Swedish Certification Body for IT Security

Certification Report - Färist 2.5.2-RELEASE

Issue: 1.0, 2007-Oct-30

Responsible: Jerry jyjoh Johansson

Authorisation: Dag Ströman, Technical Manager , VG CSEC

Table of Contents

1 Executive Summary

The Target of Evaluation, TOE, is part of the Färist Firewall and VPN , developed by Tutus Data AB. Notably, the IP stack is included in the TOE. The Färist provides application level proxies, IP filtering, VPN functionality, and failover capabilities. All traffic will pass through a proxy and/or the VPN-crypto. Remote administration is possible through a secure channel. There are two versions of Färist covered by the evaluation, the Firewall version (Färist 2.5.2-RELEASE) and the VPN version (Färist 2.5.2-R-RELEASE). The difference between the versions is that the VPN version will not work in firewall only mode.

The cryptographic module used by the TLS and IPSEC protocols are provided by the Swedish government and are not considered part of the TOE. The implementation of the TLS and IPSEC protocols are part of the TOE, while the cryptographic module is not. It is not possible to change which cryptographic module is used. The Färist has been developed for the Swedish government.

The Färist product is delivered on an all-in-one install CD, including the TOE, additional proxies, the remaining parts of FreeBSD 6.2, and the Administrator's Manual. The CD is marked with either Färist 2.5.2-RELEASE or Färist 2.5.2-R-RELEASE.

The Färist is designed to run on Intel x86 compatible PCs with two ethernet cards.

There is one probablilistic mechanism with a strength of function claim in the security target, i.e. the integrity check of received NTP packets, for which the claim is SOF-high.

No conformance claim to any protection profile is made for Färist.

There are ten assumptions made in the ST regarding the secure usage and environment of the Färist. The TOE rely on these being met to counter the thirteen threats, and to fulfill the one organisational security policy (OSP) in the ST. The assumptions, the threats, and the organisational security policy 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 the 9th of October 2007. The evaluation was conducted in accordance with the requirements of Common Criteria, version 2.3, Part 2 and Part 3, and the Common Methodology for IT Security Evaluation, CEM, version 2.3. The evaluation was done at the evaluation assurance level EAL4, augmented by ALC_FLR.1 Basic Flaw Remediation.

Atsec Information Security AB is under licensing to be an IT Security Evaluation Facility, ITSEF, within the scope of the Swedish Common Criteria Evaluation and Certification Scheme, and has been granted a conditional license allowing them to perform trial evaluations under the supervision of CSEC. The evaluation of Färist has served as such a trial evaluation. Atsec Information Security AB is also under accreditation against ISO/IEC 17025 by the Swedish accreditation body, SWEDAC. A successful trial evaluation, and accreditation against ISO/IEC 17025 is necessary to be licensed as an ITSEF by CSEC.

The certifier monitored the activities of the evaluators by reviewing all work units in all successive versions of the evaluations reports, and by observing the evaluators performing site visits 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 certifier concluded that the evaluator's findings are accurate, the conclusions justified, and the conformance results correct. The conclusions of the evaluators in the final evaluation report are consistent with the evidence provided. 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 Färist 2.5.2 [ST], produced by Tutus Data 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.

The cryptographic algorithms in this product has not been analysed or tested to conform to cryptographic standards during this evaluation. All cryptography has only been asserted as tested by the vendor.

2 Identification

The TOE is part of the Färist Firewall and VPN product, including the IP stack, which is delivered on an all-in-one install CD, with the remaining parts of FreeBSD version 6.2 and the Administrator's Manual. The CD is marked with either Färist 2.5.2-RELEASE or Färist 2.5.2-R-RELEASE. The full version identifier is also visible on-screen using the remote administration interface. The manual is marked with Färist 2.5.

Certification Identification	
Certification ID	CSEC 2006001
Name and version of the certified IT product	Färist 2.5.2-RELEASE Färist 2.5.2-R-RELEASE
Security Target Identification	Security Target Färist, Release 2.5.2, Tutus Data AB, 2007-09-20, Document version 2.1
Common Criteria version	2.3 as of August 2005
CEM version	2.3 as of August 2005
EAL	EAL4 + ALC_FLR.1
National and international interpretations	Scheme Note 5 (Scheme crypto policy) Scheme Note 8 (Guide to evaluation of crypto)
Sponsor and Developer	Tutus Data AB Svärdvägen 11 SE-182 33 Danderyd PoC: Per Holmer, President of Tutus Data AB +46 8 551 102 30 per.holmer@tutus.se
ITSEF	atsec information security AB Svärdvägen 11 SE-182 33 Danderyd PoC: Staffan Persson, President/Head of ITSEF +46 8 551 104 00 staffan.persson@atsec.com
Certification Body	CSEC SE-115 88 Stockholm PoC: Jerry Johansson, Lead Certifier +46 8 782 66 43 jerry.johansson@fmv.se
Quality Assurance, CSEC	Anders Staaf, Certifier Dag Ströman, Technical Manager
Certification completion date	2007-10-23

3 Security Policy

The security functionality of the TOE is divided into services and outlined below.

3.1 Security Audit

The TOE generates audit data for events associated with the communication links it monitors. The full set of auditable events are listed in the ST, section 5.1.1.1. Administrators are able to select the audited events from this list, and to read the log file via the remote administration tool.

3.2 Cryptographic Support

For all incoming NTP packets, a keyed MD5 hash sum is checked to verify the origin and integrity of the packet.

After identifying and authenticating, RSA key exchange is performed for remote administrators and failover peers, RSA signed Diffie-Hellman key exchange is performed for users requesting restricted access to the internal network. The data is protected using AES 256 or 3DES encryption and SHA-1 hash.

The IPSEC VPN data streams are encrypted using AES 256 or 3DES, and integrity protected using SHA-1 HMAC with a 160 bit key. The key exchange is done using SKUT.

Note that the implementation of the cryptographic algorithms is provided by the Swedish government and is not included in the TOE.

3.3 Information Flow Control

There are two security function policies for information flow control, and one for access control, in the ST.

The information flow policies are the *Unauthenticated SFP*, and the *Authenticated SFP*. The access control policy is the *Authenticated User Access SFP*.

The *Unauthenticated SFP* applies to internal and external entities that have not been authenticated, is based on source and destinaltion IP address, port number, protocol type, and protocol specific rules. The protocol must be one of the supported, and the source and destination IP addresses has to be explicitly allowed for the protocol. IP packets with an IP address that belongs to the internal/external network has to arrive at the corresponding network interface. IP packets that arrive in wrong context and does not belong to an axisting TCP connection are denied.

The *Authenticated SFP* applies to IP packets arriving through an established VPN channel, where the remote VPN endpoint has been authenticated. Outgoing IP packets has to have a destination IP address that belongs to the network at the remote end of the VPN channel.

The *Authenticated User Access SFP* applies to remote administrators, failover peer firewalls, and users accessing services requiring authentication (as configured in the TCP plug proxy). The user or firewall peer must have a known X.509 certificate, which has been listed in the respective access control list, and must pass the authentication to be allowed access to the requested service.

3.4 Identification and Authentication

Remote administrators, failover peers, and users requesting access to services configured to require authentication by the TCP plug proxy, are mutually authenticated, i.e. the TOE also authenticates itself to the other party. This is done using TLS v1 and X.509 certificates.

When establishing an IPSEC VPN connection, the endpoints are mutually authenticated using TLS v.1 and X.509 certificates.

3.5 Security Management

The TOE has well-defined initial default values. Initial configuration is done using a local configuration tool. During normal operation, a more convenient remote interface may be used for configuration and audit review. To access the local tool, the administrator needs physical access and a username/password to the underlying operating system. To access the remote interface, an administrator will have to be authenticated using a X.509 certificate.

3.6 Protection of the TOE Security Functions

The TOE has been designed to enforce that all incoming packets have to be inspected by one of the proxies, and/or encrypted/decrypted, before it can reach an outgoing interface.

3.7 Trusted Communication Path

Using Färist as VPN endpoints, it is possible to connect trusted networks over an insecure network. The VPN endpoints has to be mutually authenticated, and all the information flowing through the VPN channel will be confidentiality and integrity protected cryptographically.

4 Assumptions and Clarification of Scope

In order to function securely, the TOE relies upon a number of assumptions being met in the operational environment. These are listed in section 4.1 and 4.2 below.

Threats against the environment and considerations about the cryptographic functionality are discussed in section 4.3.

4.1 Usage Assumptions

A.AUTKEY - It is assumed that private keys used for the certificates imported to the TOE are of high quality and not disclosed, replaced or modified. This applies to the private keys of the certificates for the administrators, the users, the server, as well as for the certificates used by the VPN connection.

A.GENPUR - There are no general-purpose computing capabilities (e.g., the ability to execute arbitrary code or applications) on the TOE. The underlying system of the TOE is solely deployed to host the TOE.

A.MD5KEY - It is assumed that secret keys used for the generation and verification of the keyed MD5 hash sums are of high quality, are not disclosed and do belong to the assigned NTP server.

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

A.SINGE - The connection from the TOE to an external trusted network using the VPN functionality has only one connection point on the other network, i.e. the external network meets the assumption A.SINGI for its Färist.

A.SINGI - Information cannot flow among the internal and external networks unless it passes through the TOE or a failover firewall to the TOE, i.e. the TOE or its failover firewall is the only connection point between those two networks.

A.PEERTRUST - The TOE firewall peers that are configured as failover must be trustworthy. That means that they are all under the same administration as the TOE, identically configured and that the same assumptions can be made about them as for the TOE.

4.2 Environmental Assumptions

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.

4.3 Clarification of Scope

All threats to the TOE, as specified in the ST, are countered by the TSF. Therefore only the threats to the TOE environment are listed, since they are countered by the environment rather than the TOE.

TE.AUDIT - An attacker may manipulate the underlying system of the TOE in a way that authorised administrators are not able to read the audit data via console access.

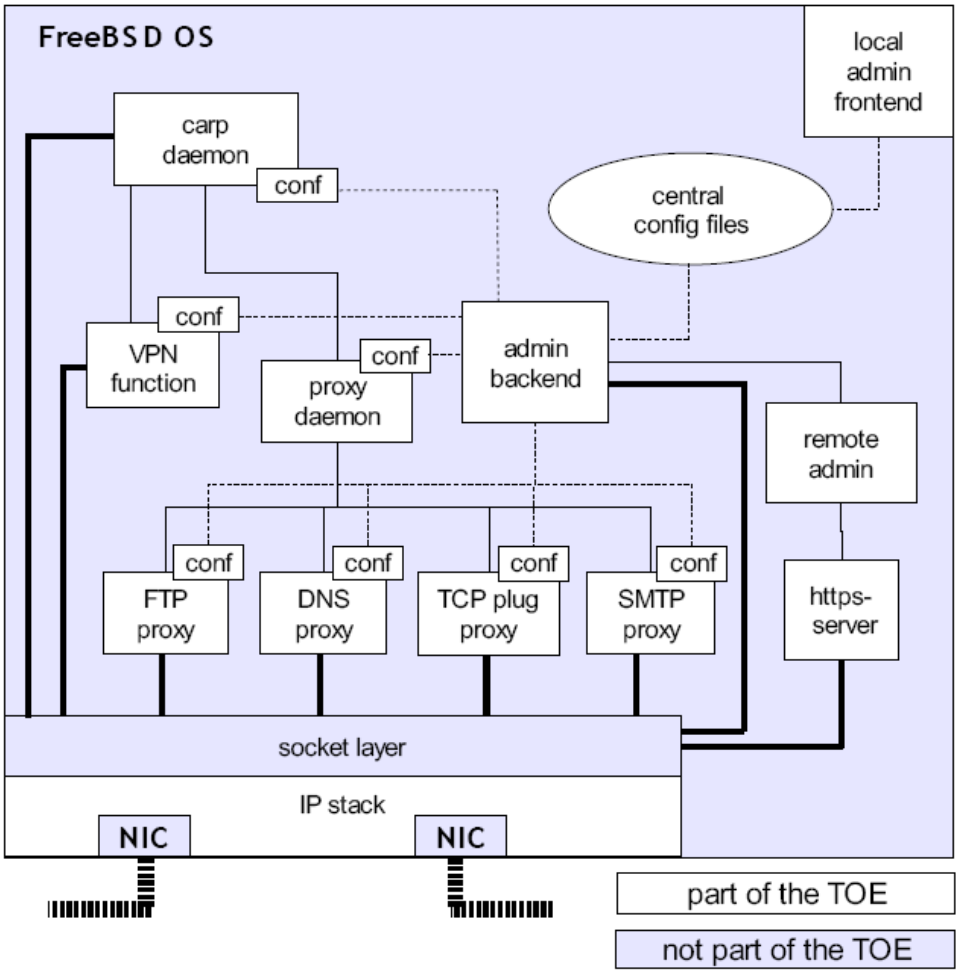
TE.FILE - An attacker may gain the possibility to alter user or TSF data without being detected.

TE.INFO - An attacker may gain access to TSF data (like TLS session keys used for the remote administration encryption) by allocating memory on the underlying operating environment which still contains such data from a previous allocation.

The cryptographic algorithms in this product has not been analysed or tested to conform to cryptographic standards during this evaluation. All cryptography has only been asserted as tested by the vendor.
The implementation of the cryptographic module is excluded from the TOE, but the correctness of the calls to the cryptographic module is covered by the evaluation.
The boundary of the cryptographic module coincides with the cryptographic engine boundary in OpenSSL.

5 Architectural Information

The TOE includes the parts of Färist 2.5.2-RELEASE and Färist 2.5.2-R-RELEASE identified in the picture below, using FreeBSD version 6.2 as the underlying operating system.



The TOE consists of the following parts:

- the FTP-proxy,
- the SMTP-proxy consisting of omb_smtp and omb_smtpd,
- the DNS-proxy,
- the TCP Plug-proxy,
- the VPN functionality consisting of vpnd and skutd,
- the failover system consisting of the proxy daemon and carp daemon
- the IP stack of the kernel including
  - the FreeBSD packet filter
  - the VPN-check routing function,
  - the packet screening daemon,
- the PHP-based remote administration tool including

  - the reboot cgi application,
  - the https server
- administration backend, consisting of
  - modifications to the FreeBSD sysinstall program,
  - fwadmin wrapper script,
  - fconfig and its wrapper newfconfic
  - the configuration daemon configd using the configc and config_sync script.

working together as described in the security target, chapter 2.

The cryptographic module implementation is excluded from the TOE (note this does not show in the figure). The boundary of the excluded part corresponds precisely to the boundary of the OpenSSL cryptographic engine.

All components are handled under version control and are part of the Färist 2.5.2-RELEASE, Färist 2.5.2-R-RELEASE.

6 Documentation

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

Färist Administrator's Manual, Release 2.5, Tutus Data AB, 2007-08-22, document version 2.9.3.

7 IT Product Testing

7.1 Developer Testing

7.1.1 TOE test configuration

All developer testing was conducted in the developer's test environment, providing a suitable test network with machines to access services on the inside and outside interfaces of the TOE, and to connect to the TOE for remote administration tasks.
A BSD or Windows XP based PC was used either in the internal or external network (relative to the TOE) as external testing system. Standard services (SMTP relay, SSH host, DNS server and FTP server) were provided in the test environment as was a gateway to the Internet.
The TOE itself was installed on the Färist 40100c4HD hardware, which is a standard PC with a 32 bit Intel architecture CPU, 256 MB of main memory, 40GM hard disk and 4 standard 10/100 MBit Ethernet ports.
A clean install of the TOE software (FÄRIST 2.5.2-RELEASE and FÄRIST 2.5.2-R-RELEASE) was performed upfront, and the machines were set up according to the specifications in the developer test plan.
The evaluators verified that the test environment corresponded to the evaluated configuration as described in the Security Target.

7.1.2 Testing approach

The developer performed all tests by stimulating external interfaces of the TOE. This is considered to be sufficient due to the information flow between the TOE subsystems – it is always clearly defined to which subsystem information, given to an external interface, will be transferred via the internal interfaces.
The developer's overall approach was to send valid and invalid input to the external interfaces, and evaluating the behavior observed and output obtained (error messages and log files). All tests were performed manually and the results recorded.
The developer performed a total of 33 tests, covering both parallel and serial tunnel mode of the TOE, exercising all security functions through their external interfaces. Implicitly, audit and management functions (local and remote administration) were exercised in all tests when setting up the test conditions and when observing the output of the tests.

7.1.3 Test results

All developer testing was performed according to plan. The expected results were met in each case and the evaluators were able to determine that the developer testing provides sufficient support for the evaluation.
Note that the cryptographic algorithms in this product has not been analysed or tested to conform to cryptographic standards during this evaluation. All cryptography has only been asserted as tested by the vendor.

7.2 Evaluator Testing

The evaluators conducted their independent testing after the site visit on June 13-14, 2007. As required by CEM, they split their test effort into

1. the repetition of developer test samples and

2. independent evaluator testing.

7.2.1 Test Environment

All evaluator testing was conducted in the developer's test environment, providing a suitable test network with machines to access services on the inside and outside interfaces of the TOE, and to connect to the TOE for remote administration tasks.
A BSD or Windows XP based PC was used either in the internal or external network (relative to the TOE) as external testing system. Standard services (SMTP relay, SSH host, DNS server and FTP server) were provided in the test environment as was a gateway to the Internet.
The TOE itself was installed on the Färist 40100c4HD hardware, which is a standard PC with a 32 bit Intel architecture CPU, 256 MB of main memory, 40GB hard disk and 4 standard 10/100 MBit Ethernet ports.

7.2.2 Test Configuration

The evaluators, assisted by the developer, performed a clean install of the TOE software version 2.5.1 from a USB stick obtained from the developer on the machine and configured the machine according to the specifications in the developer's test plan.
The TOE version used for testing was 2.5.1, which at the time of testing was the current version. Since the final TOE version for this evaluation is 2.5.2, the evaluators conducted a detailed analysis of the changes introduced between these versions and documented it in their report. They found their tests to be still valid, as none of the changes affected the security functions tested by the evaluators.

7.2.3 Testing approach

The evaluators have performed all their tests by stimulating external interfaces of the TOE. This is considered to be sufficient due to the information flow between the TOE subsystems – it is always clearly defined to which subsystem information given to an external interface will be transferred via the internal interfaces.
The overall approach was similar to the one the developer used: valid and invalid input was sent to the external interfaces, the output was observed at the interfaces and in the log file.

7.2.4 Subset size and selection criteria for test repetition

The evaluators used the CEM guidance to choose a sample from the set of developer tests that would explicitly exercise all security functions and three of the four proxies, focusing on functionality that had been changed (esp. the DNS proxy) in this release. Management and audit functionality was sufficiently exercised by the setup of the tests, which were all manually performed.
The evaluators chose a total of 11 tests from the 33 tests in the developer's test plan. Three of these tests were performed in the serial tunnel (VPN) setting of the Färist. All tests ran successfully, delivering the expected results as specified in the developer test documentation.

7.2.5 Additional evaluator tests

Since the examination of the developer tests had proven a good test coverage and depth for all security functions, interfaces and components, there was no compelling reason to supplement the developer testing in a specific area. The evaluators devised a set of additional tests according to the criteria outline in CEM:

- to supplement the developer testing in places, where the evaluator sees the demand for additional tests,
- to cover a broad range of security functions provided by the TOE,
- to cover public domain weaknesses concerning firewalls,
- and to stay in the projected schedule for the evaluator testing activities.

A total of seven additional tests was developed by the evaluators. They were executed in the developer's test environment as described above.
All tests ran successfully, delivering the expected results as specified in the evaluators' test documentation.

7.2.6 Verdict for the activity

All evaluator testing could be performed as intended. The expected results were met in each case and were able to support the persuasion of the evaluators that the overall developer and evaluator testing activities are sound and sufficient to support the EAL 4 evaluation of the TOE.

7.3 Evaluator penetration testing

The evaluators performed penetration testing.

7.3.1 TOE test configuration

The TOE was set up with a basic network configuration (internal and external interfaces, routing, external services available (e.g. DNS server)), with all proxies belonging to the evaluated configuration (i.e. FTP, DNS, SMTP and TCP plug proxy) enabled, whereby a plug proxy was configured to serve port 22, and with the remote administration tool accessible from the external and internal network. The set up included the activation of all features being part of the evaluated configuration, as described in the Administrator's Manual, section 4.3, Because of the nature of the tests, no Färist VPN system was used (i.e. FÄRIST 2.5.2-R-RELEASE), since the tests would not have been able to test that system.
On a Linux-based remote test PC, the network security scanner “Nessus” for Linux was set up and configured to probe the TOE for public domain vulnerabilities and exploits by stimulating the external network interface of the TOE.

7.3.2 Security functions tested

The penetration test was aimed predominantly at the security functions of the TOE processing the user information, i.e. the IP packets mediated through the TOE and their upper protocol specific treatment (e.g. FTP), which are:

- SF.IPS (IP stack)
- SF.PF (packet filter), and
- SF.AP (application proxies)
  - FTP
  - SMTP
  - DNS

7.3.3 Obvious vulnerabilities tested

The evaluators did not identify any obvious vulnerabilities worth testing. Instead, they

took the approach of an attacker trying to footprint the system and scan for any unusual behavior possibly leading to an unknown vulnerability and hence an exploit. However, they were not able to identify such behavior, since the TOE withstood all attempts to confuse it or to reveal any useful information to an attacker.

7.3.4 Results

No vulnerabilities were detected during penetration testing.

The TOE version used for testing was 2.5.1, which at the time of testing was the current version. Since the final TOE version for this evaluation is 2.5.2, the evaluators conducted a detailed analysis of the changes introduced between these versions and documented it in their report. They found their tests to be still valid, as none of the changes affected the security functions tested by the evaluators.
The developer vulnerability analysis and the results of the evaluator penetration testing show that no exploitable vulnerabilities were found.
After careful analysis, the evaluators also determined that one residual vulnerability initially reported by the developer and rated as theoretically exploitable is not exploitable in any real-world scenario.

No exploitable vulnerabilities were discovered.

8 Evaluated Configuration

The evaluated configuration is part of the Färist Firewall and VPN product. Two variants have been covered by the evaluation, the firewall version (Färist 2.5.2-RELEASE) and the VPN version (Färist 2.5.2-R-RELEASE). The only difference is that the VPN version will not work in firewall only mode.

The Färist product is delivered on a CD, which also includes the Administrator's Manual.

9 Results of the Evaluation

The evaluators applied each CEM work unit. For all temporary fail or inconclusive verdicts, the developer supplied updated or complementary evidence.

The certifier reviewed the work of the evaluators, and verified that sufficient evidence and justification was provided by the evaluators to confirm that the evaluation was conducted in accordance with the requirements of the CEM.

The evaluators'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*
Security Target	ASE	*PASS*
- TOE description	ASE_DES.1	*PASS*
- Security environment	ASE_ENV.1	*PASS*
- ST introduction	ASE_INT.1	*PASS*
- Security objectives	ASE_OBJ.1	*PASS*
- PP claims	ASE_PPC.1	*PASS*
- IT security requirements	ASE_REQ.1	*PASS*
- Explicitly stated IT security requirements	ASE_SRE.1	*PASS*
- TOE summary specification	ASE_TSS.1	*PASS*
Configuration management	ACM	*PASS*
- CM automation	ACM_AUT.1	*PASS*
- CM capabilities	ACM_CAP.4	*PASS*
- CM scope	ACM_SCP.2	*PASS*
Delivery and operation	ADO	*PASS*
- Delivery	ADO_DEL.2	*PASS*
- Installation, generation and start-up	ADO_IGS.1	*PASS*
Development	ADV	*PASS*
- Functional specification	ADV_FSP.2	*PASS*
- High-level design	ADV_HLD.2	*PASS*
- Implementation representation	ADV_IMP.1	*PASS*
- Low-level design	ADV_LLD.1	*PASS*
- Representation correspondence	ADV_RCR.1	*PASS*
- Security policy modeling	ADV_SPM.1	*PASS*
Guidance documents	AGD	*PASS*
- Administrator guidance	AGD_ADM.1	*PASS*
- User guidance	AGD_USR.1	*PASS*
Life cycle support	ALC	*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*

Assurance Class Name / Assurance Family Name	*Short name (including component identifier for assurance families)*	*Verdict*
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*
- Misuse	AVA_MSU.2	*PASS*
- Strength of TOE security functions	AVA_SOF.1	*PASS*
- Vulnerability analysis	AVA_VLA.2	*PASS*

Summarising the results of all assurance classes, the final evaluation result is PASS.

The evaluator's conclusion is that the evaluation of Färist 2.5.2-RELEASE and Färist 2.5.2-R-RELEASE fulfils the requirements of EAL4 and ALC_FLR.1 and that the minimum strength of function for the integrity check of NTP packets is SOF-high. During the assessment of the evaluators' work, the certifier found that the evaluators' conclusions were justified.

One observation report was written by the certifier during the evaluation, requesting the developer to provide clarification to the description of the threats against TOE. The security target was updated, and the threat descriptions clarified by the developer.

10 Evaluator Comments and Recommendations

The evaluators have not reported any particular considerations regarding the use of Färist 2.5.2-RELEASE or Färist 2.5.2-R-RELEASE.

11 Glossary

Glossary

(the) Scheme	The Swedish Common Criteria Evaluation and Certification Scheme.
CCRA	International arrangement to promote mutual recognition of Common Criteria certificates.
Certification	The formal approval of a product or protection profile based on the result of the evaluation.
Certification ID	Unique identifier issued by the Certification Body to clearly identify a certification.
Certification report	Report issued by the certifier at the end of each certification showing the outcome of the certification. Certification reports will be issued for all completed certifications, successful or not. The certification report is based on the final evaluation report.
Conditional license	Stage before the Evaluation Facility is granted a full license, permitting the evaluation facility to perform a trial evaluation.
Evaluation	The assessment of an IT product or protection profile against the Common Criteria using the Common Methodology to determine whether or not the security claims on the product or protection profile are justified.
Evaluation and certification scheme	The systematic organisation of the functions of evaluation and certification under the authority of a Certification Body in order to ensure that high standards of competence and impartiality are maintained and that consistency is achieved.
Evaluation evidence	All documentation and provided information submitted by the Developer and/or Sponsor during evaluation and certification.
Evaluation facility	A non-licensed organisation that carries out independent IT product or protection profile evaluations, usually on a commercial basis. *See also* IT security evaluation facility.
Evaluation report	*See* Evaluation technical report.
Evaluation technical report	A report produced by the Evaluation Facility. Either addresses specific assurance aspects, as in the single evaluation reports, or is the final evaluation report. The final evaluation report summarises the single evaluation reports for all assessment aspects required in the Common Criteria.
Final evaluation report	Final report produced by an Evaluation Facility regarding the procedures performed and the results of evaluation of a target of evaluation. The final evaluation report summarises the single evaluation reports for all the assessment aspects required in the Common Criteria.
Full ITSEF license	After all licensing requirements are fulfilled, an Evaluation Facility is granted a full license and becomes an ITSEF.
IT security evaluation facility	An organisation licensed by the Certification Body to carry out independent IT product or protection profile

Glossary

	evaluations, usually on a commercial basis.
Licensing	Licensing of an Evaluation Facility by the Certification Body constitutes confirmation that that Evaluation Facility is qualified to perform evaluations.
Product	A package of IT software, firmware, and/or hardware providing functionality designed for use or incorporation within a multiplicity of systems.
Security target	A set of security requirements and specifications to be used as the basis for evaluation of an identified target of evaluation.
Single evaluation report	Report produced by an Evaluation Facility covering individual assurance aspects specified in the Common Criteria.
Site visit	There are several different site visits within the Scheme: auditing of the development environment of the Developer, auditing of the evaluation tests at the ITSEF, and auditing of the ITSEF during licensing. During a site visit, checks are performed as to whether the documented configuration control processes, policies, and security procedures are being applied. In addition, during a site visit to a development environment, the skills of Developers and other staff in performing tasks are assessed.
Sponsor	The organisation that applies and pays for a certification from the Certification Body.
Target of evaluation	An IT product and its associated administrator and user guidance documentation that is the subject of an evaluation.
Trial evaluation	An evaluation conducted as part of the Evaluation Facility licensing process to demonstrate technical competence and the ability of the Evaluation Facility to work in compliance with the Scheme.

Abbreviation	Description
CB	Certification Body
CC	Common Criteria (CC Part 1-3 refers to the Common Criteria standard documentation)
CCMB	Common Criteria Maintenance Board
CCRA	Common Criteria Recognition Arrangement
CEM	Common Methodology for Information Technology Security Evaluation (CEM Part 1-2 refers to the CEM standard documentation)
CM	configuration management
CR	certification report
EAL	evaluation assurance level
FER	final evaluation report
FMV	Försvarets Materielverk - The Swedish Defence Material Administration
IEC	International Electrotechnical Commission
ISO	International Organisation for Standardisation
IT	information technology
ITSEF	IT Security Evaluation Facility

Abbreviation	Description
OR	observation report
SER	single evaluation report
ST	security target
TOE	target of evaluation
TOR	technical oversight report

12 Bibliography

ST	Security Target Färist, Release 2.5.2, Tutus Data AB, 2007-09-20, document version 2.1
ADM	Färist Administrator's Manual, Release 2.5.1, Tutus Data AB, 2007-08-22, document version 2.9.3
SKUT	Simple key-exchange using TLS (SKUT), P. Holmer and R.Lind, March 2004
CC	Common Criteria for Information Technology Security Evaluation, version 2.3, August 2005, Part 1-3
CEM	Common Methodology for Information Technology Security Evaluation, version 2.3, August 2005
SP-002	Evaluation and Certification, FMV/CSEC 25550:558/2005, 2007-07-28, document version 8.0
SN5	Scheme Note 5, FMV/CSEC 25550:64 543/2006, 2007-05-25
SN8	Scheme Note 8, FMV/CSEC 25550:29 747, 2007-06-25