Certification Report

STARCOS 3.6 ID Tachograph C1

Sponsor and developer: ***Giesecke & Devrient GmbH***
Prinzregentenstr. 159
Postfach 80 07 29
D-81607 München
Germany

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

Report number:	**NSCIB-CC-15-77633-CR**
Report version:	**1**
Project number:	**NSCIB-CC-15-77633**
Author(s):	**Carolina Lavatelli & Wouter Slegers**
Date:	**14 Sept 2016**
Number of pages:	**13**
Number of appendices:	**0**

Headoffice:
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 7 859

TÜV Rheinland Nederland B.V. is a registered company with the Amsterdam Chamber of Commerce under number 27288788

VAT number: NL815820380B01
IBAN: NL61DEUT0265155096

Certificate

Standard	Common Criteria for Information Technology Security Evaluation (CC), Version 3.1 Revision 4 (ISO/IEC 15408)
Certificate number	**CC-16-77633**

TÜV Rheinland Nederland B.V. certifies:

Certificate holder and developer	**Giesecke & Devrient GmbH** **Prinzregentenstr. 159, D-81607 München, Germany**
Product and assurance level	**STARCOS 3.6 ID Tachograph C1** Assurance Package: ▪ EAL4 augmented with ATE_DPT.2 and AVA_VAN.5 Protection Profile Conformance: ▪ BSI-CC-PP-0070: Protection Profile Digital Tachograph – Smart Card (Tachograph Card) Compliant to EU Commission Regulation 1360/2002, Annex I(B), Appendix 10, Version 1.02, 15th of November 2011
Project number	**NSCIB-CC-15-77633-CR**
Evaluation facility	**Brightsight, located in Delft, The Netherlands** Applying the Common Methodology for Information Technology Security Evaluation (CEM), Version 3.1 Revision 4 (ISO/IEC 18045)

Common Criteria Recognition Arrangement for components up to EAL2

SOGIS IT SECURITY CERTIFIED

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 4 for conformance to the Common Criteria for IT Security Evaluation version 3.1 Revision 4. 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 : **16-09-2016**

Certificate expiry: **16-09-2021**

Registration number

PRODUCTS RvA C 078

Accredited by the Dutch Council for Accreditation

TÜV Rheinland Nederland B.V
P.O. Box 2220
6802 CE Arnhem
The Netherlands.

www.tuv.com/nl

TÜVRheinland®
Precisely Right.

TÜVRheinland®
Precisely Right.

CONTENTS:

TÜVRheinland®
Precisely Right.

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.

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

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

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

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

TÜVRheinland®
Precisely Right.

Recognition of the certificate

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

International recognition

The CCRA has been signed by the Netherlands in May 2000 and provides mutual recognition of certificates based on the CC. Starting 8 September 2014 the CCRA has been updated to provide mutual recognition of certificates based on cPPs (exact use) or STs with evaluation assurance components up to and including EAL2+ALC_FLR. The current list of signatory nations and approved certification schemes can be found on: http://www.commoncriteriaportal.org.

European recognition

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

1 Executive Summary

This Certification Report states the outcome of the Common Criteria security evaluation of the STARCOS 3.6 ID Tachograph C1. The developer of the STARCOS 3.6 ID Tachograph C1 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.

STARCOS 3.6 ID Tachograph C1 is a contact Tachograph card that implements the EU directive [TACH], which comprises the following main functions:

- Store card and cardholder identification data. This data is used by the Vehicle Unit to identify the cardholder, provide services and data access rights accordingly, and ensure cardholder accountability for his activities.
- Store cardholder activities data, events and faults data, and control activities data, related to the cardholder.

STARCOS 3.6 ID Tachograph C1 supports the configuration to the following Tachograph card types: Driver card, Workshop card, Control card and Company card.

The TOE has been evaluated by Brightsight, located in Delft, The Netherlands. The evaluation was completed on September 8th 2016 with the approval of the ETR. The certification procedure has been conducted in accordance with the provisions of the Netherlands Scheme for Certification in the Area of IT Security *[NSCIB]*.

This evaluation was a composite evaluation on the Infineon M7892 B11 chip, certified under BSI with reference BSI-DSZ-CC-0782-V2-2015 *[HW-CERT]*.

The scope of the evaluation is defined in the Security Target *[ST]*, which identifies the assumptions made during the evaluation, the intended environment for the STARCOS 3.6 ID Tachograph C1, 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 3.6 ID Tachograph C1 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 provided in this certification report.

The results documented in the evaluation technical report *[ETR]*[1] for this product provide sufficient evidence that the evaluated security functionality meets the EAL4 augmented (EAL4 (+)) assurance requirements. This assurance level is augmented with ATE_DPT.2 (Testing: security enforcing modules) 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 4 *[CEM]*, for conformance to the Common Criteria for Information Technology Security Evaluation, version 3.1 Revision 4 *[CC]*.

TÜV Rheinland Nederland B.V., as the NSCIB Certification Body, declares that the STARCOS 3.6 ID Tachograph C1 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 that has been evaluated.

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

2 Certification Results

2.1 Identification of Target of Evaluation

The Target of Evaluation (TOE) for this evaluation is the STARCOS 3.6 ID Tachograph C1 from Giesecke & Devrient GmbH located in Munich, Germany.

The TOE comprises the following components:

Delivery item type	Identifier	Version
Hardware (IC)	Infineon M7892 B11 Certificate: BSI-DSZ-CC-0782-V2-2015	SLE78CFX2400P contact configuration: • Flash: up to 404 kByte • ROM: not available • User RAM 1-8 kByte • SCP: accessible • Crypto2304T: accessible • ISO/IEC 7816 interfaces
Software	STARCOS 3.6 ID OS	0x47, 0x44, 0x00, 0xB6, 0x04, 0x01, 0x01
Data	Tachograph C1 (card initialisation tables)	0x01, 0x00, 0x01
Guidance	[AGD InitGuide] [AGD PersoGuide] [GUI Ope] [GUI Pre]	See section 2.5

The TOE life cycle complies with the standard smartcard life cycle and the requirements from PP0070. It consists of the following steps:

- (Phases 2, 3 and 4) IC development and manufacturing, by Infineon
- (Phase 1) STARCOS 3.6 ID OS development and production of Tachograph C1 Data, by G&D
- (Phase 5a) STARCOS 3.6 ID OS loading into the IC, by Infineon or G&D
- (Phases 5b and 6) Tachograph card initialisation with C1 Data and personalisation, by the Customer
- (Phase 7) Tachograph card usage, by the End User

IC identification occurs upon STARCOS 3.6 ID OS loading in Phase 5a.

TOE delivery takes place after STARCOS 3.6 ID OS loading.

The TOE is delivered to the Customer in three pieces:

- SLE78CFX2400P with embedded STARCOS 3.6 ID OS platform
- Data (Tachograph C1 initialisation tables)
- Guidance

The delivery acceptance procedure includes verification of the Tachograph card through the GET PROTOCOL DATA command, which must provide the identification data defined above.

The STARCOS 3.6 ID Tachograph C1 must be initialized and personalized as defined in the guidance provided together with the smartcard components. Details can be found in section 2.5 of this report.

The TOE lifecycle is described in *[ST]* section 2.3.

2.2 Security Policy

STARCOS 3.6 ID Tachograph C1 is a contact Tachograph card that implements the EU directive [TACH], which comprises the following main functions:

- Store card and cardholder identification data. This data is used by the Vehicle Unit to identify the cardholder, provide services and data access rights accordingly, and ensure cardholder accountability for his activities.
  Store cardholder activities data, events and faults data, and control activities data, related to the cardholder.

STARCOS 3.6 ID Tachograph C1 supports the configuration to the following Tachograph card types: Driver card, Workshop card, Control card and Company card.

The main security features of the TOE, compliant with [TACH] Appendix 10, are the following:

- Prevent and detect unauthorised data access or manipulation.
- Enforce integrity and authenticity of the data exchanged with the recording equipment.

The security features of the TOE are provided by the IC and the STARCOS 3.6 ID OS.

2.3 Assumptions and Clarification of Scope

2.3.1 Assumptions

The Security Target of STARCOS 3.6 ID Tachograph C1 contains one assumption, namely A.Personalisation_Phase (Personalisation Phase Security), which is defined in the Tachograph Protection Profile PP0070 section 3.4.

This assumption addresses the secure handling of all the data produced and managed in the Personalisation Phase (Phase 6) to prevent the counterfeit of the TOE.

The objective for the environment OE.Personalisation_PhaseSecure (Handling of Data in Personalisation Phase) fully covers such assumption.

2.3.2 Clarification of scope

The Security Target of STARCOS 3.6 ID Tachograph C1 contains the following two objectives for the TOE environment, which are defined in the Tachograph Protection Profile PP0070 section 4.2:

- OE.Personalisation_PhaseSecure (Handling of Data in Personalisation Phase) is addressed in [Gui Pre];
- OE.Tachograph_Components (Implementation of Tachograph Components), which recalls the Vehicle Unit requirements defined in [TACH] concerning handling, construction and functionality, is addressed in [Gui Ope].

Note that OE.Tachograph_Components implies that the digital signature verification happens in a secure environment where no man-in-the-middle or perturbation attacks are possible.

2.4 Architectural Information

The TOE functional design consists of an ISO 7816 file structure, which complies with [TACH] Appendix 2. The APDU commands implemented in the TOE are organised in three sets:

- APDU commands available in the Initialisation phase (Phase 5b): they allow the administrator to authenticate to the card, to load the initialisation table and to set the personalisation keys. [AGD InitGuide] provides the instructions to load the initialisation table.
- APDU commands available in the Personalisation phase (Phase 6): they allow an external authenticated device to write personalisation data and keys to the application. [AGD

PersoGuide] provides the personalisation instructions. Cryptographic keys can be created off-card and injected, or generated on-card.

- APDU commands available in the Usage phase (Phase 7): they allow an authenticated external device to store and read data using secure channel communication, and to write and verify certificates and signatures. The usage phase typically starts by getting the public key of the Vehicle Unit, which is necessary for the mutual authentication between the card and the Vehicle Unit. Using secure messaging the card data can be read and updated with the Read Binary and Update Binary commands. [Gui Ope] provides instructions for the usage phase.

The TOE architecture consists of two layers: the Infineon M7892 B11 chip and the G&D native STARCOS 3.6 ID OS that supports the configuration of the ISO file structure.

2.5 Documentation

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

ST reference	Title of the document	Version / Issuance date
[AGD InitGuide]	STARCOS 3.6 ID Tachograph C1 Initialization Guide	Version 1.3 / Status 30.06.2016
[AGD PersoGuide]	Persoguide - PDI STARCOS 3.6 ID Tachograph C1	Version 1.0 / Date 08.06.2016
[GUI Ope]	Operational User Guidance STARCOS 3.6 ID Tachograph C1	Version 1.7 / Date 19.07.2016
[GUI Pre]	Preparative procedures STARCOS 3.6 ID Tachograph C1	Version 1.8 / Date 21.07.2016

2.6 IT Product Testing

The evaluators examined the developer's functional security testing activities documentation and verified that the developer has met the coverage and depth requirements.

The evaluators performed successful independent security functional testing and penetration testing.

2.6.1 Testing approach and depth

The developer has defined several test suites that cover all the TOE security functionality. They contain:

- Positive and negative test cases for each APDU command
- Test cases for all the access rules to Tachograph card data
- Test cases for the internal workings of the interfaces of the SFR-enforcing modules of the STARCOS 3.6 ID OS

All the test cases in each of the test suites have passed successfully.

The evaluator has repeated all the developer tests, including the AIS test for the random number generator.

The evaluator has defined and executed a set of independent security functional tests focused on:

- RNG tests
- Negative testing of data access control rules for the four types of Tachograph cards.

2.6.2 Independent Penetration Testing

The independent penetration test plan has been designed based on the evaluator's white box vulnerability analysis, in compliance with the attack methodology *[JIL-AM]* for products claiming resistance to attackers with high attack potential (AVA_VAN.5) and the composite evaluation methodology *[JIL-COMP].*

2.6.3 Test Configuration

Figure 1 shows the card configurations used for developer's functional security testing, which cover all the Tachograph functionality present in the four card types (Driver, Workshop, Control and Company).

variables	possible values	Card Type							
Applications	Driver, Workshop, Control, Company	Driver		Workshop		Control		Company	
		#CD1		#CD2		#CD3		#CD4	
		1	2	1	2	1	2	1	2
PIN	Present			x	x				
	Not present	x	x			x	x	x	x
Key Generation	On card	x		x		x		x	
	off card		x		x		x		x

Figure 1 Developer card configurations tested

The evaluator used test samples of Driver and Workshop cards and test equipment provided by the developer to run the security functional tests.

2.6.4 Testing Results

The Evaluation Technical Report *[ETR]* summarises the vulnerability analysis methodology, the test equipment, and the tests effectively conducted on the TOE; it provides references to the documents that contain the full details.

The developer's tests and the laboratory's independent security functional tests produced the expected results, giving assurance that the TOE behaves as specified in its Security Target, functional and design specifications.

No exploitable or residual vulnerabilities have been found in the TOE.

The algorithmic security level of the cryptographic functionality has not been rated in this certification process.

The TOE uses cryptographic primitives with security level lower than 100 bits, namely two-key TDES, 1024-bit RSA and SHA-1. This fact does not contradict NSCIB Scheme Interpretation NSI#8 since the TOE is a finished product that does not support composition on top of it. The usage of such cryptographic primitives is required by the EU regulation [TACH].

2.7 Evaluated Configuration

The TOE is defined uniquely by its name and version number STARCOS 3.6 ID Tachograph C1.

The evaluated configuration is defined in the preparative guidance [Gui Pre].

2.8 Results of the Evaluation

The evaluation laboratory has documented their evaluation results in the *[ETR]*, which references the ASE Intermediate Report and other NSP#6-compliant evaluator documents.

The assessment of the STARCOS 3.6 ID Tachograph C1 development and production sites relied on the sites certificates [CertM] and [CertN].

Based on the evaluation results the evaluation laboratory has concluded that

- The Security Target is CC Part 2 extended[2] and CC Part 3 conformant;

[2]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 is strictly conformant to the Protection Profile Digital Tachograph – Smart Card (Tachograph Card) Compliant to EU Commission Regulation 1360/2002, Annex I(B), Appendix 10, Version 1.02, 15th of November 2011, registered and certified by BSI under the reference BSI-CC-PP-0070;
- The TOE and its development and product environment meet the requirements of EAL 4 augmented with ATE_DPT.2 and AVA_VAN.5.

The verdict of the entire claimed EAL4+ assurance requirements is “Pass”.

This implies that the TOE satisfies the security requirements specified in Security Target STARCOS 3.6 ID Tachograph C1, Version 1.10, 18.08.2016.

2.9 Comments/Recommendations

The user guidance as outlined in section 2.5 contains necessary information about the usage of the TOE. There are no particular obligations or recommendations for the user apart from the user guidance.

In addition, all aspects of assumptions, threats and policies outlined in the Security Target that are not covered by the TOE itself must be fulfilled by the operational environment of the TOE.

The customers or users of the product shall consider the results of the certification within their system risk management process. In order for the evolution of attack methods and techniques to be covered, they should define the period of time until a re-assessment of the TOE is required and thus requested from the sponsor of the certificate.

The strength of the implemented cryptographic algorithms has not been rated in the course of this evaluation. To fend off attackers with high attack potential appropriate cryptographic algorithms with adequate key lengths must be used (references can be found in national and international documents and standards).

3 Security Target

The Security Target STARCOS 3.6 ID Tachograph C1, Version 1.10, 18.08.2016 *[ST]* is included here by reference. Please note that a public document Security Target Lite STARCOS 3.6 ID Tachograph C1, Version 1.0, 18.08.2016 has been created by the developer and verified against *[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:

IT	Information Technology
ITSEF	IT Security Evaluation Facility
NSCIB	Netherlands scheme for certification in the area of IT security

5 Bibliography

This section lists all the referenced documentation that has been used as source material in the compilation of this Certification Report:

[AGD InitGuide] STARCOS 3.6 ID Tachograph C1 "Initialization Guide", Version 1.3 / Status 30.06.2016

[AGD PersoGuide] STARCOS 3.6 ID Tachograph C1 " Persoguide – PDI ", Version 1.0 / Date 08.06.2016

[CC] Common Criteria for Information Technology Security Evaluation, Part I version 3.1 revision 1, and Part II and III, version 3.1, revision 4, September 2012.

[CEM] Common Methodology for Information Technology Security Evaluation, Version 3.1, Revision 4, September 2012

[CertM] Certification Report BSI-DSZ-CC-S-0070-2016, Site certificate Development Center Germany, Munich, valid until 8 August 2018

[CertN] Certification Report BSI-DSZ-CC-S-0062-2016 [CertN], Site certificate G&D Slovakia, Nitra, valid until 12 May 2018

[ETR] Evaluation Technical Report STARCOS 3.6 ID Tachograph C1 – EAL4+, reference 16-RPT-309 v3.0, September 8th 2016

[GUI Ope] Operational user guidance STARCOS 3.6 ID Tachograph C1, Version 1.7 / Date 19.07.2016

[GUI Pre] Preparative procedures STARCOS 3.6 ID Tachograph C1, Version 1.8 / Date 21.07.2016

[HW-CERT] Certification Report “Infineon Security Controller M7892 B11 with optional RSA2048/4096 v1.02.013, EC v1.02.013, SHA-2 v1.01 and Toolbox v1.02.013 libraries and with specific IC dedicated software (firmware)”, reference BSI-DSZ-CC-0782-V2-2015, dated 03.11.2015

[JIL-COMP] JIL, (Mandatory) Composite product evaluation for Smart Cards and similar devices, Version 1.4, August 2015

[NSCIB] Netherlands Scheme for Certification in the Area of IT Security, Version 2.2, August 10th, 2015

[NSP#6] NSCIB Scheme interpretation #6, Alternative evaluator reporting, version 1.2, May 2014

[NSP#8] NSCIB Scheme Interpretation #8, Remaining strength of cryptographic implementations, version 1.0, July 2015

[PP0070] Protection Profile Digital Tachograph – Smart Card (Tachograph Card) Compliant to EU Commission Regulation 1360/2002, Annex I(B), Appendix 10, Version 1.02, 15th of November 2011, reference BSI-CC-PP-0070

[ST] Security Target STARCOS 3.6 ID Tachograph C1, Version 1.10, 18.08.2016

[STLite] Security Target Lite STARCOS 3.6 ID Tachograph C1, Version 1.0, 18.08.2016

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

[TACH] Annex I(B) of Commission Regulation (EC) No. 1360/2002 ‘Requirements for construction, testing, installation and inspection’, 05.08.2002 and last amended by CR (EC) No. 432/2004 and corrigendum dated as of 13.03.2004 (OJ L 71)

(This is the end of this report).