Ärendetyp: 6 Diarienummer: 10FMV7611-133:1
Dokument ID FMVID-297-724

Swedish Certification Body for IT Security

Certification Report - Comex Smart Card Reader KT2USB / BioSec Reader

Issue: 1.0, 2013-Dec-19

Authorisation: Daniel Poignant, Lead Certifier , CSEC

Report Distribution: Johan Anstrell, Comex Electronics AB
Daniel Poignant, CSEC
Arkiv

Table of Contents

1 Executive Summary 3

2 Identification 5

3 Security Policy 6
3.1 Information Flow Control 6
3.2 TSF self-testing and function recovery 6
3.3 Residual information protection (user data erasure) 6
3.4 Emergency erase 6
3.5 TOE identification to the host PC 7
3.6 Alerting the user of critical events 7

4 Assumptions and Clarification of Scope 8
4.1 Usage Assumptions 8
4.2 Environmental Assumptions 8
4.3 Clarification of Scope 8

5 Architectural Information 10

6 Documentation 12

7 IT Product Testing 13
7.1 Developer Testing 13
7.2 Evaluator Testing 14
7.3 Evaluator Penetration Testing 15

8 Evaluated Configuration 16

9 Results of the Evaluation 17

10 Evaluator Comments and Recommendations 19

11 Glossary 20

12 Bibliography 21

1 Executive Summary

The Target of Evaluation, TOE, is a smart card reader with a keypad, a fingerprint reader and a display. The TOE consists of hardware, firmware, and documentation, developed by Comex Electronics AB.

The TOE exists in two product families and in three different versions within each product family:

- Comex KT2USB – The Swedish Defence series
  - KT2USB/U1
  - KT2USB/U2
  - KT2USB/STD
- Comex BioSec Reader – An export series
  - BioSec/A
  - BioSec/B
  - BioSec/C

The difference between the models in each series is that they are designed to reduce compromising electromagnetic emanations to various degrees: KT2USB/U1 and BioSec/A have the lowest emanations, KT2USB/STD and BioSec/C the highest. However, reduction of electromagnetic emanations is not part of the evaluation.

The smart card reader's security features are mainly protection of the PIN and fingerprint data by enforcing PIN entry on the keypad and by sending PIN and fingerprint data only to the smart card interface; self-testing and function recovery; user data erasure; TOE identification to the host PC; alerting the user of critical events; emergency erase (only for KT2USB STD/U1/U2 with Swedish Defence smart cards). The KT2USB versions feature an emergency erase button (F1).

The TOE also has security features that have not been considered during the evaluation, including reduction of electromagnetic emanations and tamper protection (a sealing label).

The TOE is delivered as a hardware unit containing firmware and with documentation. The TOE is sealed with a security seal before delivery. It is crucial that the sealing label makes it possible for the customer to detect whether the smart card reader has been opened and that the user checks the sealing label regularly. The sealing label is not part of the evaluation.

No conformance claims to any PP are made for the TOE.

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

The evaluation has been performed by atsec information security AB in Danderyd, Sweden, and was completed on October 21, 2013. The evaluation was conducted in accordance with the requirements of Common Criteria, version 3.1 R4, and the Common Methodology for IT Security Evaluation, version 3.1 R4. The evaluation was performed at the evaluation assurance level EAL4, augmented by ALC_FLR.1 Basic Flaw Remediation.

atsec information security AB is licensed to be an IT Security Evaluation Facility, ITSEF, within the scope of the Swedish Common Criteria Evaluation and Certification Scheme. atsec information security AB is also accredited against ISO/IEC 17025 by the Swedish accreditation body, SWEDAC. This accreditation is necessary to be licensed as an ITSEF by CSEC.

The certifier audited the activities of the evaluators by reviewing all evaluation reports and by overseeing the evaluators performing site visit and testing. The certifier determined that the evaluation results show that the product satisfies all functional and assurance requirements stated in the Security Target [ST]. The evaluators concluded that the Common Criteria requirements for evaluation assurance level EAL4 augmented by ALC_FLR.1 have been met.

The technical information included in this report has been compiled from the Security Target [ST], produced by Comex Electronics AB, and from the final evaluation report produced by atsec information security 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	CSEC2011003

Name and version of the certified IT products

Smart card Reader	Hardware version	Firmware version	Product Article number
Comex KT2USB/U1	P20355-05	KT2USB v1.00.17	X223001-02
Comex KT2USB/U2	P20356-04	KT2USB v1.00.17	X222001-01
Comex KT2USB/STD	P20357-03	KT2USB v1.00.17	X221001-01
Comex BioSec/A	P20355-05	BioSec v1.00.03	X423001-01
Comex BioSec/B	P20356-04	BioSec v1.00.03	X422001-01
Comex BioSec/C	P20357-03	BioSec v1.00.03	X421001-01

Security Target Identification	Comex Smart Card Reader KT2USB / BioSec Reader Security Target, Comex Electronics AB, 2013-06-10, document version 1.21, FMV Dnr: 10FMV7611-109
EAL	EAL 4 + ALC_FLR.1
Sponsor	Comex Electronics AB
Developer	Comex Electronics AB
ITSEF	atsec information security AB
Common Criteria version	3.1 revision 4
CEM version	3.1 revision 4
National and international interpretations	-
Certification completion date	2013-10-21

3 Security Policy

The TOE provides the following security services:

- Information Flow Control *
- TSF self-testing and function recovery
- Residual information protection (user data erasure)
- Emergency erase (only for KT2USB STD/U1/U2 with Swedish Defence smart cards) *
- TOE identification to the host PC
- Alerting the user of critical events

*) For these TOE security features to be enabled the TOE requires the use of specific smart cards, see section 1.4.1 in [ST]:

  - Swedish Defence smart cards shall be used together with a KT2USB smart card reader.
    - TAK (Totalförsvarets Aktiva Kort)
    - TEID (Totalförsvarets Elektroniska ID kort)
    - NBK (Nyckelbärarkort)
    - CEK (Card for Encrypted Keys)
    - DBK (Databärarkort)
    - "Known Type" – future versions of TAK (Totalförsvarets aktiva kort)
  - BioSec smart cards shall be used together with a BioSec smart card reader.
    - BioSec card (a smart card type provided by Comex Electronics AB)

3.1 Information Flow Control

- All information flow between the USB interface and the smart card interface shall pass through the microcontroller (UDFLOW SFP).
- PIN, PUK and fingerprint data entered on the keypad and fingerprint sensor shall only flow to the smart card interface, never to the USB interface (the USB interface is deactivated before enabling user data entry) (NFLOW SFP).
- All ISO7816 PIN and fingerprint commands sent by the host PC to the smart card reader shall be blocked - when the intended smart card types are used (CBLOCK SFP).

3.2 TSF self-testing and function recovery

- TSF shall erase all user data and reset the TOE when:
  - Self-test at start-up discovers an error.
  - Self-test during operation discovers an error.
  - An unexpected exception or interrupt occurs.
  - A watchdog timeout occurs.

3.3 Residual information protection (user data erasure)

- All user data such as PIN, PUK and fingerprint data shall be erased when not needed and before the USB interface is activated.

3.4 Emergency erase

- Only for KT2USB STD/U1/U2 with Swedish Defence smart cards.

- The KT2USB versions of the TOE can erase symmetrical encryption keys and associated data stored on Swedish Defence smart cards having the correct profile, e.g. NBK and TAK. The erasure can be performed without the user having to open the smart card by entering a PIN.

3.5 TOE identification to the host PC

- The TOE identifies itself to the host PC by sending model version number within the USB interface handshake process, when connected to the host PC.

3.6 Alerting the user of critical events

- The TOE alerts the user of critical events on the display and by buzzer sound.

4 Assumptions and Clarification of Scope

4.1 Usage Assumptions

The Security Target [ST] makes one assumption on the usage of the TOE:

- A.USER - The TOE User is trustworthy and trained to use the smart card and the TOE in accordance with any existing security policies. This includes that the user knows how to verify the sealing label before using the smart card reader and knows when to perform emergency erase (if equipped with such a smart card), but also to use Swedish Defence smart cards and BioSec cards only in their respective smart card readers.

4.2 Environmental Assumptions

Four assumptions are made in the ST [ST] on the environment:

- A.SUBSTITUTE - The host PC has the means to check the identity of the smart card reader so that a substitution to another approved model of the smart card reader can be detected.
- A.EMERGENCY - The Swedish Defence smart cards used for storing specific symmetrical encryption keys have the capability of emergency erase, which means erasure of symmetrical encryption keys without first having to open the smart card with a PIN.
- A.SEAL - The sealing label used to seal the TOE cannot be broken or removed and re-attached without the user being able to detect the manipulation.
- A.TAMPERING - The TOE environment must provide the means for the user to detect physical tampering that may affect the integrity of the TSF.

4.3 Clarification of Scope

- All cryptographic operations are performed by the smart cards, not by the smart cart reader itself.
- Reduction of electromagnetic emanations is not part of the evaluation.
- The tampering seal is not part of the evaluation.
- The TOE is intended to be used with specific smart card types to enable all security services of the TOE.

The ST [ST] contains five threats, which have been considered during the evaluation:

- T.RESIDUAL – Exploiting residual information: An attacker may gain access to user data from previous use of the TOE, such as PINs and data entered into the TOE and transferred to and from the TOE and the smart card, by for example having access to, using or dismantling the smart card reader.
- T.LEAKAGE – Information leakage: An attacker may gain access to PIN, PUK or fingerprint data through leakage outside of the smart card reader to any other external interface, such as the USB interface.
- T.TAMPERING – Tampering of the Smart Card Reader: An attacker may alter the TSF to modify or bypass the security mechanisms, for example to gain fraudulent access to user data. This may be done by manipulating or replacing some components in the TOE or by using external interfaces, such as the USB or the smart card interface, to manipulate or replace the TOE firmware or influence its operations.

- T.SUBSTITUTION – Substitution of approved models of the Smart Card Reader: A user may replace the TOE by similar equipment that is not authorized for this specific use and thus leak user data, for example equipment without protection against compromising emanations when such protection is required.
- T.MALFUNCTION – Malfunction of the Smart Card Reader: Malfunction of the TOE may arise from spontaneous hardware or software errors. This may modify or bypass the security mechanisms within the TSF, possibly displaying user data.

The ST [ST] contains three organisational security policies, which have been considered during the evaluation:

- P.EMERGENCY – Emergency erase: The product family KT2USB of the TOE must for all versions of Swedish Defence smart cards, having the correct profile, provide the users the means with an emergency erase and verification, to immediately delete Swedish Defence specific symmetric encryption keys and associated data stored on the smart card. The erasure shall be possible without having to open the smart card, i.e. without having to enter a PIN.
- P.COMMANDS – Filtering of commands: The product family KT2USB of the TOE must for all versions of Swedish Defence smart cards, block all [ISO7816] PIN and fingerprint commands sent from the host PC interface to the smart card interface of the TOE. The product family BioSec Reader of the TOE must for all versions of BioSec smart cards, block all [ISO7816] PIN and fingerprint commands sent from the host PC interface to the smart card interface of the TOE.
- P.RESIDUAL – Erasure of user data: The TOE must erase all user data, such as PINs and data entered into the TOE and transferred to and from the TOE and the smart card, as soon as the data has been processed and is no longer needed.

5 Architectural Information

The TOE is a smart card reader with a keypad, a fingerprint reader and a display. The TOE consists of hardware, firmware, and documentation, developed by Comex Electronics AB. The hardware uses an Atmel AVR32 microprocessor with flash memory.

The TOE exists in two product families and in three different versions within each product family:

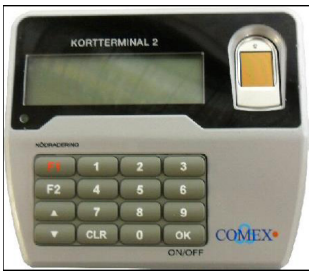
- Comex KT2USB – The Swedish Defence series
  - KT2USB/U1
  - KT2USB/U2
  - KT2USB/STD
- Comex BioSec Reader – An export series
  - BioSec/A
  - BioSec/B
  - BioSec/C

The difference between the models in each series is that they are designed to reduce electromagnetic emanations to various degrees: KT2USB/U1 and BioSec/A have the lowest emanations, KT2USB/STD and BioSec/C the highest. However, reduction of electromagnetic emanations is not part of the evaluation.

The smart card reader's security features are mainly protection of the PIN and fingerprint data by enforcing PIN entry on the keypad and by only sending PIN and fingerprint data to the smart card interface; self-testing and function recovery; user data erasure; TOE identification to the host PC; alerting the user of critical events; emergency erase (only for KT2USB STD/U1/U2 with Swedish Defence smart cards). The KT2USB versions feature an emergency erase button (F1).

Smart card Reader	Hardware version	Firmware version	Product Article number
Comex KT2USB/U1	P20355-05	KT2USB v1.00.17	X223001-02
Comex KT2USB/U2	P20356-04	KT2USB v1.00.17	X222001-01
Comex KT2USB/STD	P20357-03	KT2USB v1.00.17	X221001-01
Comex BioSec/A	P20355-05	BioSec v1.00.03	X423001-01
Comex BioSec/B	P20356-04	BioSec v1.00.03	X422001-01
Comex BioSec/C	P20357-03	BioSec v1.00.03	X421001-01

KT2USB/U1, KT2USB/U2 and BioSec/A, BioSec/B



KT2USB/STD and BioSec/C

The information flow control policies NFLOW SFP and UDFLOW SFP are implemented using three security modes with source code separation (black, yellow, and red). Together with three states of operation (connected, standalone and KOP) a state machine with five states is constructed, see [ST], sections 1.4.4, 1.4.5, and 7.1.1.3.

The KOP state (Key Overwrite Procedure) is used for Emergency Erase, which applies only to KT2USB STD/U1/U2 with Swedish Defence smart cards.

6 Documentation

The following documents are included in the scope of the TOE:

Smart card Reader	Documentation
Comex KT2USB/U1	I TST KT2 USB - Instruktion för Kortterminal 2 USB, 2012-11-06, version 1.2 [ManU1U2]
Comex KT2USB/U2	I TST KT2 USB - Instruktion för Kortterminal 2 USB, 2012-11-06, version 1.2 [ManU1U2]
Comex KT2USB/STD	I TST KT2 USB - Manual för Kortterminal 2 USB STD, 2012-11-06, version 1.2 [ManSTD]
Comex BioSec/A	Comex BioSec Reader - User Guide, 2012-11-06, version 1.1 [ManBioSec]
Comex BioSec/B	Comex BioSec Reader - User Guide, 2012-11-06, version 1.1 [ManBioSec]
Comex BioSec/C	Comex BioSec Reader - User Guide, 2012-11-06, version 1.1 [ManBioSec]

7 IT Product Testing

7.1 Developer Testing

7.1.1 Testing Effort and Approach

The developer used manual tests that tested the following security functionality:

- User data erasure (Residual information protection)
- Emergency erase (only for KT2USB STD/U1/U2 with Swedish Defence smart cards)
- Security modes: Red, Yellow and Black (Information Flow Control: NFLOW SFP, UDFLOW SFP)
- [ISO7816] PIN and fingerprint command blocking (Information Flow Control: CBLOCK SFP)
- Self-testing (TSF self-testing and function recovery)
- Watchdog timer (TSF self-testing and function recovery)
- TOE identification (TOE identification to the host PC)
- Status indication (Alerting the user of critical events)

The developer provided two types of test descriptions "User tests" and "Developer tests".

- The user tests test the TSF that provide externally visible output via TSFIs, e.g. the Key Overwrite Procedure that ensures that the TOE is capable of emergency erase and that this function can be started at any time by pressing F1 key.
- The developer tests test the TSF that does not always provide externally visible output, e.g. USB in Security Mode ensures that the USB endpoint interrupts are enabled only in Black mode. This function is tested by performing source code inspection.

Each test case constitutes of a number of sub-tests where each sub-test tests several functions and interface parameters. The developer testing was used to test each ST claim, all TSFI functions, and subsystems. A separate mapping table presents testing depth and coverage. Testing results were documented for all six versions of the TOE.

7.1.2 Test Configuration

The user tests' configuration was Windows 7, KrAPI, and KT2USB/BioSec Windows driver. The tests were performed on the smart card readers, as specified in Chapter 8 Evaluated Configuration, unless it was stated to use the in-circuit emulator instead.

The developer tests' configuration was Windows 7, KrAPI, KT2USB/BioSec Windows driver, and AVR32 Studio. The tests were performed on the smart card readers, as specified in Chapter 8 Evaluated Configuration, but using AVR32 Studio to enable test code and to set breakpoints. The JTAG programmers used were JTAGICE mkII or AVR ONE.

7.1.3 Coverage and Depth

The tested behaviour was covered down to the level of subsystems, and the evaluator could verify that most relevant execution paths were taken into account. Most test cases directly referred to SFRs, TSFIs as well as subsystems and modules.

7.1.4 Results

The testing was successful for all TOE configurations.

7.2 Evaluator Testing

7.2.1 Testing Effort

The evaluators verified the developer testing by re-running all the developer tests and six out of eight of the user tests. Additionally, the evaluators devised eleven independent tests covering "unexpected power loss", "emergency erase", "command blocking", "TOE identification", "APDU buffer" and "fingerprint buffer erase".

7.2.2 Approach

First, the evaluator analyzed the coverage and depth of the developer testing, and then the evaluator chose a subset of them to be re-run and devised new independent tests. The evaluator was focusing on the external interfaces, the USB interface, and the smart card interface.

The independent testing was performed in two phases:

- the original independent testing on 2012-05-24 and 2012-05-15
- the additional independent testing on 2013-01-18

The TOE was updated as a consequence of the first testing. Parts of the evaluator testing was reperformed on the updated TOE.

The evaluator tested three versions of the smart card reader: KT2USB/U1 and BioSec/C in May 2012 and KT2USB/U2 and BioSec/C in January 2013.

Smart card Reader	Hardware version	Firmware version	Date
KT2USB/U1	P20355-03	KT2USB v1.00.16	2012-05-24
BioSec/C	P20357-03	BioSec v1.00.02	2012-05-25
KT2USB/U2	P20356-04	KT2USB v.1.00.17	2013-01-18
BioSec/C	P20357-03	BioSec v.1.00.03	2013-01-18

All independent tests were executed in the developer's testing environment.

7.2.3 Test Configuration

The evaluator executed independent testing on three versions of the smart card reader: KT2USB/U1, KT2USB/U2, and BioSec/C. The evaluator used various smart cards to test specific smart card functionality that is only available in conjunction with certain smart card profiles.

7.2.4 Coverage and Depth

Execution of the developer's tests covered all security-relevant interfaces and subsystems. The additional evaluator tests covered the following security functions described in section 7 in [ST]:

- TSF_ERASE - Unexpected power loss, Fingerprint buffer erase
- TSF_EMERGENCY - Emergency erase
- TSF_CBLOCK - Command blocking

- TSF_ID - TOE identification

7.2.5 Results

The independent testing was performed in two phases:

- During the original independent testing on 2012-05-24 and 2012-05-15, the evaluator confirmed the test results of the developer testing, i.e. all actual developer test results were consistent with the expected test results. However, the TOE could not demonstrate expected behaviour for all additional evaluator tests.
- During the additional independent testing on 2013-01-18, the evaluator re-run test cases that failed during the independent testing in May 2012, re-run a sample of developer tests and performed an additional ad hoc test. The actual test results matched the expected results and no deviations were observed.

7.3 Evaluator Penetration Testing

The evaluator conducted source code review of the code handling critical security functionality such as USB communication and user data erasure. The evaluator also performed negative variations of functional tests during testing. No penetration testing beyond this was performed on the TOE by the evaluator since the evaluator has determined that no potential vulnerabilities, that would be candidate for testing, exist.

8 Evaluated Configuration

The evaluated configurations of the TOE are:

Smart card Reader	Hardware version	Firmware version	Product Article number
Comex KT2USB/U1	P20355-05	KT2USB v1.00.17	X223001-02
Comex KT2USB/U2	P20356-04	KT2USB v1.00.17	X222001-01
Comex KT2USB/STD	P20357-03	KT2USB v1.00.17	X221001-01
Comex BioSec/A	P20355-05	BioSec v1.00.03	X423001-01
Comex BioSec/B	P20356-04	BioSec v1.00.03	X422001-01
Comex BioSec/C	P20357-03	BioSec v1.00.03	X421001-01

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 ST [ST] for an attack potential of Enhanced-Basic.

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

The evaluators overall verdict is: PASS.

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

Assurance Class Name / Assurance Family Name	Short name (including component identifier for assurance families)	Verdict
Development	ADV	PASS
Security Architecture	ADV_ARC.1	PASS
Functional specification	ADV_FSP.4	PASS
Implementation representation	ADV_IMP.1	PASS
TOE design	ADV_TDS.3	PASS
Guidance documents	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.4	PASS
Delivery	ALC_DEL.1	PASS
Development security	ALC_DVS.1	PASS
Flaw remediation	ALC_FLR.1	PASS
Life-cycle definition	ALC_LCD.1	PASS
Tools and techniques	ALC_TAT.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
Tests	ATE	PASS
Coverage	ATE_COV.2	PASS
Depth	ATE_DPT.1	PASS
Functional tests	ATE_FUN.1	PASS
Independent testing	ATE_IND.2	PASS
Vulnerability assessment	AVA	PASS
Vulnerability analysis	AVA_VAN.3	PASS

10 Evaluator Comments and Recommendations

The evaluators do not have any comments or recommendations concerning the product or using the product.

11 Glossary

CC	Common Criteria for Information Technology Security, set of three documents, CC Part 1-3, standard for security evaluation of IT products
CEM	Common Methodology for Information Technology Security, document describing the methodology used in Common Criteria evaluations
ITSEF	IT Security Evaluation Facility, test laboratory licensed to operate within a evaluation and certification scheme
PP	Protection Profile, document containing evaluation requirements and specifications for a product category
ST	Security Target, document containing security requirements and specifications , used as the basis of a TOE evaluation
TOE	Target of Evaluation
TSFI	TOE Security Functional Interface

12 Bibliography

ST	Comex Smart Card Reader KT2USB / BioSec Reader Security Target, Comex Electronics AB, 2013-06-10, document version 1.21, FMV Dnr: 10FMV7611-109
CC	Common Criteria for Information Technology Security Evaluation, Version 3.1 rev 4, CCMB-2012-09-001, CCMB-2012-09-002, CCMB-2012-09-003, September 2012
CEM	Common Methodology for Information Technology Security Evaluation, Version 3.1 rev 4, CCMB-2012-09-004, September 2012
SP-002	SP-002 Evaluation and Certification, CSEC, 2013-06-17, document version 19.0, FMV Dnr: 13FMV1287-86:1
ManBioSec	Comex BioSec Reader - User Guide, Comex Electronics AB, 2012-11-06, document version 1.1, FMV Dnr: 10FMV7611-68
ManSTD	I TST KT2 USB - Manual för Kortterminal 2 USB STD, Comex Electronics AB, 2012-11-06, document version 1.2, FMV Dnr: 10FMV7611-70
ManU1U2	I TST KT2 USB - Instruktion för Kortterminal 2 USB, Comex Electronics AB, 2012-11-06, document version 1.2, FMV Dnr: 10FMV7611-69