TNO CERTIFICATION

Laan van Westenenk 501
P.O. Box 541
7300 AM Apeldoorn
The Netherlands

Phone +31 55 5493468
Fax +31 55 5493288
E-mail: Certification@certi.tno.nl

BTW/VAT NR NL8003.32.167.B01
Bank ING at Delft
Bank account 66.77.18.141
stating 'TNO Certification'
BIC of the ING Bank: INGBNL2A
IBAN: NL81INGB0667718141

Date
July 20, 2010

Reference
NSCIB-CC-09-11192-CR2

Subject

Project number
11192

NSCIB-CC-09-11192

Certification Report

STARCOS 3.4 ID Tachograph C2

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

TNO Certification is an independent body with access to the expertise of the entire TNO-organization

TNO Certification is a registered company with the Delft Chamber of Commerce under number 27241271

TNO CERTIFICATION

TNO CERTIFICATION
HEREBY DECLARES THAT EVALUATION
HAS DEMONSTRATED THAT THE PRODUCT

STARCOS 3.4 ID Tachograph C2,
Assurance Package: EAL4 augmented with ADV_IMP.2, ALC_DVS.2
and AVA_VAN.5
Product and version

FROM

Giesecke & Devrient GmbH, Prinzregentenstrasse 159
D-81677 Munich, Germany
Sponsor's name and address

COMPLIES WITH THE

Common Criteria for Information Technology Security Evaluation (CC),
Version 3.1 Revision 2

Certification guidelines or standards

AS DEMONSTRATED BY / EVALUATION PERFORMED BY

Brightsight BV, located in Delft, the Netherlands
Testing Laboratory

APPLYING THE

Common Methodology for Information Technology Security
Evaluation (CEM), Version 3.1 Revision 2

NSCIB-CC-09-11192-CR
Certification Report number

THE CERTIFICATE HAS BEEN ISSUED ON

September 2, 2010
1st Issue Date

September2, 2025

Expiry Date

ISSUED IN: Apeldoorn, the Netherlands

DIRECTOR TNO CERTIFICATION

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 2 for conformance to the Common Criteria for IT Security Evaluation version 3.1 Revision 2. 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 TNO Certification or by any other organisation that recognises or gives effect to this certificate, and no warranty of the IT product by TNO Certification or by any other organisation that recognises or gives effect to this certificate, is either expressed or implied.

CERTIFICATE NUMBER C10-29265

ACCREDITED BY THE COUNCIL FOR ACCREDITATION

Versie: 2006-09-06

Table of contents

Document Information

Date of issue	20th July 2010
Version of report	2
Certification ID	NSCIB-CC-09-11192
Sponsor and Developer	Giesecke & Devrient GmbH
Evaluation Lab	Brightsight BV
TOE name	STARCOS 3.4 ID Tachograph C2
TOE reference name	STARCOS 3.4 ID Tachograph C2
Report title	Certification Report
Report reference name	NSCIB-CC-09-11192-CR

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 the NSCIB, TNO Certification 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 in the Netherlands are performed by an IT Security Evaluation Facility (ITSEF) under the oversight of the NSCIB Certification Body, which is operated by TNO Certification 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 TNO Certification 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, TNO Certification 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.

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

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 Recognition Agreement approved by the SOG-IS in April 1999 provides mutual recognition of ITSEC and Common Criteria certificates for all evaluation levels (E6, resp. EAL7). This agreement was originally signed by Finland, France, Germany, Greece, Italy, The Netherlands, Norway, Portugal, Spain, Sweden, Switzerland and the United Kingdom.

1 Executive Summary

This Certification Report states the outcome of the Common Criteria security evaluation of the STARCOS 3.4 ID Tachograph C2. The developer of this product is Giesecke & Devrient GmbH 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.

The previous C1 version of the STARCOS 3.4 ID Tachograph TOE was certified on June 22nd 2010 at the same EAL level under certification identifier NSCIB-09-11192 with an certification report identified as 'version 1'. Version C2 of the TOE is identical to the previous C1 version except for the TOE software being patched to allow some personalization commands to be performed without requiring a PIN to first be entered. As a result of this change, the guidance documentation has also been updated. The developer has performed regression testing that has been analyzed by the evaluation facility who have determined that there is no impact on the security functionality offered by the TOE in its final configured, personalized state. The original certification report NSCIB-CC-09-11192 version 1 has now been extended to cover the STARCOS 3.4 ID Tachograph C2 as described in this document, certification report NSCIB-CC-09-11192 version 2.

The TOE consists of the tachograph card hardware (chip), the tachograph card software (chip operating system and tachograph application) and the accompanying guidance documentation. The hardware consists of the chip ATMEL AT90SC24036RCU that has already been evaluated by the French Agence Nationale de la Sécurité des Systèmes d'Information (ANSSI) Certification Body under certification ID ANSSI-2009/24. The software consists of the chip operating system STARCOS 3.4 ID Tachograph C2 and one appropriate application out of the four applications (data structure and data) defined in Appendix 2 (driver, company, workshop, control) of Annex 1B of Commission Regulation (EC) No. 1360/2002 *[TACH]*. The TOE complies with the Tachograph Card Specification Annex 10 and Annex 11 of Commission Regulation (EC) 1360/2002. This implies that the ST and the TOE claim compliance with two Protection Profiles. The first, Smartcard Integrated Circuit with Embedded Software, Version 2.0, June 1999, registered and certified by Agence Nationale de la Sécurité des Systèmes d'Information (ANSSI) under the reference PP/9911. The second, Smartcard IC Platform Protection Profile Version 1.0, July 2001, registered and certified by the German Bundesamt für Sicherheit in der Informationstechnik (BSI) under the reference BSI-PP-0002.

According to the procedures defined in *[AC]*, the updated TOE has been examined by Brightsight B.V. located in Delft, The Netherlands based on an Impact Analysis Report *[IAR]* written by the developer and this analysis was completed on July 12th 2010. The original STARCOS 3.4 ID Tachograph C1 was evaluated by Brightsight B.V. located in Delft, The Netherlands and was completed on June 4th 2010. Both certification procedures were conducted in accordance with the provisions of the Netherlands Scheme for Certification in the Area of IT Security *[NSCIB]*. The original certification was completed on June 15th 2010 with the preparation of this Certification Report. The certification of the C2 version of the TOE under assurance continuity was completed on July 20th 2010 with the preparation of version 2 of this Certification Report.

The scope of the evaluation is defined by the security target *[ST]*, that identifies assumptions made during the evaluation, the intended environment for the STARCOS 3.4 ID Tachograph C2, 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 STARCOS 3.4 ID Tachograph C2 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] and *[IAR]* for this product provide sufficient evidence that it meets the Evaluation Assurance Level 4 augmented (EAL 4+) assurance requirements for the evaluated security functionality. The assurance level is augmented with: ADV_IMP.2 (Complete mapping of the implementation representation of the TSF), 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 2 *[CEM]*, for conformance to the Common Criteria for Information Technology Security Evaluation, version 3.1 Revision 2 *[CC]*.

TNO Certification, as the NSCIB Certification Body, declares that the STARCOS 3.4 ID Tachograph C2 evaluation meets all the conditions of the Arrangement on the 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 is a NSCIB document that 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 Assurance Level (EAL) 4+ evaluation is the STARCOS 3.4 ID Tachograph C2, from Giesecke & Devrient GmbH located in Munich, Germany.

This report pertains to the TOE, which comprises the following main components:

Delivery item type	Identifier
Hardware	ATMEL AT90SC24036RCU Rév. B
Software	STARCOS 3.4 ID Tachograph C2 1 out of 4 applications defined in Appendix 2 (driver, company, workshop, control) *[TACH]*

To ensure secure usage, a set of guidance documents is provided together with the STARCOS 3.4 ID Tachograph C2. Details can be found in section 2.6 of this report.

2.2 Security Policy

The TOE is the STARCOS 3.4 ID Tachograph C2 product from Giesecke & Devrient. The TOE implements the Tachograph Card Specification Annex 10 and Annex 11 of EC regulation 1360/2002. Annex I B of this regulation defines in Chapter IV the construction and functional requirements for Tachograph cards. The TOE is a smart card that allows for identification by the recording equipment of the identity (or identity group) of the cardholder and allow for data transfer and storage. A Tachograph card may be of the following types driver card, control card, workshop card or company card. Additionally, a general card type exists after initialisation and prior to the personalisation of the card. One of the four previously mentioned card types is created as desired by the customer by using a specific initialisation table.

2.3 Assumptions and Clarification of Scope

2.3.1 Usage assumptions

The following usage assumption holds for the TOE as it is certified:

A.Personalization
During the personalization the identification data, certificates and secret keys will be written to the file system of the TOE. The communication of the personalization device will be under the control of the Administrator and is done in a secure manner. For the detailed and precise definition of the assumptions refer to the *[ST]*, chapter 3.3.

2.3.2 Environmental assumptions

There are no environmental assumptions for the TOE as it is certified.

2.3.3 Clarification of scope

There are no defined threats for the TOE that require additional measures in the environment, they have all been met by the TOE. All objectives for the environment defined in *[HW-ST]* are met in the composite TOE in order to meet the requirements of the *[PP]*.

2.4 Life cycle

The usual smart card product life-cycle is decomposed in 7 phases (*[PP9911]* Fig. 2.2 p. 13) as follows:

Ø Phase 1: Smart card Embedded Software Development

Ø Phase 2: IC Design and IC dedicated software development

Ø Phase 3: IC Manufacturing

Ø Phase 4: IC Packaging and testing

Ø Phase 5: Smart card product Finishing process

Ø Phase 6: Smart card Personalization

Ø Phase 7: Smart Card product end-usage

The phase 6 described in *[PP9911]* as personalization can be separated in two steps, the initialization of the embedded software and personalization of the end-user data, for short referred in the following as initialization and personalization. The product is finished after initialization, after testing the OS and creation of the dedicated filesystem with security attributes. The TOE exists only in the end-usage phase.

The security policy (cf. [*[TACH]*.Appendix 10] formulated in the current ST is valid only for phase 7. The correct delivery and the correct personalization are covered by the Preparative procedures document. Nevertheless all elements, objectives, assumptions from phases 1 to 5 and phase 6 before the personalization are referenced here. The phase 6 after the initialization and phase 7 of the card life-cycle is considered in detail.

The delivery of the TOE is to the personalization body during phase 6 of the TOE life cycle after initialization, testing of the OS and creation of the dedicated file system with security attributes has taken place.

2.5 Architectural Information

The TOE consists of the:

- Mask Software: STARCOS 3.4 ID native operation system;
- Embedded Software: Tachograph C2 application;
- CC certified EAL5+ Integrated Circuit: ATMEL AT90SC24036RCU.

In following figure, the structure of the TOE is depicted in terms of subsystems. The blocks on the left hand side indicate a type of layer where subsystems reside. The security relevant parts are implemented in the following seven subsystems:

1. *System Library*. Application framework consisting of system startup, initialisation, error and exception handling, hardware attack and integrity handling, logical channel handler and generic helper functions.
2. *Runtime System*. Steers the flow of command processing (transmission protocol, secure messaging, security analysis, etc.) and the command interpreter, which manages the APDU's (CLA, INS) and the Life Cycle State (LCS) of the commands by means of ROM and EEPROM tables.
3. *Chip Card Commands Command System*. The command pre-processor sets expected APDU case and setting to find any rules. The command processor implements the command. There are different groups of commands: (1) File system commands, (2) Authentication commands, (3) Pin/Pwd commands, (4) PSO commands, (5) Initialisation and Personalisation commands and (6) Security Environment related Commands
4. *Security Management*. Manages the Security Environment in which the card operates and controls and maintains the Security States of the card. It also controls access to commands by performing rule analysis.
5. *Key Management*. A range of operations on keys via a set of interfaces, such as provide interfaces to perform cryptographic calculations, manage and provide a key's attributes and properties, search keys/PINs/passwords and their specific attributes, derive session keys for trusted channel (TC) and manage trusted channel session key validity.
6. *Secure Messaging (SM)* consists of three API's: (1) RUN (SM pre processing, SM case handler, SM post processing), (2) Security Management (Ruleanalyze interface) and (3) Delete command (Determine SM response for delete command)
7. *Crypto Functions* is a library with an API to all cryptographic operations of the card. It wraps the cryptographic hardware support and implements the remaining features by software.

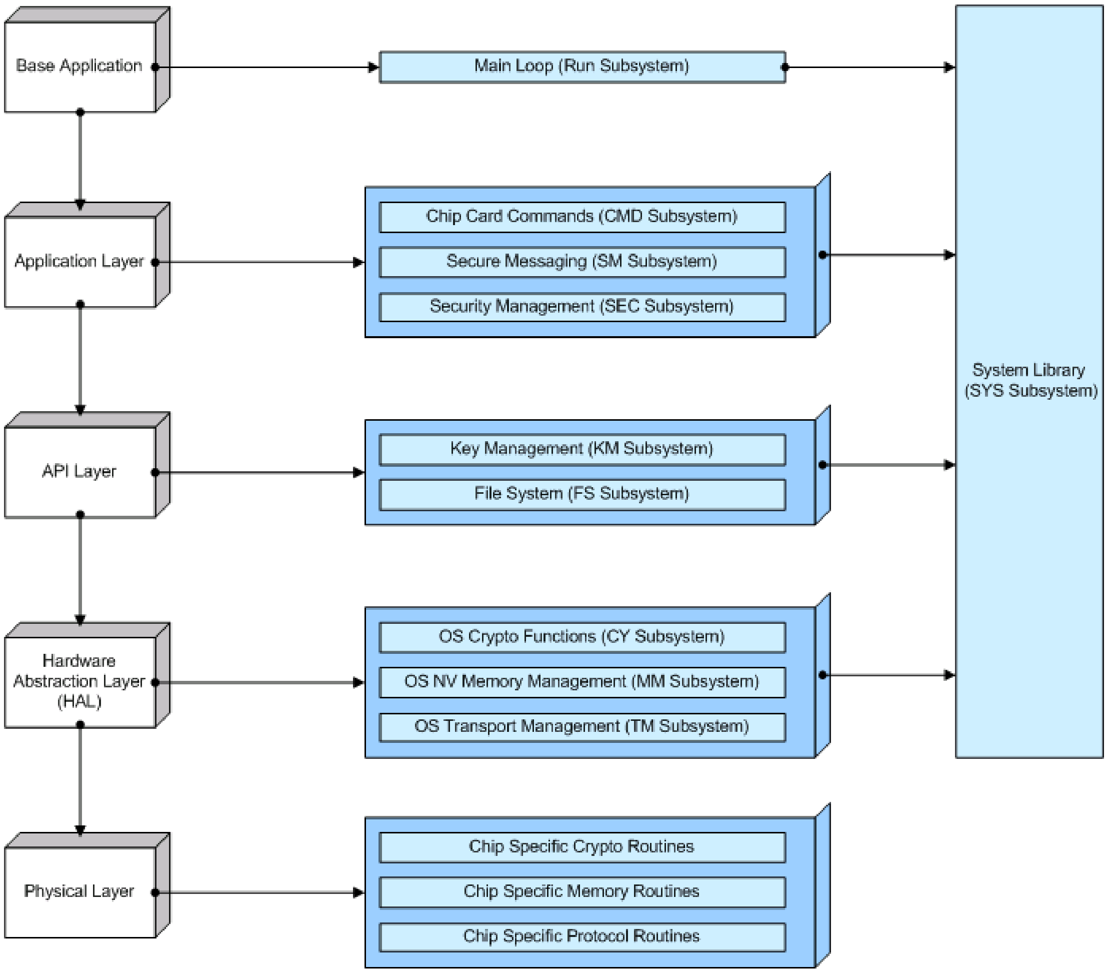
Base Application
Main Loop (Run Subsystem)
Application Layer
Chip Card Commands (CMD Subsystem)
Secure Messaging (SM Subsystem)
Security Management (SEC Subsystem)
System Library
(SYS Subsystem)
API Layer
Key Management (KM Subsystem)
File System (FS Subsystem)
Hardware
Abstraction Layer
(HAL)
OS Crypto Functions (CY Subsystem)
OS NV Memory Management (MM Subsystem)
OS Transport Management (TM Subsystem)
Physical Layer
Chip Specific Crypto Routines
Chip Specific Memory Routines
Chip Specific Protocol Routines

Figure 1, Components of the TOE.

Furthermore the TOE has three subsystems that do not perform security activities. These are File System (manages non-volatile memory in order to organize and access data in form of files), Non-Volatile Memory Management (administers non-volatile memory (EEPROM) in order to organize and access data in form of memory blocks of variable size) and Transport Management (command reception and transmission according to a variety of different protocols.

The TOE satisfies all requirements of the underlying hardware for embedded software. This includes the crypto functions developed by G&D and that avoid using the crypto functions of the underlying hardware platform via the Atmel toolbox.

2.6 Documentation

The accompanying guidance documentation consists of the preparative procedures and the operational user guidance as listed below.

Identifier	Version
Preparative procedures STARCOS 3.4 ID Tachograph C2	Version 1.1, 2010
Operational user guidance STARCOS 3.4 ID Tachograph C2	Version 1.1, 2010

2.7 *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.

2.7.1 Testing approach

Developer Testing
Below the developer testing effort, outlining the testing approach, configuration, depth and results are reported.

Testing approach
The developer has approached the testing of the TOE in a methodical manner by making use of a requirements management tool. For test specifications and test case mappings to requirements the developer makes use of a RM (requirements management) tool called DOORS. This tool generates test specifications and test case mapping documents in printable form.

Test Strategies
The following test strategies are used by the developer:

1. Maintain a correspondence between the test cases and the TSF described in the functional specification and the TOE design
2. Demonstrate the behaviour of the TSFs: The tests demonstrate the TSF as described in the *[ST]* and further demonstrate the behaviour of the actions as described in the ADV_FSP and ADV_TDS evidence.
3. Testing of TOE application variants. Tests of actions shall use the applications provided by the TOE, as far as possible.
4. Access Rules tests. A reasonable set of usage phase tests for access rules for all four applications is performed. All commands available in the usage phase are checked against the application files.
5. ATMEL ATV4/ATV4 plus Emulator Tests. If a requirement cannot be tested by ordinary means (i.e. sending commands to a real card and checking its responses), it needs to be verified using an emulator.

Vulnerability Tests. To prove that only instruction codes defined in the ADV FSP evidence are available on the module (in the four different phases: initial, PDI personalization start, ISO completed creational MF, Usage phase) a complete set of all 65536 possible class-/instruction byte combinations is sent to the module with P1=P2=0xFF. Results other than 6D00, 6E00 and 6881 are checked against a validation tree, which contains the allowed return codes for those combinations.

Testing Configuration
For testing the developer has used the following configurations:

1. Hardware (Test PC, ICC-Terminal, Emulator):
   a. Standard developer PC with Card Reader:
   CCR550 (Firmware CCR550V160, USB-Driver: CCR550USB 1.2 Beta 1)
   b. Emulator ATV4 Voyager.

2. Software (OS, Compiler, Test tools, Simulation Tools, ...):
   a. Standard developer PC software with IAR IDE, ATV4 Emulator with AT90SC24036RCU config file.

Depth

- The developer has chosen to present the following developer tests:
- Tests to cover all actions defined in the ADV_FSP evidence.
- One good case test for each command defined in the ADV_FSP evidence and executable on the TOE.
- One bad case test for each command defined in the ADV_FSP evidence and executable on the TOE.
- Access Rules test as part of the requirements on TSF data.
- Tests covering all TSF subsystems in the TOE design. Subsystems and interfaces are described in the technical design used as evidence for ADV_TDS. Subsystem behaviour and interactions relevant for testing are described and mapped to test cases.
- Tests covering all SFR-enforcing module interfaces for the TOE design.

Independent evaluator testing

Below the evaluator testing effort, outlining the testing approach, configuration, depth and results are reported.

Approach

The evaluator has witnessed all tests done by the developer as described in test specification document. The testing approach followed by the evaluator for repetition of developer tests consists of the selection of a list of subjects to be part of independent testing. This list is composed based on the claims made regarding the security functionalities and the experience with the TOE gained during the evaluation in which the evaluators regarded certain security functionality to be key for the TOE. A second category of tests has been defined for SFR-enforcing module interfaces. In this category the developer has explicitly tested all SFR enforcing module interfaces.

Depth

All tests include positive and negative test cases. The evaluator has witnessed the complete developer test set. In addition a selection of at least 10% of the developer tests have been selected to be part of the independent testing effort of the evaluator. The evaluator found that the developer tests are very complete regarding coverage and depth. The evaluator has defined two additional tests to cover the independent test set. These tests focus on the identification mechanism of the TOE, the authentication mechanism and the non-volatile memory update mechanism.

Results

All actual results are identical to the expected results.

2.7.2 Test Configuration

The following items were used to perform the tests:

1. A set of card samples (the TOE) containing
   a. Driver card
   b. Workshop card
   c. Control card
   d. Company card
   e. Non-initialised card

2. A laptop provided by the developer containing

a. Test software (Cascade)
b. Test scripts as executed by the developer
c. Card reader
d. Dongle for test software activation

2.7.3 Independent Penetration Testing

Below the evaluator penetration testing effort, outlining the testing approach, configuration, depth and results are reported.

Testing approach

1. The evaluators assessed all possible vulnerabilities found during evaluation of the classes. This resulted in a shortlist with a number of possible vulnerabilities to be tested.
2. The evaluators assessed the attacks defined by *[JIL]* for applicability to the TOE. This resulted in a shortlist with a number of possible vulnerabilities to be tested.
3. The evaluators made an analysis of the TOE in its intended environment to check whether the developer vulnerability analysis has assessed all information.

The evaluators performed tests to determine whether the TOE contains undocumented commands and whether these commands can be misused to gain control over assets in the TOE.

A crucial part of the TOE are the mechanisms for Mutual Authentication/Signature verification. A code inspection by the evaluator has shown that the TOE contains countermeasures against SPA. For the TOE mechanisms for Mutual Authentication/Signature verification the evaluators verify that an attacker has no means to retrieve secret key material using SPA techniques or DPA techniques.

A second crucial part of the TOE are the access condition mechanisms for Mutual Authentication. To rule out susceptibility for light manipulation on these mechanisms light manipulation techniques are performed on these mechanisms.

2.7.4 Testing Results

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

The following results are obtained from the tests indicated above:

- The TOE contains undocumented commands. These commands are either equal to the supported commands or return an error code and can therefore not be misused to gain control over assets in the TOE.
- The feasibility of mounting an SPA attack on the card's secret key used in the RSA operation by distinguishing square and multiply operations, and subsequently disclosing secret key components is not practical.
- The test provided additional support to theoretical analysis. With this it is concluded that, due to the implemented countermeasures, an attack on the modular reduction or the modular exponentiation is not feasible. Additionally, due to the implemented countermeasures, a straightforward attack on the recombination is not practical. Additional verification by DPA measures showed that disclosing secret key components is not practical.
- The light manipulation attacks aiming to modify the access condition mechanisms were not successful.

The testing results from the developer shows that the TOE exhibits the expected behaviour at TSFI, subsystem and SFR-enforcing module level.

The developer’s tests and the independent functional tests produced the expected results, giving assurance that the TOE behaves as specified in the Security Target at SFR-enforcing module level.

No exploitable vulnerabilities were found with the independent penetration tests.

2.8 Evaluated Configuration

For setting up / configuring the TOE all guidance documents were followed (refer to section 2.6 of this report).

2.9 Results of the Evaluation

The evaluation lab documented their evaluation results in the *[ETR]*[2] which references several Intermediate Reports. The verdict of each claimed assurance requirement is given in the following table:

Security Target		**Pass**

Development		**Pass**
Security architecture	ADV_ARC.1	Pass
Functional specification	ADV_FSP.4	Pass
Technical design	ADV_TDS.3	Pass
Implementation representation	ADV_IMP.2	Pass

Guidance documents		**Pass**
Operational	AGD_OPE.1	Pass
Preparative	AGD_PRE.1	Pass

Life cycle support		**Pass**
Configuration Management Capabilities	ALC_CMC.5	Pass
Configuration Management Scope	ALC_CMS.4	Pass
Delivery	ALC_DEL.1	Pass
Development Security	ALC_DVS.2	Pass
Lifecycle definition	ALC_DEL.1	Pass
Tools and Techniques	ALC_TAT.1	Pass

Tests		**Pass**
Coverage	ATE_COV.2	Pass
Depth	ATE_DPT.2	Pass
Functional	ATE_FUN.1	Pass
Independent	ATE_IND.2	Pass

Vulnerability assessment		**Pass**
Vulnerability analysis	AVA_VAN.5	Pass

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

Based on the above evaluation results the evaluation lab concluded the Giesecke & Devrient GmbH STARCOS 3.4 ID Tachograph C2 to be CC Part 2 extended, CC Part 3 conformant, and to meet the requirements of EAL 4 augmented by ADV_IMP.2, ALC_DVS.2 and AVA_VAN.5 as required by Smartcard Integrated Circuit with Embedded Software protection profile, Version 2.0, June 1999, registered and certified by Agence Nationale de la Sécurité des Systèmes d'Information (ANSSI) under the reference PP/9911 and the, Smartcard IC Platform Protection Profile, Version 1.0, July 2001, registered and certified by Bundesamt für Sicherheit in der Informationstechnik (BSI) under the reference BSI-PP-0002.

This implies that the product satisfies the security technical requirements specified in the STARCOS 3.4 ID Tachograph C2 Security Target, Version 2.0, dated June 29th 2010.

2.10 Compliance to Functional Tests [TACH] Appendix 9(4)

Some of the Certification reports of Tachograph products contain a statement that the TOE complies to *[TACH]* Appendix 9 TYPE APPROVAL – LIST OF MINIMUM REQUIRED TESTS. Appendix 9 defines functional tests for all parts of the Tachograph system.

G&D has provided evidence that the STARCOS 3.4 ID Tachograph C2 complies with this Appendix. The evaluators have assessed the requirements of Appendix 9 (4) and conclude that STARCOS 3.4 ID Tachograph C2 complies to the requirements.

2.11 Evaluator Comments/Recommendations

None.

3 Security Target

The Security Target, “STARCOS 3.4 ID Tachograph C2”, Version 2.0, dated June 29th 2010 is included here by reference. Please note that for the need of publication a public version of the Security Target *[ST]* 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:

EEPROM	Electronically Erasable Programmable Read Only Memory
ITSEF	IT Security Evaluation Facility
NSCIB	Nederlands Schema voor Certificatie op het gebied van IT-Beveiliging
PP	Protection Profile
ROM	Read Only Memory
RSA	Rivest-Shamir-Adleman Algorithm
SPA/DPA	Simple/Differential Power Analysis
TNO	Netherlands Organization for Applied Scientific Research
TOE	Target of Evaluation

5 Bibliography

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

[AC] Assurance Continuity: CCRA Requirements, Version 1.0, February 2004 (CCIMB-2004-02-009)

[CC] Common Criteria for Information Technology Security Evaluation, Parts I, II and III, Version 3.1 Revision 2, September 2007.

[CEM] Common Methodology for Information Technology Security Evaluation, Evaluation Methodology, Version 3.1 Revision 2, September 2007

[ETR] Evaluation Technical Report STARCOS 3.4 ID Tachograph C2 June 3rd 2010.

[HW-ST] Custodian Security Target, Atmel Registered Confidential Proprietary, Custodian_ST_V1.2 (23 Apr 09)

[IAR] Impact Analysis Report STARCOS 3.4 ID Tachograph C2, version 0.5, 12 July 2010

[JIL] CCDB-2009-03-001, (Mandatory) Application of Attack Potential to Smartcards, Version 2.7, Revision 1, March 2009

[NSCIB] Nederlands Schema for Certification in the Area of IT Security, Version 1.2, 9 December 2004.

[PP/91] Smartcard Integrated Circuit with Embedded Software Protection Profile, Version 2.0, June 1999

[PP/02] Smartcard IC Platform Protection Profile, Version 1.0, July 2001

[ST] Security Target Lite STARCOS 3.4 ID Tachograph C2, Version 2.0, dated June 29th 2010.

[ST-SAN] ST sanitising for publication, CC Supporting Document CCDB-2006-04-004, April 2006.

[TACH] Commission Regulation (EC) No. 1360/2002 on recording equipment in road transport: Requirements for Construction, Testing, Installation and Inspection (in: Official Journal of the European Communities, August 2002