Swedish Certification Body for IT Security

Certification Report - Kapsch SAM 5000, Version B

Issue: 1.0, 2018-aug-28

Authorisation: Helén Svensson, Lead certifier , CSEC

Table of Contents

1 Executive Summary

The TOE is SAM 5000, a smartcard/VQFN chip used for cryptographic operations and secure storage of cryptographic keys. The TOE is used in several roles as part of a road-toll system. The TOE is a composition of an application software and a certified platform consisting of a hardware chip, a firmware, and a software library.

The application software version is SAM 5000 build 4.12. The hardware chip is the Infineon Technologies Smart Card IC Security Controller M9900, design step A22 and G11, of the SLE97 family (smart card), or the SLI97 family (VQFN chip). The BOS-V1 firmware version is used. The firmware has identifier 80001141, and the software library is CL97 Asymmetric Crypto Library for Crypto@2304T RSA/ECC/Toolbox v2.07.003.

The TOE is delivered in batches to customers who operate a road-toll system, who in turn deliver single TOEs to end users of the road-toll system.

The certified platform is compliant with the Security IC Platform Protection Profile, BSI-PP-0035 [PP], and is certified by BSI in 2017-11-02 with certificate identifier BSI-DSZ-CC-0827-V7-2017.

There are four assumptions being made in the ST regarding the secure usage and environment of the TOE. The TOE relies on these to counter the fourteen threats and comply with the five organisational security policies (OSPs) in the ST. The assumptions, threats and OSPs are described in chapter 4 Assumptions and Clarification of Scope.

The evaluation has been performed by Combitech AB in Växjö, Sweden. Site-visit and parts ot the testing was performed in Vienna, Austria.

The evaluation was completed in 2018-06-11. The evaluation was conducted in accordance with the requirements of Common Criteria (CC), version 3.1 release *5*.

Combitech AB is a licensed evaluation facility for Common Criteria under the Swedish Common Criteria Evaluation and Certification Scheme. Combitech AB is also accredited by the Swedish accreditation body according to ISO/IEC 17025 for Common Criteria.

The certifier monitored the activities of the evaluator by reviewing all successive versions of the evaluation report*s*, and by observing site-visit and testing. The certifier determined that the evaluation results confirm the security claims in the Security Target (ST) and the Common Methodology for evaluation assurance level EAL 5.

The technical information in this report is based on the Security Target (ST) and the Final Evaluation Report (FER) produced by Combitech AB.

The certification results only apply to the version of the product indicated in the certificate, and on the condition that all the stipulations in the Security Target are met.

This certificate is not an endorsement of the IT product by CSEC or any other organisation that recognises or gives effect to this certificate, and no warranty of the IT product by CSEC or any other organisation that recognises or gives effect to this certificate is either expressed or implied.

2 Identification

Certification Identification	
Certification ID	CSEC2017020
Name and version of the certified IT product	SAM 5000 build 4.12, CL97 Asymmetric Crypto Library for Crypto@2304T RSA/ECC/Toolbox v2.07.003, BOS-V1 and RMS firmware with ID 80001141 Infineon Technologies Smart Card IC Security Controller M9900, design step A22 and G11, of the SLE97 family (smart card), or the SLI97 family (VQFN chip)
Security Target Identification	Security Target for Kapsch SAM 5000, Kapsch TrafficCom, 2018-03-21, revision L, Confidential Security Target Lite for Kapsch SAM 5000, Kapsch TrafficCom, 2018-03-21, revision D
EAL	EAL 5
Sponsor	Kapsch TrafficCom AB
Developer	Kapsch TrafficCom AB
ITSEF	Combitech AB
Common Criteria version	3.1 release 5
CEM version	3.1 release 5
QMS version	1.21.3
Recognition Scope	CCRA, SOGIS och EA/MLA Within CCRA the certificate is recognised as EAL 2 and within SOGIS the certificate is recognized as EAL 4.
Certification date	2018-08-28

3 Security Policy

- Cryptographic Support
- User Data Protection
- Identification and Authentication
- Security Management
- Protection of the TSF

3.1 Cryptographic Support

The TOE provides cryptographic support to the user and for the protection of the TSF. The cryptographic support includes encryption and decryption of data and keys using AES, DES, RSA and ECC algorithms. Authentication of data is provided as AES and DES MAC calculation and verification as well as digital signatures using RSA or ECC algorithms.

Cryptographic keys are generated for AES, DES, RSA, and ECC as well as using an EC DH scheme.

Backup is taken of cryptographic keys and keys are destroyed in a secure way.

Algoritmer

- Data Encryption Standard (DES),
- Triple Data Encryption Standard (3DES),
- Rivest-Shamir-Adleman Cryptography (RSA),
- Advanced Encryption Standard (AES),
- Secure Hash Algorithm (SHA-1, SHA-256) as part of signature calculation/verification,
- Random Number Generator (RNG), and
- Elliptic Curve Cryptography (ECC).

3.2 User Data Protection

Access control to sensitive assets is restricted by an access control policy, Access Condition Policy that requires authentication according to configurable access conditions.

Import and export of sensitive assets are restricted by an information flow control policy, Import/Export Key Policy, that requires authentication before import or export can take place and ensures that the assets are confidentiality, integrity, and authentication protected.

3.3 Identification and Authentication

Authentication is required according to access conditions set for each asset. The authentication can be performed either by PIN, a challenge-response scheme, a Diffie-Hellman key exchange scheme, or a calculated MAC authentication code. Re-authentication is required according to configurable conditions. The PIN secrets shall be of a certain length and unsuccessful authentication attempts shall block the PIN. Unsuccessful attempts to unblock the PIN shall block the unblocking function.

3.4 Security Management

Certain management functions can be performed and the access condition security attributes shall have restricted default values.

3.5 Protection of the TSF

Measures are applied to detect replay attempts at export and import of keys as well as for reading and updating binary file contents within the TOE. Memory provided by the operational environment is functionally tested at start-up and the result can be read by the user.

4 Assumptions and Clarification of Scope

4.1 Usage Assumptions

The Security Target [ST] makes three assumptions on the usage of the TOE.

A.Deployment – The TOE operational environment is assumed to react on faulty deployment performed by the Authorized service personnel.

A.No_Evil – Authorized admins and service personnel are assumed to be security screened to be non-hostile, sufficiently trained, and willing to follow their instructions, before authorized to interact with the TOE.

A.Counter – The TOE operational environment is assumed to use the Security Critical Commands Usage Counter to request a new authentication before e.g. 20000 Triple-DES or AES operations have been performed.

4.2 Environmental Assumptions

The Security Target [ST] makes one assumption on the operational environment of the TOE.

A.OBU_Protection – The operational environment of the TOE when deployed as TR-SAM in an OBU is assumed to be equipped with tamper protection.

4.3 Clarification of Scope

The Security Target contains six threats, which have been considered during the evaluation.

T.Logical_Leak – A threat agent may logically attack the TOE in order to reveal sensitive assets. The modification may be achieved through deficiencies in the TOE external communication protocols or in the TOE internal asset handling.

T.Logical_Manipulation – A threat agent may logically attack the TOE in order to modify or remove sensitive assets. The attack may be achieved through deficiencies in the TOE external communication protocols or in the TOE internal assets handling.

T.Eavesdropping – A threat agent may listen to and successfully interpret sensitive assets sent or received over the TOE external interface.

T.Spoofing – A threat agent may try to disguise as an authorised user to disclose, manipulate or remove sensitive assets.

T.Replay – A threat agent may gain access to sensitive information by replaying TOE external communication.

T.Unint_Corruption – An authorised user may by mistake override or bypass security features of the TOE or enable opportunities for others to do so.

The Security Target also contains eight threats, which have been considered both during the evaluation and certification of the underlying platform and during the evaluation of the current TOE.

T.Phys-Manipulation – Physical Manipulation – see [PP] section 3.2.

T.Phys-Probing – Physical Probing – see [PP] section 3.2.

T.Malfunction – Malfunction due to Environmental Stress – see [PP] section 3.2.

T.Leak-Inherent – Inherent Information Leakage – see [PP] section 3.2.

T.Leak-Forced – Forced Information Leakage – see [PP] section 3.2.

T.Abuse-Func – Abuse of Functionality – see [PP] section 3.2.

T.RND – Deficiency of Random Numbers – see [PP] section 3.2.

T.Mem-Access – Memory Access Violation – see [PlatformST] section 3.3.

The Security Target contains five Organisational Security Policies (OSPs), which have been considered during the evaluation.

P.Crypto – The TOE shall provide cryptographic mechanisms, including mechanisms to encrypt and decrypt user data, calculate and verify message authentication codes over user data, calculate and verify digital signatures over user data, derive keys, encrypt and decrypt keys, and generate random data for key and challenge generation.

P.Keys – The TOE shall provide secure key mechanisms, including mechanisms to generate, derive, import, export, and backup keys. The TOE (P-SAM) shall increment a derivation counter monotonically every time a key is derived. The derivation counter shall start on zero and shall not be possible to reset after SAM production until the key is deleted.

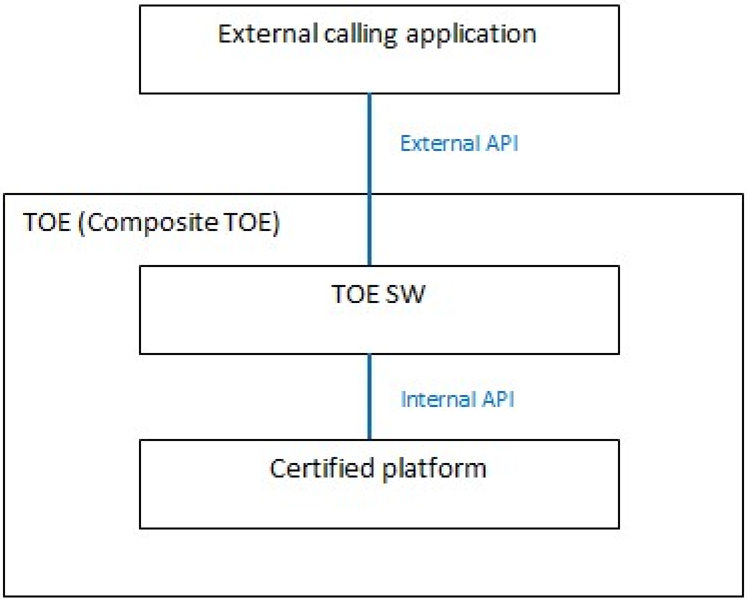
P.Memory_Test – The TOE shall detect memory deficiencies in the operational environment at initial start-up.

P.Process-TOE - Protection during TOE Development and Production – see [PP] section 3.3.

P.Add-Functions – Additional Specific Security Functionality – see [PlatformST] section 3.4.

5 Architectural Information

The TOE physical scope is illustrated in the figure below.



The external calling application represents components in the road-toll system where TOE is used.

The TOE SW is SAM 5000 build 4.12.

The certified platform consists of:

- the software library CL97 Asymmetric Crypto Library for Crypto@2304T RSA/ECC/Toolbox v2.07.003
- the firmware, including the boot software (BOS-V1) and the resource management system (RMS)
- the hardware Infineon Technologies Smart Card IC Security Controller M9900, design step A22 and G11, of the SLE97 family (smart card), or the SLI97 family (VQFN chip).

6 Documentation

The end users of the TOE do not interact directly with the TOE. All interaction takes place through components of the road-toll system. Therefore, the relevant guidance is the API description used by the developer of the road-toll system, Kapsch TrafficCom AB who also are the developer of the TOE:

Interface specification for Kapsch SAM 5000 [API].

7 IT Product Testing

7.1 Developer Testing

All external interfaces were tested thoroughly by the developer using a proprietary programmable test tool. Both positive and negative tests were performed. The internal interfaces were tested indirectly via testing the external interfaces. The SFRs were completely covered. Both form factors were covered.

7.2 Evaluator Testing

The evaluators tested the TOE in their own premises in Växjö, Sweden. The developer's test tool was used to verify a subset of the devloper's tests, as well as to run some complementary tests. All versions of the TOE were tested.

The internal interfaces also were investigated by means of code review.

7.3 Penetration Testing

The evaluators performed negative tests, verifying the handling of various parameter values and lengths.

The penetration testing also was supported by code review.

8 Evaluated Configuration

The TOE is comprised of the card application SAM 5000 build 4.12, and the certified platform.

The configurations of the certified platform that are used in the TOE are:

- the software library CL97 Asymmetric Crypto Library for Crypto@2304T RSA/ECC/Toolbox v2.07.003
- the firmware, including the boot software (BOS-V1) and the resource management system (RMS), firmware ID 80001141
- the hardware Infineon Technologies Smart Card IC Security Controller M9900, design step A22 and G11, of the SLE97 family (smart card), or the SLI97 family (VQFN chip).

The TOE is used by a road-toll system in one of five different roles:

- Communication Point SAM, CP-SAM - Installed in a Road Side System.
- Central Services SAM, CS-SAM - Installed centrally in a security server in the Toll Charger Central Services.
- Master SAM, M-SAM - Installed in a secure environment in a Key Initialization Facility.
- OBU Personalisation SAM, P-SAM - Used for programming of On Board Units. e.g. in On Board Unit production.
- Trusted Recorder SAM, TR-SAM - Installed in an On Board Unit in a vehicle.

9 Results of the Evaluation

The evaluators applied each work unit of the Common Methodology [CEM] within the scope of the evaluation, and concluded that the TOE meets the security objectives stated in the Security Target [ST] for an attack potential of Moderate.

The certifier reviewed the work of the evaluator and determined that the evaluation was conducted in accordance with the Common Criteria [CC].

The evaluators overall verdict is PASS.

The verdicts for the assurance classes and components are summarised in the following table:

Development	ADV	PASS
Security Architecture	ADV_ARC.1	PASS
Functional Specification	ADV_FSP.5	PASS
Implementation Representation	ADV_IMP.1	PASS
TSF Internals	ADV_INT.2	PASS
TOE Design	ADV_TDS.5	PASS
Design compliance with the platform	ADV_COMP.1	PASS
Guidance Documents	AGD	PASS
Operational User Guidance	AGD_OPE.1	PASS
Preparative Procedures	AGD_PRE.1	PASS
Life-cycle Support	ALC	PASS
CM Capabilities	ALC_CMC.4	PASS
CM Scope	ALC_CMS.5	PASS
Delivery	ALC_DEL.1	PASS
Development Security	ALC_DVS.1	PASS
Life-cycle Definition	ALC_LCD.1	PASS
Tools and Techniques	ALC_TAT.2	PASS
Integration of the application	ALC_COMP.1	PASS
Security Target Evaluation	ASE	PASS
ST Introduction	ASE_INT.1	PASS
Conformance Claims	ASE_CCL.1	PASS
Security Problem Definition	ASE_SPD.1	PASS
Security Objectives	ASE_OBJ.2	PASS
Extended Components Definition	ASE_ECD.1	PASS
Security Requirements	ASE_REQ.2	PASS
TOE Summary Specification	ASE_TSS.1	PASS
Consistency of Security Target	ASE_COMP.1	PASS
Tests	ATE	PASS
Coverage	ATE_COV.2	PASS
Depth	ATE_DPT.3	PASS
Functional Tests	ATE_FUN.1	PASS
Independent Testing	ATE_IND.2	PASS
Composite product functional testing	ATE_COMP.1	PASS
Vulnerability Assessment	AVA	PASS

Vulnerability Analysis	AVA_VAN.4	PASS
Composite product Vulnerability assessment	AVA_COMP.1	PASS

10 Evaluator Comments and Recommendations

DES has been included as a security mechanism in the TOE for compatibility with legacy systems. Whenever possible, it is recommended to use triple-DES or AES instead.

11 Bibliography

ST	Security Target for Kapsch SAM 5000, Kapsch TrafficCom, 2018-03-21, revision L, Confidential
STLite	Security Target Lite for Kapsch SAM 5000, Kapsch TrafficCom, 2018-03-21, revision D
PP	Security IC Platform Protection Profile, BSI-PP-0035, 2007-06-15, version 1.0
PlatformST	Security Target Lite M9900, M9905, M9906 including optional Software Libraries RSA-EC-SCL-PSL, Infineon, 2017-08-18, Version 2.8.0
API	Interface Specification for Kapsch 5000, Kapsch TrafficCom, 2018-02-02, revision H
CC	Common Criteria for Information Technology Security, Part 1-3, CCMB-2017-04-001 through 003, version 3.1, revision 5
CEM	Common Methodology for Information Technology Security Evaluation, CCMB-2017-04-004, version 3.1, revision 5
SP-002	Evaluation and Certification, CSEC, 2018-04-24, version 29.0
SP-188	Scheme Crypto Policy, CSEC, 2017-04-04, version 7.0
JIL	Composite product evaluation for Smart Cards and similar devices, JIL, version 1.5, Oct 2017
ARC	Security Architecture requirements (ADV_ARC) for Smart Cards and similar devices, CCRA, CCDB-2014-04-001, version 2.1, Apr. 2014,

Appendix A Scheme Versions

During the certification the following versions of the Swedish Common Criteria Evaluation and Certification scheme has been used.

A.1 Scheme/Quality Management System

During the certification project, the following versions of the quality management system (QMS) have been applicable since the certification application was received:

QMS 1.21 valid from 2017-11-15

QMS 1.21.1 valid from 2018-03-09

QMS 1.21.2 valid from 2018-03-09

QMS 1.21.3 valid from 2018-05-24

In order to ensure consistency in the outcome of the certification, the certifier has examined the changes introduced in each update of the quality management system.

The changes between consecutive versions are outlined in “Ändringslista CSEC QMS 1.21.3”. The certifier concluded that, from QMS 1.12 to the current QMS 1.21.3, there are no changes with impact on the result of the certification.

A.2 Scheme Notes

The following Scheme interpretations have been considered during the certification.

Scheme Note 11 - Methodology for AVA_VAN 4 and 5

Scheme Note 15 - Demonstration of test coverage

Scheme Note 16 - Additional planning requirements

Scheme Note 18 - Highlighted Requirements on the Security Target