.2-4 on the ISO7816 interface, which comprises approximately 68% (=156 tests) of the total amount of tests. Except of negative testing on the reset interface, and the methods of the CVM class of GP system all TSFI are at least invoked once in the test.

In addition the evaluator performed independent testing in the context of ATE_IND.2-6. The evaluator has defined 6 independent tests. The considerations for defining these tests were the following.

1. The TSFI methods of the CVM class in the global platform are selected, because of the rigour of testing of these interfaces by the developer.
2. The APDU interfaces for authentication of a user (INITIALIZE UPDATE, EXTERNAL AUTHENTICATE), loading applets and installing applets (LOAD, INSTALL) are selected because of their significance. A user has first to successfully load and install an applet for getting access to the API (Java Card and Global Platform) and Java Card Machine byte codes.
3. The Firewall mechanism and buffer overflow detection mechanism are tested because of their complexity in the amount of interfaces that invoke the mechanisms.
4. Identification of countermeasures for DFA and SPA/DPA in the power profile of the crypto algorithms, for validity reasons and to implicitly test interfaces.
5. An undocumented command search is performed to determine that the TOE does not contain any undocumented interfaces that could be misused.

### 2.6.2 Independent Penetration Testing

These evaluator independent penetration tests were conducted according to the following testing approach:

1. During evaluation of the ADV, ATE and ALC classes the evaluators hypothesized possible vulnerabilities. This resulted in a shortlist of possible vulnerabilities to be further analysed in AVA using the design knowledge gained in particular from the source code analysis in IMP and from the hardware 'ETR for composition'. This resulted in a shortlist of potential vulnerabilities to be tested.
2. Next the evaluators analysed the TOE design and implementation for resistance against the *[JIL]* attacks. This resulted in further potential vulnerabilities to be tested.
3. The evaluators made an analysis of the TOE in its intended environment to check whether the developer vulnerability analysis in ARC has assessed all information.
4. The evaluators concluded that a number of areas could be potentially vulnerable for attackers possessing a high attack potential. Consequently practical penetration testing was performed for absolute assurance. These included several perturbation, SPA/DPA and DFA attacks

### 2.6.3 Test Configuration

The test configuration for the independent evaluator testing and penetration testing comprised of:

- A laptop provided by the developer containing test software (IFDSIM), test scripts and test applets as executed by the developer, a card reader and a dongle for test software activation.
- A standard card reader connected to a PC, running software (Conclusion) capable of automatically and methodically executing all Class-Instruction combinations.
- For the acquisition of power consumption traces:
  - Digital oscilloscope;
  - Power supply;
  - Function generator;
  - Personal computer, Pentium 4, 3.2 GHz;
  - DPA interface / smart card reader (DPA1)
- Brightsight DPACenter, version 2.24
- Brightsight Brightdesktop, version 0.94 and version 0.95
- Brightsight Light manipulation set-up LM3:
  - PC equipped with 4 COM ports and a GPIB interface.
  - Laser Module
  - Laser Power Supply
  - Laser User Interface Module
  - XY table with controller
  - Waveform Generator (TOE supply voltage)
  - Waveform Generator (TOE clock signal)
  - Waveform Generator (Laser Trigger Delay)
  - Power supply E3640A
  - Digital oscilloscope
  - Brightsight card reader (4242 + modification)
  - Brightsight – LM MotherBoard v1.0
- Other tools:
  - EMVTool Version 1.00-b73, developed by Brightsight
  - Sideways acquisition center, version 0.95 16.01.2011
  - Matlab script, Brightsight / sst (surface scan tool), V1.0 and V1.2

- Matlab script, Brightsight / Brighttoolbox (second generation surface scan tool) (version 0.20)

### 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.

## *2.7 Results of the IAR assessment*

This security evaluation re-used the evaluation results of the recently performed evaluation of the "ProxSIM Taurus, v1.0". This version 1.0 of the ProxSIM Taurus was certified on May 31th, 2011 under the certification identifier NSCIB-09-26151.

On June 29th, 2011, G&D, the developer of the ProxSIM Taurus submitted an application form and Impact Analysis Report *[IAR]* to the NSCIB Certification Body requesting to issue a new certificate for their updated v1.02 ProxSIM Taurus product. The IAR is intended to satisfy the requirements outlined in the document 'Assurance Continuity: CCRA Requirements' *[CCRA-AC]*. In accordance with those requirements, the IAR describes the changes made to the recently certified TOE, the evidence updated as a result of the changes and the security impact of the changes.

The changes between version 1.02 and version 1.0 of the TOE can be categorized as:

- Feature upgrades and maintenance
- Updates as result of the above changes, including ST and Guidance Documents

The assessment of the IAR by the evaluation lab in the *[ETR]* indicated that most of the changes have no security issues and that the original evaluation results could be re-used. For the few that do have impact on security, additional testing was performed and developer evidence was analyzed to get sufficient assurance that the changes have no effect on the security level of the TOE. The evaluation lab also confirmed in the *[ETR]* that the original Vulnerability Analysis performed on version 1.0 of the ProxSIM Taurus is still valid.

## *2.8 Evaluated Configuration*

The TOE is defined uniquely by its name and version number ProxSIM Taurus, v1.02 and can be identified by reading out the data elements and the life-cycle status of the TOE as described in the user guidance.

The TOE was tested in the following Life-Cycle states:

- OP_READY
- INITIALIZED
- SECURED

It is noted that the TOE is delivered in the life-cycle INITIALIZED or SECURED to the card issuer.

## *2.9 Results of the Evaluation*

The evaluation lab documented their evaluation results in the *[ETR]*[3] which references several Intermediate Reports and other evaluator documents. The verdict of each claimed assurance requirement is given in the following tables:

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

| Development | | Pass |
|---|---|---|
| Security architecture | ADV_ARC.1 | Pass |
| Functional specification | ADV_FSP.4 | Pass |
| Implementation representation | ADV_IMP.1 | Pass |
| TOE design | ADV_TDS.3 | Pass |

| Guidance documents | | Pass |
|---|---|---|
| Operational user guidance | AGD_OPE.1 | Pass |
| Preparative procedures | AGD_PRE.1 | Pass |

| Life-cycle support | | Pass |
|---|---|---|
| Configuration Management capabilities | ALC_CMC.4 | Pass |
| Configuration Management scope | ALC_CMS.4 | Pass |
| Delivery | ALC_DEL.1 | Pass |
| Development security | ALC_DVS.2 | Pass |
| Life-cycle definition | ALC_LCD.1 | Pass |
| Tools and techniques | ALC_TAT.1 | Pass |

| Security Target | | Pass |
|---|---|---|
| Conformance claims | ASE_CCL.1 | Pass |
| Extended components definition | ASE_ECD.1 | Pass |
| ST introduction | ASE_INT.1 | Pass |
| Security objectives | ASE_OBJ.2 | Pass |
| Security requirements | ASE_REQ.2 | Pass |
| Security problem definition | ASE_SPD.1 | Pass |
| TOE summary specification | ASE_TSS.1 | Pass |

| Tests | | Pass |
|---|---|---|
| Coverage | ATE_COV.2 | Pass |
| Depth | ATE_DPT.1 | Pass |
| Functional tests | ATE_FUN.1 | Pass |
| Independent testing | ATE_IND.2 | Pass |

| Vulnerability assessment | | Pass |
|---|---|---|
| Vulnerability analysis | AVA_VAN.5 | Pass |

Based on the above evaluation results the evaluation lab concluded the ProxSIM Taurus, v1.02, to be **CC Part 2 extended**[4]**, CC Part 3 conformant**, and to meet the requirements of **EAL 4 augmented by ALC_DVS.2 and AVA_VAN.5**. This implies that the product satisfies the security technical requirements specified in Security Target ProxSIM Taurus, version 3.5 / Status 26.04.2011.

[4] The TOE is a composite TOE with a certified hardware platform. Claiming CC Part 2 extended is because the underlying platform claims CC Part 2 extended

The Security Target claims demonstrable conformance to the Java Card™ System Protection Profile, Open Configuration, Version 2.6, April 19th, 2010, registered and certified by Agence Nationale de la Sécurité des Systèmes d'Information (ANSSI) under the reference ANSSI-CC-PP-2010/03.

## *2.10 Evaluator Comments/Recommendations*

### 2.10.1 Obligations and hints for the developer

The TOE shall be delivered along with the Card Manager.

### 2.10.2 Recommendations and hints for the customer

The customer must/shall follow the provided guidance documentation, in particular:

- The package/applet loaded onto the TOE must be verified using the SUN bytecode verifier at least once.
- The customer must set-up a secure channel using Initialize update and external authenticate to enforce the SFRs that prevent Man-in-the-middle attacks, replay attacks, information gathering and editing commands.
- The documentation listed in section 2.5, especially the chapter containing "General Programming Recommendations for Sensitive Applications" provides necessary information about the usage of the TOE and all security recommendations have to be considered.

# 3 Security Target

The Security Target ProxSIM Taurus v1.02, version 3.5 / Status 26.04.2011 is included here by reference. Please note that for the need of publication a public version (Security Target Lite ProxSIM Taurus, version 1.1 / Status 21.07.2011) 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:

| | |
|---|---|
| AES | Advanced Encryption Standard |
| AID | Application Identifier |
| APDU | Application Protocol Data Unit |
| API | Application Programming Interface |
| G&D | Giesecke & Devrient GmbH |
| CAP | Converted Applet |
| CVM | Cardholder Verification Method |
| DES | Data Encryption Standard |
| DFA | Differential Fault Analysis |
| ETSI | European Telecommunication Standards Institute |
| GP | Global Platform |
| IC | Integrated Circuit |
| IT | Information Technology |
| ITSEF | IT Security Evaluation Facility |
| NFC | Near Field Communication |
| NSCIB | Nederlands Schema voor Certificatie op het gebied van IT-Beveiliging |
| OTA | Over-the-air |
| PP | Protection Profile |
| RMI | Remote Method Invocation |
| RSA | Rivest-Shamir-Adleman Algorithm |
| SCP | Smart Card Platform |
| SPA/DPA | Simple/Differential Power Analysis |
| SWP | Single Wire Protocol |
| TOE | Target of Evaluation |
| USIM | Universal Subscriber Identity Module |

# 5 Bibliography

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


| | |
|---|---|
| [BSI-PP-0035] | "Security IC Platform Protection Profile", Version 1.0, June 2007. |
| [CC] | Common Criteria for Information Technology Security Evaluation, Parts I version 3.1 revision 1, and Part II and III, version 3.1 revision 3. |
| [CCRA-AC] | Assurance Continuity: CCRA Requirements, Common Criteria document CCIMB-2004-02-009, version 1.0, February 2004 |
| [CEM] | Common Methodology for Information Technology Security Evaluation, version 3.1, Revision 3, July 2009. |
| [ETR] | Brightight, Evaluation Technical Report ProxSIM Taurus v1.02 - EAL4+, Version 5.0, August 3, 2011. |
| [ETR-HW] | Evaluation Technical Report - Lite for composition Partners, COWICHAN 2 CONFIDENTIAL, Version 1.0, 12.01.2010. |
| [HW-CERT] | Rapport de certification ANSSI-CC-2009/57, 18 mars 2010, Microcontrôleurs RISC 32-bits SAMSUNG S3FS91J / S3FS91H / S3FS91V / S3FS93I, avec SWP, Rév. 7. |
| [IAR] | Giesecke & Devrient GmbH, ProxSIM Taurus Code Config Record and Impact Analysis Report, Version 1.7/Build #119. |
| [ISO7816-3] | ISO/IEC 7816-3 (2006): Identification cards – Integrated circuit cards – Part 3: Cards with contacts – Electrical interface and transmission protocols. |
| [ISO7816-4] | ISO/IEC 7816-4 (2005): Identification cards – Part 4: Organization, security and commands for interchange |
| [JCSPP] | Java Card System Protection Profile Version 2.6, Open Configuration, ANSSI-CC-PP-2010/03, Sun Microsystems Inc., April 2010. |
| [JCVM222] | Java Card 2.2.2 Virtual Machine (JCVM) Specification. October 2005. Published by Sun Microsystems, Inc. |
| [JCAPI222] | Java Card 2.2.2 Application Programming Interface. March 2006. Published by Sun Microsystems, Inc. |
| [JCRE222] | Java Card 2.2.2 Runtime Environment (JCRE) Specification. March 2006. Published by Sun Microsystems, Inc. |
| [JIL] | Attack methods for Smart cards and similar devices, JIL, version 2.0, February 2011. |
| [NSCIB] | Nederlands Schema for Certification in the Area of IT Security, Version 1.2, 9 December 2004. |
| [ST] | Giesecke & Devrient GmbH, Security Target ProxSIM Taurus v1.02, Version 3.5 / Status 26.04.2011. |
| [ST-HW] | Project Cowichan II, Security Target of S3FS91J/S3FS91H/S3FS91V/S3FS93I 32-bits RISC Microcontroller for Smart Card With SWP, version 1.0, 30th November 2009. |
| [ST-SAN] | ST sanitising for publication, CC Supporting Document CCDB-2006-04-004, April 2006. |
| [SUN_BCV22] | Java Card 2.2 Off-Card Verifier, SUN Microsystems Inc., White Paper, June 2002 |


(This is the end of this report).