Certification Report

SLM10TLD002Y design step A12 with CALYPSO™ move software

Sponsor and developer: ***Infineon Technologies AG***
Am Campeon 1-15
85579 Neubiberg
Germany

Evaluation facility: ***TÜV Informationstechnik GmbH***
Am TÜV 1
45307 Essen
Germany

Report number: **NSCIB-CC-0449671-CR**

Report version: **1**

Project number: **0449671**

Author(s): **Jordi Mujal**

Date: **29 November 2022**

Number of pages: **11**

Number of appendices: **0**

Head Office:
Westervoortsedijk 73
NL-6827 AV Arnhem

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

Location Leek:
Eiberkamp 10
NL-9351 VT Leek

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

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

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

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

VAT number: NL815820380B01
IBAN: NL61DEUT0265155096

TÜVRheinland®
Precisely Right.

CONTENTS

Foreword 3

Recognition of the Certificate 4

International recognition 4
European recognition 4

1 Executive Summary 5

2 Certification Results 6

2.1 Identification of Target of Evaluation 6
2.2 Security Policy 6
2.3 Assumptions and Clarification of Scope 7
2.3.1 Assumptions 7
2.3.2 Clarification of scope 7
2.4 Architectural Information 7
2.5 Documentation 7
2.6 IT Product Testing 7
2.6.1 Testing approach and depth 8
2.6.2 Independent penetration testing 8
2.6.3 Test configuration 8
2.6.4 Test results 8
2.7 Reused Evaluation Results 8
2.8 Evaluated Configuration 8
2.9 Evaluation Results 8
2.10 Comments/Recommendations 9

3 Security Target 10

4 Definitions 10

5 Bibliography 11

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.

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

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

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

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

TÜVRheinland®
Precisely Right.

Recognition of the Certificate

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

International recognition

The CCRA was signed by the Netherlands in May 2000 and provides mutual recognition of certificates based on the Common Criteria (CC). Since September 2014 the CCRA has been updated to provide mutual recognition of certificates based on cPPs (exact use) or STs with evaluation assurance components up to and including EAL2+ALC_FLR.

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

European recognition

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

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

1 Executive Summary

This Certification Report states the outcome of the Common Criteria security evaluation of the SLM10TLD002Y design step A12 with CALYPSO™ move software. The developer of the SLM10TLD002Y design step A12 with CALYPSO™ move software is Infineon Technologies AG located in Neubiberg, 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 TOE is a Calypso Basic product, a contactless smartcard, running a single Calypso Basic application that is functionally compliant with the Calypso Basic specification *[C-BASIC]*. Such products focus on providing access to public transportation and possibly other associated services that can be combined into a transport title or ticket.

The TOE has been evaluated by TÜV Informationstechnik GmbH located in Essen, Germany. The evaluation was completed on 29 November 2022 with the approval of the ETR. The certification procedure has been conducted in accordance with the provisions of the Netherlands Scheme for Certification in the Area of IT Security *[NSCIB]*.

The scope of the evaluation is defined by the security target *[ST]*, which identifies assumptions made during the evaluation, the intended environment for the SLM10TLD002Y design step A12 with CALYPSO™ move software, 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 SLM10TLD002Y design step A12 with CALYPSO™ move software are advised to verify that their own environment is consistent with the security target, and to give due consideration to the comments, observations and recommendations in this certification report.

The results documented in the evaluation technical report *[ETR]* [1] for this product provide sufficient evidence that the TOE meets the EAL2 augmented (EAL2+) assurance requirements for the evaluated security functionality. This assurance level is augmented ALC_DVS.1 (identification of security measures) and AVA_SPECIFIC.1 (as defined in *[PP]* section 6.2 “AVA_SPECIFIC –Vulnerability analysis of Calypso Basic products”).

The evaluation was conducted using the Common Methodology for Information Technology Security Evaluation, Version 3.1 Revision 5 *[CEM]* for conformance to the Common Criteria for Information Technology Security Evaluation, Version 3.1 Revision 5 *[CC]* (Parts I, II and III).

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

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

2 Certification Results

2.1 Identification of Target of Evaluation

The Target of Evaluation (TOE) for this evaluation is the SLM10TLD002Y design step A12 with CALYPSO™ move software from Infineon Technologies AG located in Neubiberg, Germany.

The TOE is comprised of the following main components:

Delivery item type	Identifier	Version
Hardware	SLM10TLD002Y	Platform ID: 0x51 (product name) DSI: 0x0C (corresponds to design step A12)
Software	Calypso™ move software	Version: 0x02 Revision: 0x01

To ensure secure usage a set of guidance documents is provided, together with the SLM10TLD002Y design step A12 with CALYPSO™ move software. For details, see section 2.5 “Documentation” of this report.

For a detailed and precise description of the TOE lifecycle, see the *[ST]*, Chapter 1.4.5.

2.2 Security Policy

The TOE provides the following features:

- Cryptographic support: RNG (True Random Number Generator PTG.1), MAC authentication mechanism based on TDES with dual key (112 Bit)
- Key hierarchy of cryptographic static secret keys: debit key, load key and issuer key are the static secret keys. The debit key’s access rights are a subset of the load key’s access rights. The load key’s access rights are a subset of the issuer key’s access rights.
- Session key derivation and monotonic transaction counter to limit the usage of the static application keys (Issuer key, Load key and Debit key)
- Session authentication mechanism: each transaction is MACed. The MAC is based on a session key derived from one of the static keys, random challenge and transaction counter
- File access control mechanism based on the static application keys: access conditions are mapped to commands and file types. Access conditions can be “always” (command can be performed outside a secure session), “never” (command cannot be performed for the mapped file type) or session (command can only be executed within a secure session) indicating the hierarchically lowest required static key for authentication.
- Session atomicity, i.e. rollback of file modifications in case of secure session failure except transaction counter
- Integrity protected ratification status in order to prevent abuse of ratification status to gain unallowed access.
- Secured management of static application keys in NVM
- Robust set of sensors and detectors for the purpose of monitoring proper chip operating conditions.
- Hardware enabled program flow integrity protection mechanism
- Test entry protection
- Peripheral locking via a Memory Management Unit to prevent unallowed peripheral accesses
- NVM integrity protection

2.3 Assumptions and Clarification of Scope

2.3.1 Assumptions

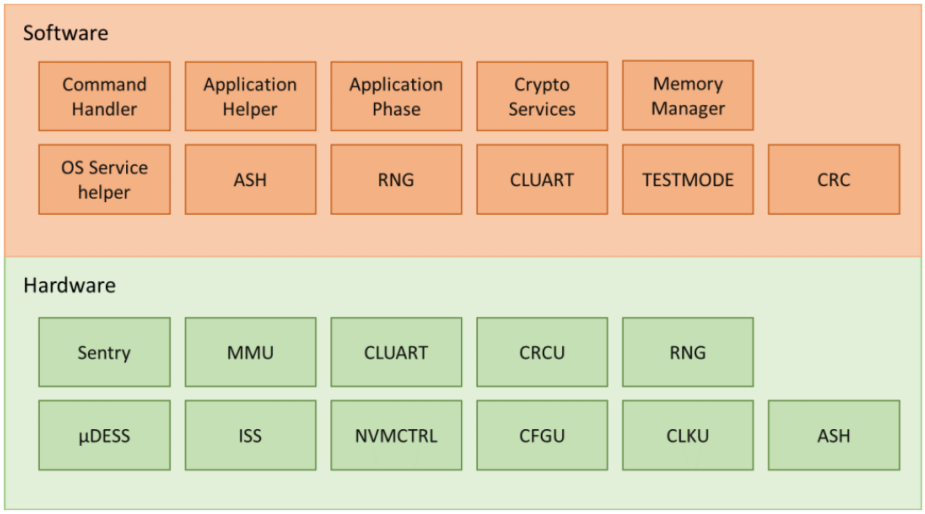
The assumptions defined in the Security Target are not covered by the TOE itself. These aspects lead to specific Security Objectives to be fulfilled by the TOE-Environment. For detailed information on the security objectives that must be fulfilled by the TOE environment, see section 4 of the *[ST]*.

2.3.2 Clarification of scope

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

2.4 Architectural Information

The following figure depicts the main TOE architecture. Note that Test code (TESTMODE) is deactivated before entering pre-personalisation phase.



2.5 Documentation

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

Identifier	Version	Date
CALYPSO™ move, Extended Datasheet	1.1	2022-07-15
CALYPSO™ move Personalization Guide	1.1	2022-07-15
Calypso Specification - Calypso Basic [2]	1.1	2020-12-15

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] Provided upon request from Calypso Networks Association.

2.6.1 Testing approach and depth

The developer performed extensive testing on functional specification. All TSFs and related security mechanisms, subsystems and modules were tested in order to assure complete coverage of all SFRs.

For the testing performed by the evaluators, the developer provided samples and a test environment. The evaluators reproduced a selection of the developer tests. In addition, a small number of test cases designed by the evaluator were also performed.

2.6.2 Independent penetration testing

For penetration testing the evaluators took all security functionalities into consideration. Intensive penetration testing was planned based on the analysis results and performed for the underlying mechanisms of security functionalities. The penetration tests covered semi-invasive attacks (i.e. laser fault injection) and non-invasive attacks (leakage analysis).

The total test effort expended by the evaluators was 11 weeks. During that test campaign, 50% of the total time was spent on Perturbation attacks, 28% on side-channel testing, and 22% on logical tests.

2.6.3 Test configuration

Only a single configuration of the TOE is available. The configuration of the samples used for independent evaluator testing and penetration testing was the same as described in the *[ST]*.

2.6.4 Test results

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

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

No exploitable vulnerabilities were found with the independent penetration tests.

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

2.7 Reused Evaluation Results

There has been extensive reuse of the ALC aspects for the sites involved in the development and production of the TOE, by use of 1 site certificate and 19 Site Technical Audit Reports.

No sites have been visited as part of this evaluation.

2.8 Evaluated Configuration

The TOE is defined uniquely by its name and version number SLM10TLD002Y design step A12 with CALYPSO™ move software.

2.9 Evaluation Results

The evaluation lab documented their evaluation results in the *[ETR]*, which references an ASE Intermediate Report and other evaluator documents.

The verdict of each claimed assurance requirement is "**Pass**".

Based on the above evaluation results the evaluation lab concluded the SLM10TLD002Y design step A12 with CALYPSO™ move software, to be **CC Part 2 extended, CC Part 3 extended**, and to meet the requirements of **EAL 2 augmented with ALC_DVS.1 and AVA_SPECIFIC.1**. This implies that the product satisfies the security requirements specified in Security Target *[ST]*.

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

2.10 Comments/Recommendations

The user guidance as outlined in section 2.5 “Documentation” contains necessary information about the usage of the TOE. Certain aspects of the TOE’s security functionality, in particular the countermeasures against attacks, depend on accurate conformance to the user guidance of both the software and the hardware part of the TOE. There are no particular obligations or recommendations for the user apart from following the user guidance. Please note that the documents contain relevant details concerning the resistance against certain attacks.

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

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

The strength of the cryptographic algorithms and protocols was not rated in the course of this evaluation. This specifically applies to the following proprietary or non-standard algorithms, protocols and implementations:

- Calypso Crypto
- Calypso Basic protocol.

3 Security Target

The SLM10TLD002Y A12 CALYPSO™ move Security Target, Revision v3.0, 25 November 2022 *[ST]* is included here by reference.

4 Definitions

This list of acronyms and definitions contains elements that are not already defined by the CC or CEM:

IC	Integrated Circuit
IT	Information Technology
ITSEF	IT Security Evaluation Facility
JIL	Joint Interpretation Library
MAC	Message Authentication Code
NSCIB	Netherlands Scheme for Certification in the area of IT Security
NVM	Non Volatile Memory
PP	Protection Profile
RNG	Random Number Generator
TOE	Target of Evaluation

5 Bibliography

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

[C-BASIC]	Calypso Specification - Calypso Basic – Version 1.1 (Ref. 191011), 15 December 2020
[CC]	Common Criteria for Information Technology Security Evaluation, Parts I, II and III, Version 3.1 Revision 5, April 2017
[CEM]	Common Methodology for Information Technology Security Evaluation, Version 3.1 Revision 5, April 2017
[ETR]	EVALUATION TECHNICAL REPORT SUMMARY (ETR SUMMARY), 8119065097/NSCIB-CC-0449671, Version 3, 29 November 2022
[JIL-AAPS]	JIL Application of Attack Potential to Smartcards, Version 3.1, June 2020
[JIL-AM]	Attack Methods for Smartcards and Similar Devices, Version 2.4, January 2020 (sensitive with controlled distribution) Must be retained for all smartcard-related TOEs
[NSCIB]	Netherlands Scheme for Certification in the Area of IT Security, Version 2.5, 28 March 2019
[PP]	Calypso Basic - Protection Profile, version 1.0, 26 October 2021, registered under the reference ANSSI-CC-PP-2021/01
[ST]	SLM10TLD002Y A12 CALYPSO™ move Security Target, Revision v3.0, 25 November 2022
[ST-SAN]	ST sanitising for publication, CC Supporting Document CCDB-2006-04-004, April 2006

(This is the end of this report.)