Swedish Certification Body for IT Security

Certification Report Färist 4

Issue: 1.0, 2015-jun-17

Authorisation: Jerry Johansson, Lead Certifier , CSEC

Table of Contents

1 Executive Summary

The Target of Evaluation, TOE, is the VPN firmware part of a complete appliance. The hardware, and a Linux operating system for the administrative subsystem, are outside the scope of the TOE. The product can be extended with a filter providing firewall functionality to the VPN channel. In the evaluated configuration a filter without firewall functionality was used. Also, please note that the correct usage of cryptographic functions is covered by the evaluation, but the implementation of the cryptographic module is not.

The TOE is available in two different versions, the Färist and the Färist Micro. The Färist supports both IPSec and MACSec, the Färist Micro only supports IPSec. The main purpose of the product is to connect two networks securely, on OSI level 2 or 3, i.e. the Färist will work as a router or a bridge, the Färist Micro as a router, where the data is encrypted during transport between the networks.

The evaluation covers the VPN functionality, auditing, management of the security functions, automatic updating, and self-test.

The TOE is delivered pre-installed on an appliance, along with the user guidance.

The ST does not claim conformance to any Protection Profile.

The evaluation has been performed by atsec information security AB in their premises in Danderyd, Sweden, and was completed on the 27th of May 2015. The evaluation was conducted in accordance with the requirements of Common Criteria, version 3.1, release 4, and the Common Methodology for IT Security Evaluation, version 3.1, release 4. The evaluation was performed at the evaluation assurance level EAL 5, augmented by ALC_FLR.1 Basic flaw remediation.

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

The certifier monitored the activities of the evaluator by reviewing all successive versions of the evaluation reports. The certifier determined that the evaluation results confirm the security claims in the Security Target [ST], and have been reached in agreement with the requirements of the Common Criteria and the Common Methodology for evaluation assurance level:

EAL 5 + ALC_FLR.1.

The certification results only apply to the versions of the products indicated in the certificate, and on the condition that all the stipulations in the Security Target [ST] are met.
This certificate is not an endorsement of the IT product by CSEC or any other organization that recognizes or gives effect to this certificate, and no warranty of the IT product by CSEC or any other organization that recognizes or gives effect to this certificate is either expressed or implied.

2 Identification

Certification Identification

Certification ID	CSEC2013002
Name and version of the certified IT product and the TOE	Färist 4.0.1 and Färist Micro 4.0.1 with the Färist 4.0.1 firmware
Security Target	Färist 4 - Security Target, Tutus AB, 2015-06-08, document version 2.0
Assurance level	EAL 5 + ALC_FLR.1
Sponsor	Tutus AB
Developer	Tutus AB
ITSEF	atsec information security AB
Common Criteria version	3.1 release 4
CEM version	3.1 release 4
Recognition scope	CCRA, SOGIS, EA/MLA
Certification date	2015-06-17

3 Security Policy

The TOE provides the following security services:

- VPN
- Audit
- Management
- Automatic Update
- Self-test

3.1 VPN

The VPN functionality is the main security functionality of the Färist. It creates private networks over public networks using encryption.

The key exchange and authentication is done with the SKUT protocol using an RSA-signed Diffie-Hellman key exchange. Encryption is done using either IPSec ESP in tunnel mode or MACSec with the AES encryption algorithm.

The cryptographic library for the VPN functionality is implemented in a proprietary library provided by the Swedish NCSA.

3.2 Audit

Audit records that are created in different components are sent to a log daemon, which will forward the audit records to one or more remote log servers.

If the log servers are not reachable the log will be kept in RAM until it can be sent.

A smaller number of the latest log events are also kept in a local audit file.

3.3 Management

The TOE supports the following administrative roles:

- Administrator
  - Remote administrator

    The remote administrator can perform all administrative tasks. Changing keys however requires local access to the machine, which means that by not allowing the administrator local access, key management can be handled solely by the key manager.

    The remote administrator is authenticated through his certificate.
  - Local administrator

    The local administrator can perform the basic administrative tasks using the front panel. The local administrator is authenticated through organizational means, by allowing only authorized personnel physical access to the TOE.
- Operator

  The (remote) operator can perform the same tasks as the remote administrator but cannot perform any changes, such as changing configuration. The operator is authenticated through his certificate.
- Key manager

  The key manager can change cryptographic keys by either changing the smart card or reading a new key from the USB memory.

Remote management requires authentication using X.509 certificates.

Note that the environment must ensure that physical access are provided only to the local administrators and the key managers.

3.4 Automatic Update

The TOE has an automatic update functionality that checks for new firmware updates, downloads, verifies the origin and integrity of the update and ensures that the update is newer than the current version before the update is installed. Note that after an update, the Färist version will not be the certified version anymore.

3.5 Self-test

The TOE has built-in functionality self tests that are run both at startup and at regular intervals. Self tests verify the integrity of the system files and ensure the proper working of the encryption engine. If a self test fails the TOE will preform a restart.

If the USB-memory or smart card holding the RSA certificate/private key is removed, the TOE will also restart.

4 Assumptions and Clarifications of Scope

4.1 Usage Assumptions

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

A.NOEVIL - Authorised administrators given privileges, are competent, nonhostile and follow all their guidance; however, they are capable of error.

4.2 Environmental Assumptions

Seven assumptions on the environment are made in the Security Target.

A.AUDIT - The TOE environment must be able to receive, store and protect the audit records generated by the TOE and provide the means for audit analysis.

A.DHPARA - The Diffie-Hellman parameters of the TOE and the remote host are of good quality.

A.KEYS - It is assumed that private RSA keys used for remote administration and the VPN tunnel are of high quality and not disclosed.

A.NOEMA - Interception of emanation of any kind is addressed by environmental controls that reduce the signal to noise ratio for an interceptor to a level that prohibits useful evaluation of the intercepted signals.

A.PHYSEC - The TOE is physically secure, i.e. no unauthorised persons have physical access to the TOE and its underlying system.

A.RELHARD - The underlying hardware, firmware (BIOS and device drivers) and the operating system functions needed by the TOE to guarantee secure operation, are working correctly and have no undocumented security critical side effect on the functions of the TOE.

A.TIME - The TOE environment provides the TOE with a reliable time stamp.

4.3 Clarification of Scope

The Security Target [ST] contains eight threats, which have been considered during the evaluation.

T.DISCLOSE - An external attacker gains unauthorised access to information transmitted between the TOE and a remote trusted network.

T.CHANNEL - An external attacker gain unauthorized access to information or resources in the trusted network by breaking out of the secure channel over the trusted network.

T.INISEC - For configuration settings which are not provided by an administrator, insecure default values may be set by the TOE.

T.MEDIATE - An attacker on the clear interface sends information through the TOE to the crypto interface without sending it through the trusted channel; and an attacker using the trusted tunnel on the crypto interface will break out of the trusted channel and generate traffic on the crypto interface outside of the trusted channel.

T.MODIFY - The attempts of an external attacker to modify data transmitted between the TOE and a remote trusted network goes undetected.

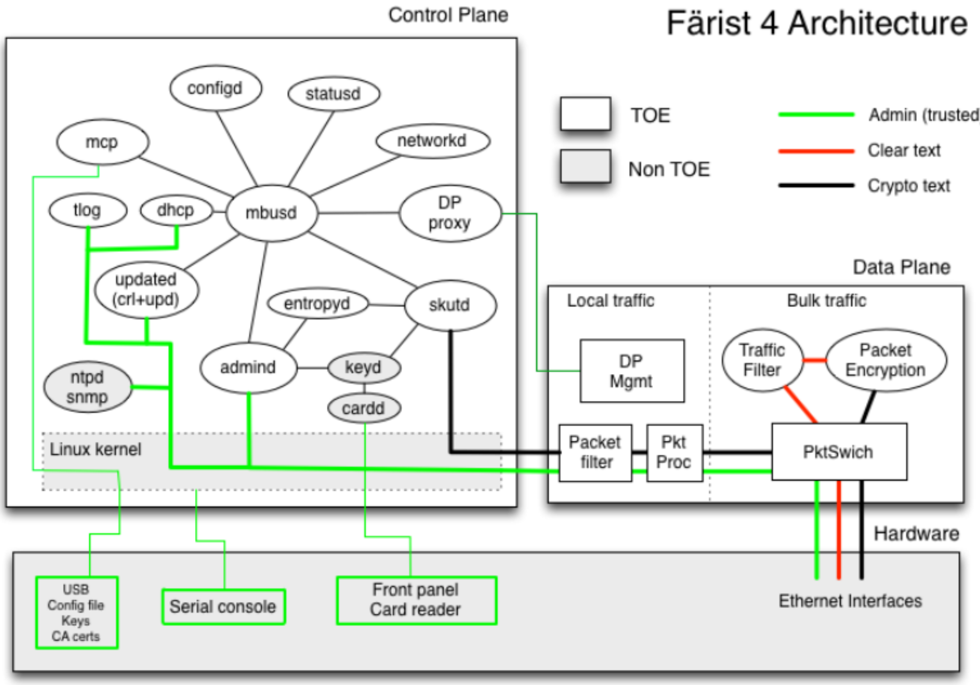
T.ADMIN - An attacker may be able to perform administration or configuration of the TOE, or gain access to administration information and configuration data, such as secret keys or audit records, or may be able to modify such data.

T.SELPRO - An attacker may read, modify, or destroy TOE internal data by transmitting data to the TOE via one of its network connections that causes modification or deletion of TOE internal data.

T.UPDATE - Attacker may provide malicious TOE updates or old versions of the TOE software to introduce back-doors or exploitable weaknesses into the TOE.

5 Architectural Information

The TOE consists of two subsystems, the control plane and the data plane. The data plane is further subdivided into a “local traffic” and a “bulk traffic” part. The control plane runs on top of a Linux kernel while the data plane operates directly on top of the hardware. All packets are received by the data plane and a check is first made to see if the packet is directed to the TOE itself, in which case the traffic is filtered before it is sent to the control plane. All other traffic is sent to the crypto engine and filter system in the data plane. The components of all subsystems are described below.



Note: Non TOE modules have connections over MBus not shown on the figure

Version 1.8
2014-05-02

Figure 1: Färist 4 Architecture

The network interfaces for user traffic are designated “crypto” (i.e. carrier network) and “clear” (i.e. tunnelled network). The designation indicates which kind of information is flowing through them.

The roles of the individual parts are explained in the ST.

6 Documentation

The following document is included in the scope of the TOE:

Färist 4 Administrator's manual [Admin]

7 IT Product Testing

7.1 Developer Testing

The developer performed extensive testing of all functionality, using a proprietary automated test framework. The framework contains physical instances and virtualized instances of Färist, hosts, and clients, enabling highly complex network environments. Some manual testing was done to cover features that are difficult to automate. The testing of the security features is a subset of the developer testing.

The Färist 4.0.1 was tested using the R200 and H300 hardware platforms, the Färist Micro 4.0.1 was tested using the C200 hardware platform.

7.2 Evaluator Testing

The evaluators repeated all automated developer test cases, using the developer's framework. The evaluators found that the developer's testing had good coverage of TSFI and modules, and mainly added manual negative test cases for the independent testing.

The evaluator's testing was done using the R200 hardware platform.

7.3 Evaluator Penetration Testing

The evaluators performed portscans, tests for some specific vulnerabilities, automated fuzz testing of many of the exposed protocols. Code review was used instead of fuzzing for the remaining accessible protocols. Testing was focussed on the protocols that are visible for an attacker.

The fuzz testing was done using one Färist on the R200 and one Färist Micro on the C200 platform.

8 Evaluated Configuration

The Färist 4.0.1 is delivered as a complete appliance, comprised of the TOE, a Linux operating system, and either the R200 or the H300 hardware platform.

The Färist Micro 4.0.1 is also delivered as a complete appliance, comprised of the TOE, a Linux operating system, and the C200 hardware platform.

The software is pre-installed, and guidance for secure configuration is found in the Administrator Guide [Admin].

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 respective assurance classes and components are summarised in the following table:

Assurance Class/Family		*Short name*	*Verdict*
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.4	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
	Flaw Remediation	ALC_FLR.1	PASS
	Life-cycle Definition	ALC_LCD.1	PASS
	Tools and Techniques	ALC_TAT.2	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.3	PASS
	Functional Tests	ATE_FUN.1	PASS
	Independent Testing	ATE_IND.2	PASS
Vulnerability Assessment		AVA	PASS
	Vulnerability Analysis	AVA_VAN.4	PASS

10 Evaluator Comments and Recommendations

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

11 Glossary

AES	Advanced Encryption Standard
CBC	Cipher Block Chaining
ESP	Encapsulating Security Payload (IPsec)
HMAC	Hashed Message Authentication Code
IEEE	Institute of Electrical and Electronics Engineers, Inc.
IP	Internet Protocol
IPSec	Internet Protocol Security
MAC	Message Authentication Code
MACSec	MAC Security
NTP	Network Time Protocol
SFR	Security Functional Requirement
SHA	Secure Hash Algorithm
SKUT	Simple key-exchange using TLS
SMTP	Simple Mail Transfer Protocol
SNMP	Simple Network Management Protocol
TOE	Target of Evaluation
TSF	TOE Security Functionality
TSFI	TSF Interface
USB	Universal Serial Bus

12 Bibliography

ST Färist 4 - Security Target, Tutus AB, 2015-06-08, document version 2.0

Admin Färist 4 Administrator's manual, Tutus AB, 2014-11-14, document version 1.0.2

CCpart1 Common Criteria for Information Technology Security Evaluation, Part 1, version 3.1 revision 4, CCMB-2012-09-001

CCpart2 Common Criteria for Information Technology Security Evaluation, Part 2, version 3.1 revision 4, CCMB-2012-09-002

CCpart3 Common Criteria for Information Technology Security Evaluation, Part 3, version 3.1 revision 4, CCMB-2012-09-003

CC CCpart1 + CCpart2 + CCpart3

CEM Common Methodology for Information Technology Security Evaluation, version 3.1 revision 4, CCMB-2012-09-004

SP-002 SP-002 Evaluation and Certification, CSEC, 2014-12-12, document version 22.0

SP-188 SP-188 Scheme Crypto Policy, CSEC, 2013-06-18, document version 4.0

SN-11 Scheme Note 11, CSEC, 2013-01-31, document version 1.0

Appendix A - QMS Consistency

During the certification project, the following versions of the quality management system (QMS) have been applicable since the certification application was received 2013-05-20:

QMS 1.14	valid from 2013-02-22
QMS 1.15	valid from 2013-10-23
QMS 1.16	valid from 2014-02-13
QMS 1.16.1	valid from 2014-03-27
QMS 1.16.2	valid from 2014-07-07
QMS 1.17	valid from 2014-11-20
QMS 1.17.1	valid from 2014-12-02
QMS 1.17.2	valid from 2015-01-13
QMS 1.17.3	valid from 2015-01-29

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 QMS 1.17.3”.

The certifier concluded that, from QMS 1.14 to the current QMS 1.17.3, there are no changes with impact on the result of the certification.