Swedish Certification Body for IT Security

Certification Report Tutus Färist IEG

Issue: 1.0, 2026-feb-17

Authorisation: Jerry Johansson, Lead certifier , CSEC

Table of Contents

1 Executive Summary

The TOE is the firmware of Tutus Färist IEG, a network device with extendable filtering capacities and VPN. In the evaluated configuration the TOE runs on one of the two hardware appliances H220 and M110 and is delivered with two filter modules: the NTP-filer and the UDP-diode. There are also two built-in filter modules: Allow and Deny. The certified firmware version is 4.5.0.

The ST does not claim conformance to any Protection Profiles (PPs).

There are nine assumptions made in the ST regarding the secure usage and environment of the Tutus Färist IEG. The TOE relies on these being met to counter seven threat and five organisational security policies (OSPs) in the ST. The assumptions, the OSPs and the threats are described in chapter 4 Assumptions and Clarifications of Scope.

The evaluation has been performed by atsec information security AB in their premises in Stockholm, Sweden. Site-visit, testing oversight and testing was performed by the evaluator at the developer's site in Stockholm.

The evaluation was completed in 2026-02-09. The evaluation was conducted in accordance with the requirements of Common Criteria (CC), version 2022 and the Common Methodology (CEM) version 2022. The evaluation was performed at the evaluation assurance level EAL 4, augmented by ALC_FLR.1.

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 are also accredited by the Swedish accreditation body SWEDAC according to ISO/IEC 17025 for Common Criteria.

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 achieved in agreement with the requirements of the Common Criteria and the Common Methodology for evaluation assurance level EAL 4 augmented by ALC_FLR.1.

The technical information in this report is based on the Security Target [ST] and the Final Evaluation Report produced by atsec information security AB.

2 Identification

Certification Identification	
Certification ID	CSEC2024030
Name and version of the certified IT product	Tutus Färist IEG v.4.5.0
HW platform	H220 and M110
Security Target Identification	Färist IEG - Security Target
EAL	EAL 4 + ALC_FLR.1
Sponsor	Tutus Data AB
Developer	Tutus Data AB
ITSEF	atsec information security AB
Common Criteria version	CC:2022
CEM version	CEM:2022
QMS version	2.6.1
Scheme Notes Release	22.0
Recognition Scope	CCRA, SOGIS, EA/MLA
Certification date	2026–02–17

3 Security Policy

The TOE provides the following security services:

- Filter
- VPN
- Audit
- Management
- Autoupdate
- Selftest and failsafe

3.1 Filter

The filter functionality makes it possible to enforce basically any communication policy between two or more networks. Filter modules are programs that are loaded to the device and are configured using the configuration file.

The base system will direct traffic based on IP and TCP/UDP information to the filter program that performs the filtering.

Filters for NTP and a UDP-diode are included in the evaluation.

The NTP filter allows time synchronization using the NTP protocol while limiting the information leakage.

The UDP diode forwards UDP packets in one direction and drops any response packets in the other.

3.2 VPN

The VPN functionality uses encryption for the authentication and integrity of remote networks. This prevents network intrusions from untrusted networks.

Key exchange and authentication is done with the SKUT protocol [SKUT5] using an RSA-signed Diffie-Hellman key exchange combined with the FrodoKEM (eFrodoKEM-1344-SHAKE) key encapsulation to make it quantum-resistant. Encryption is done using IPSec ESP [RFC4303] in tunnel mode with the AES-256-GCM encryption algorithm.

VPN tunnels are configured using the configuration file and the TLS certificate stored in a file on USB memory or on a smart card.

3.3 Audit

Audit records that are created in different components are sent to a log daemon (tlogd), that 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.

The last few log events are also stored in a local copy of the audit file, which is kept in RAM. This is used for troubleshooting and is not considered a TSF.

3.4 Management

The TOE can have the following administrative roles:

- Administrator
  - Remote administratorThe remote administrator can perform all administrative tasks, including changing keys.The remote administrator is authenticated through their certificate.

◦ Local administratorThe local administrator can perform the same tasks as the remote administrator. In addition, the local administrator can change the smart card.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 their certificate.

Remote management is secured through certificates. The remote user is identified through the CN (common name), UID (Unique Identifier) or Email (RFC822 email) field in their certificate.

Local management is secured through organizational means and is therefore not considered a TSF.

3.5 Autoupdate

The TOE has an automatic update functionality that checks for new firmware updates, verifies the origin and integrity of the update and ensures that the update is newer than the current version. Note that it is the update function that is part of the TOE and not the updated version of the TOE.

3.6 Self-test and failsafe

The TOE has built-in functionality for 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 restart.

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

4 Assumptions and Clarification of Scope

4.1 Assumptions

The Security Target [ST] makes nine assumptions on the usage and the operational environment of the TOE.

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 the 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.NOEVIL

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

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.

A.SINGEN

Information cannot flow among the networks (local-local, remote-remote, and local-remote) unless it passes through the TOE.

4.2 Clarification of Scope

The Security Target contains seven threats, which has been considered during the evaluation.

T.CHANNEL

An attacker may impersonate a remote network by forging authentication data within the IPSec VPN tunnel.

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 may send information through the TOE bypassing the filter or access control system.

T.MODIFY

The attempts of an external attacker to modify data transmitted between the TOE and a remote 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.

The Security Target contains five Organisational Security Policies (OSPs).

P.ADMACC

Administrators shall be accountable for the actions they conduct by generating sufficient audit records for the actions.

P.AUDIT

The TOE shall be able to record all of its security relevant actions.

P.CONFIG

The TOE shall support the means to configure and manage the TSFs.

P.NTPSYNC

The TOE shall allow time synchronization information to flow as specified by its filtering policies, while limiting information leakage.

P.UDPDIODE

The TOE shall allow UDP traffic to flow only in one direction as specified by its filtering policies.

5 Architectural Information

The TOE consists of two subsystems, the control plane and the data plane. The controlplane runs on top of a Linux kernel while the data plane operates directly on top of the hardware. All packets are received and validated by the data plane. The dataplane routes packets according to a rule table. Packets directed to the TOE itself or a via a filter are sent to the control plane. Packets to or from a VPN tunnel are sent to the crypto engine. Packets that do not match any rule are dropped.

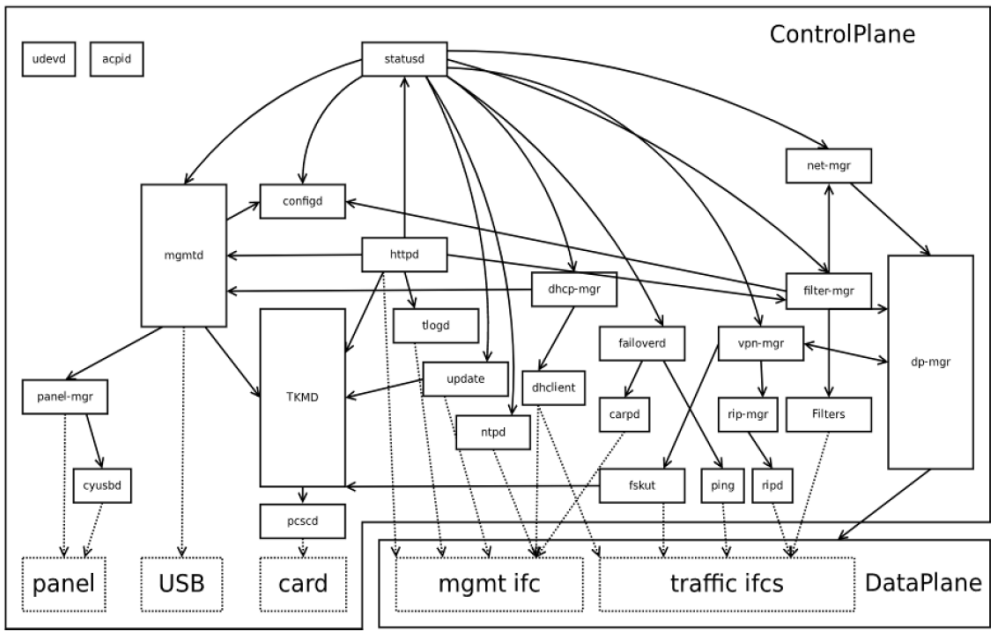

Figure 1: Färist IEG Architecture

The control plane handles all administrative roles in the TOE, including key negotiations. It consists of a number of components which run on top of a standard Linux kernel. The data plane is running directly on the hardware and is responsible for all packet processing.

6 Documentation

The TOE includes the following guidance documentation:

RefMan	Administrator's Reference Manual Färist IEG 4.5.0

7 IT Product Testing

7.1 Developer Testing

Testing Approach

The developer's testing approach is highly automated, and also complemented by manual testing. A custom testing framework is used to conduct automated testing, which covers most of the TOE tests. The framework enables different network scenarios and simulated behavior for repeatable testing. The automated testing is part of the development process, enabling regular testing runs throughout development to identify issues at an early stage The framework contains both positive and negative tests.

The developer testing is extensive, with coverage beyond the scope of the TOE, in that also non-TOE configurations and models are tested. In total more than a thousand tests are performed.

Test Configuration

Testing is executed against the actual TOE platform and version as defined in the Security Target. For each test, the framework prepares the necessary configuration both for the TOE and the test environment. This includes supporting services and network layout.

Test Results

The developer has provided the test results of all test cases that were performed, together with complete test logs and verdicts from the test execution. The evaluator examined these to verify the results. All tests were successful.

7.2 Evaluator Testing

Testing Approach

The developer testing is extensive. While certain complex functionality is intended to be verified via code review, there are no other clear gaps or areas which needed further testing. The evaluator based the testing effort on the results of the ATE_COV and ATE_DPT work units. Here, the evaluator determined that the developer testing had covered all TSFIs, Subsystems and TSF of the TOE . The evaluator has performed the following testing of the TOE:

- Re-executed a sample of the developer tests - A large sample of tests was performed, covering every TSFI and focusing also on the cryptographic functionality.
- Performed modifications in the automated tests to verify the test framework - As the testing is performed with the automated framework, the evaluator performed tests to verify its correct operation by making sure it would detect unexpected TOE behavior.
- While not documented as an evaluator test, reviewed the source code for functionality that was not trivial to verify using practical testing.

Test Configuration

The evaluator used the same environment as for the developer testing. As access to the

custom test framework was needed, it was beneficial to use the developer's environment. This was hosted at the developer's premises in Stockholm, Sweden. Before running the tests, the evaluator verified the setup of the TOE and the test configuration to ensure that it matched the [ST]. The evaluator was able to confirm that the configuration was appropriate and that all necessary non-TOE components were provided by the test environment.

Test Results

All evaluator test cases and sample developer tests were completed successfully.

7.3 Penetration Testing

Testing approach

No potential vulnerabilities were identified during the vulnerability analysis. As such, also considering the extent of the developer testing as examined by the evaluator in SER ATE, and the presence of negative tests under the ATE testing, no additional penetration tests were devised by the evaluator.

Testing depth

Since the developer performs both positive and negative testing at a detailed level, it was unlikely that vulnerabilities caused by programming errors or bugs would be found and identified by the developer. No "penetration tests" were devised.

Testing results

No vulnerabilities were detected in the TOE.

8 Evaluated Configuration

The TOE shall be installed and configured in accordance with the TOE guidance documentation: Administrator's Reference Manual Färist IEG 4.5.0.
In the evaluated configuration, the TOE runs on one of the following hardware Appliances provided by Tutus Data AB: H220 or M110.
In the evaluated configuration the

- A remote log server must be configured with the Level option set to Info.
- Remote administration must require TLS 1.3 by setting the AllowLegacyTLS option to false in the System Administration section.
- The Symmetrical VPN and Multicast functions (SymVPN and Multicast in the configuration) may not be used.
- VPN when used must require post-quantum ready encryption by setting the PQ option to Mandatory.
- Only the UDP-diode and NTP-filter filter modules may be used; no other filters may be configured in the Filter section of the configuration.

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 evaluators 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:

Assurance Class/Family	*Short name*	*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

None.

11 Acronyms

CC	Common Criteria for Information Technology Security
CEM	Common Methodology for Information Technology Security, document describing the methodology used in Common Criteria evaluations
CLI	Command Line Interface
EAL	Evaluation Assurance Level
IEG	Information Exchange Gateway
ITSEF	IT Security Evaluation Facility, test laboratory licensed to operate within a evaluation and certification scheme
OSP	Organisational Security Policy
SFP	Security Function Policy
SFR	Security Functional Requirement
ST	Security Target, document containing security requirements and specifications, used as the basis of a TOE evaluation
TOE	Target of Evaluation
TSF	TOE Security Functionality
VPN	Virtual Private Network

12 Bibliography

ST — Färist IEG - Security Target, Tutus Data AB, 2026-02-12, document version 1.0, FMV_ID 24FMV6702-36

RefMan — Administrator's Reference Manual Färist IEG 4.5.0, Tutus Data AB, 2025-11-03, document version 5.1, FMV_ID 24FMV6702-19

CC/CEM — Common Criteria for Information Technology Security Evaluation, and Common Methodology for Information Technology Security Evaluation, CCMB-2022-11-001 through 006, document versions CC:2022/CEM:2022 rev 1

Appendix A Scheme Versions

A.1 Scheme/Quality Management System

During the certification the following versions of the Swedish Common Criteria Evaluation and Certification scheme have been applicable since the certification application was registered 2024-11-04:

Version	Introduced	Impact of changes
2.6.1	2025-10-16	No impact
2.6	2025-04-23	No impact
2.5.2	2024-06-14	Application

A.2 Scheme Notes

Scheme Notes applicable to the certification:

Scheme Note	Version	Title	Applicability
SN-15	5.0	Testing	Compliant
SN-18	4.0	Highlighted Requirements on the Security Target	Compliant
SN-22	4.0	Vulnerability Assessment	Compliant
SN-27	1.0	ST Requirements at the Time of Application for Certification	Compliant
SN-28	2.0	Updated Procedures for Application, Evaluation and Certification	Compliant