Swedish Certification Body for IT Security

Certification Report MontaVista VPN Client v2.0

Issue: 1.0, 2026-jan-22

Authorisation: Jerry Johansson, Lead certifier , CSEC

Table of Contents

1 Executive Summary

The TOE is part of the MontaVista VPN Client (MVC), which is a software product.

The MVC is intended to be used with the MontaVista Linux Carrier Grade eXpress (CGX) operating system using the ARM processor architecture.

The MVC is employed by an end-user as a client on an operating environment to establish a mutually-authenticated trusted channel with a server on a remote system running a compatible implementation of the standard protocols implemented by TOE.

The MVC consists of a collection of software modules that include components from the opensource software project strongSwan and Linux kernel networking components. The TOE is provided as binary executables along with the whole MVC source code, including all of the non-TOE components and tools necessary to build the executable images. However, only the binary executables are considered the TOE and not the source code version.

The MVC utilizes features of the non-TOE hardware/firmware/software platform provided by its environment, including cryptographic operations, key management and key storage.

The TOE type is a VPN Client.

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

There are ten assumptions made in the ST regarding the secure usage and environment of the MontaVista VPN Client. The TOE relies on these being met to counter one threat and three 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 and testing oversight was performed by the evaluator at the developer's site in San Jose, two certifiers participated virtually via Teams.

The evaluation was completed in 2025-12-02. 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.2 and AVA_VAN.4.

atsec information security AB is a licensed evaluation facility for Common Criteria under the Swedish Common Criteria Evaluation and Certification Scheme. Combitech 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.2 and AVA_VAN.4.

The technical information in this report is based on the Security Target [ST] and 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	CSEC2024016
Name and version of the certified IT product	MontaVista VPN Client v.2.0 buildtag: agib-6.6-5.0-250613145912
Security Target Identification	MontaVista VPN Client (MVC) Common Criteria Security Target
EAL	EAL 4 + ALC_FLR.2 + AVA_VAN.4
Sponsor	MontaVista Software, LLC
Developer	MontaVista Software, LLC
ITSEF	atsec 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	2026–01–22

3 Security Policy

The TOE provides the following security services:

- Cryptographic protocols
- Cryptographic key negotiation and handling
- Establish mutually authenticated trusted channel
- Confidentiality and Integrity of red data-in-transit
- Generation of audit records
- Self-test of the cryptographic functions

3.1 Cryptographic protocols

Cryptographic protocols capable of successful runs despite passive eavesdropping or active manipulations of coordination and data communication messages in transit by an adversary with powers such as those defined by the Dolev-Yao symbolic model.

The MVC implements ESP protocol to provide confidentiality, data origin authentication, connectionless integrity, and anti-replay service to connections between local and remote red networks for both ipv4 and ipv6. The MVC performs encrypting and signing, to mitigate against eavesdropping and manipulation of messages while in transit over the black network.

3.2 Cryptographic key negotiation and handling

IKEv2 protocol is implemented by the MVC for IPsec keying functionality. At phase 1 the MVC performs mutual authentication of the peers using X.509 certificates, negotiates cryptographic parameters, and creates session keys for the rest of IKEv2 communication (Phase 2).

3.3 Establish mutually authenticated trusted channel

Establish a mutually authenticated trusted channel “VPN tunnel” over a public “black” network.

IPsec ESP functionality of the MVC implements IPsec tunnel mode, which encapsulates the whole IP packet by encrypting and authenticating the original IP packet. Encryption and authentication is performed by utilizing keys and algorithm selections from an Security Association (SA) entry in SA Database. The SA entry is created for the connection by IKEv2 functionality in Phase 2 negotiation

3.4 Confidentiality and Integrity of red data-in-transit

Confidentiality and integrity of red data-in-transit through VPN tunnel.

The red data in-transit is protected by encapsulating it into IPsec VPN ESP tunnel, negotiated between local and remote peer as described above. For network packets, IPsec Security Policy Database is searched to determine whether a packet is subject to IPsec transformation.

3.5 Generation of audit records

StrongSwan generates audit records of IPsec IKEv2 security-relevant events via the systemd logging interface provided by the platform. The log entries are stored into a file and accessible locally to the security administrator.

3.6 Self-test of the cryptographic functions

During start-up, the TOE will perform test of the strongSwan and test of the cryptographic functions that are provided by the platform (both the kernel and the user space part). The TOE will also test the integrity of the strongSwan configuration. If these tests are failing the TOE will not be operational and will enter a secure state. In that case the TOE will generate an audit event.

4 Assumptions and Clarification of Scope

4.1 Assumptions

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

A.PHYSICAL_SECURITY

The non-IT environment provides the TOE and the platform upon which it operates with appropriate physical security to prevent tampering commensurate with the value of the IT assets protected by the TOE..

A.PERSONNEL

Personnel that use or administer the TOE or the platform are assumed to be trusted, trained and follow all applicable guidance documentation.

A.IT_ADMIN

The operational environment of the TOE provides procedures and tools for the secure configuration and administration of the TOE.

A.IT_STORAGE

The IT environment provides protected persistent storage for programs and data of the TOE.

A.IT_ACCESS_CONTROL

The IT environment for the operation of the TOE provides appropriate and adequate access control for assets upon which the TOE depends, including: TOE executable files, configuration files, ports, or other interfaces.

A.IT_CRYPTO_EXP

The cryptographic primitives, RNG and memory management for kernel key erasure required by the TOE are provided by the underlying platform.

A.IT_CRYPTO_GEN

The IT environment provides mechanisms for the storage, distribution and management of cryptographic private keys and certificates.

A.IT_INITIALIZATION

The IT environment has hardware and software features to ensure correct establishment of initial secure state.

A.IT_TIME

The IT environment has hardware and software features to provide the current time.

A.IT_MEDIATION

All access to data assets (including red data and external network connections) that exist in the IT environment is mediated by and subject to the controls provided by the platform upon which the TOE executes.

4.2 Clarification of Scope

The Security Target contains one threat, which has been considered during the evaluation.

T.NETWORK_ATTACK

The actions of an adversary on the black network (including message inspection, disassembly, replay, deletion, modification, and creation potentially across multiple sessions) enable the adversary to defeat the objectives of the security protocols implemented by the TOE resulting in violation of a security policy, such as the confidentiality or integrity of red DIT.

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

P.LOGGING

Information regarding the occurrence of security-relevant events within the TSF shall be logged for later forensic examination, including the identity of associated individual user or subject, along with other relevant particulars.

P.RED_DATA_PROT

The TOE shall ensure that red data is protected when it is under control of the TOE and that it is only transmitted over the designated communication channel to or from a peer over a black network.

P.SELF_TEST

The TOE must verify the integrity of the configuration and verify that the cryptographic operations are performed correctly before any outside connection is established. If the test fails the TOE must come to a halt.

5 Architectural Information

The MVC is used to establish a cryptographically secure data communication channel between a local user and a remote trusted user or to establish a trusted network over a potentially unsafe network.

The client is physically realized in the MVC as a software product. The core functionality is to transmit red data with confidentiality, integrity and authenticity achieved by establishing a suitably configured VPN tunnel between the VPN client and a compatible VPN gateway. Supporting functions needed to protect the VPN client and to configure and establish the secure channel, perform encryption/decryption and signing of data, key and certificate management, key storage, etc. are provided by the platform running the MVC product. The MVC utilizes features of the non-TOE hardware/firmware/software platform provided by its environment, including cryptographic operations, key management and key storage.

MVC implements security functionality that integrates with the CGX kernel to provide IPSec ESP packet path functionality, maintaining Security Association & Security Policy databases (SAD and SPD) and enforcing IPsec ESP protocol transformation of network packets. In CGX user space, MVC implements security functionality for managing IPsec configuration, running IPsec IKEv2 keying protocol and controlling ESP transformation in the kernel by applying SA and SP information.

During start-up, the TOE will perform test of the strongSwan and test of the cryptographic functions that are provided by the platform (both the kernel and the user space part). The TOE will also test the integrity of the strongSwan configuration. If these tests are failing the TOE will not be operational and will enter a secure state. In that case the TOE will generate an audit event.

StrongSwan generates audit records of IPsec IKEv2 security-relevant events via the systemd logging interface provided by the platform. The log entries are stored into a file and accessible locally to the security administrator.

6 Documentation

The TOE includes the following guidance documentation:

RFG	Reference Guide MVC 2.0 VPN
CGX	MVSecure CGX 5.0 Getting Started Guide MVC 2.0 AGIB

7 IT Product Testing

7.1 Developer Testing

Testing Approach

The developer has performed testing against all TSFIs and subsystems of the TOE. The testing covers the cryptographic protocols and algorithms claimed in the [ST]. In total, it consists of 31 test cases. This testing is performed as a part of the development process, and to an extent the test execution and reporting of results is automated. However, the tests may also be executed manually with relative ease.

For each test case, the developer provided an overall test objective, test steps, and the expected results in the developer's test plan. The tests include both positive and negative test cases.

Test Configuration

The testing was performed using the same platform as specified in the [ST]. As most tests are simply executed on said trusted platform (part of the TOE operational environment), the testing can be completed without proprietary tools. The developer's testing has been completed between two identical TOE's, but the tests may also be executed with other compatible systems used as end-points for the VPN.

Test Results

The developer provided the test output and results separately from the test plan. The developer provided both a verdict of the test case and also the complete test output. The evaluator examined these to verify the results. All tests were successful.

7.2 Evaluator Testing

Testing Effort

The evaluator first executed a sample of the developer's testing for each TSFI via the following test cases:

- TPS-CGX26-RFC_3602_ESP
- TPS-CGX26-RFC_4945_IKEv2
- TPS-CGX26-Strongswan_strongswanconf
- TPS-CGX26-Strongswan_Host_Host
- TPS-CGX26-Strongswan_Systemd_verification
- TPS-CGX26-Strongswan_systemdlogging
- TPS-CGX26-Crypto_Tests_Interface
- TPS-CGX26-Update_SA
- TPS-CGX26-IPv6

The evaluator did not identify any gaps in the coverage of the developer's testing to TSF, Subsystems, or TSFIs. The evaluator added a test case to verify the cryptographic functionality by using a trusted reference implementation:

- ETC#1: Independent (Cryptographic) Implementation

Testing Approach

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 repeated a sample of the developer's testing, covering one test for each TSFI.

The evaluator found room for improvement the area of one cryptographic test, but opted to verify the expected behaviour of the functionality via analysis of the implementation representation, and therefore did not add any further test case related to this. The evaluator identified that the developer did not test against a fully independent cryptographic implementation. The evaluator set up a test to verify the cryptographic functionality against a Libreswan reference implementation.

Test Configuration

The evaluator had prepared and installed the testing environment, including the TOE(s) at atsec's premises in Stockholm, Sweden. The developer provided the hardware and software platform as specified in the [ST], and also the TOE. The developer also provided information about additional test systems, such as remote VPN endpoints, which assisted the evaluator in setting up an equivalent testing 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. Penetration testing was conducted against exposed areas within the TOE, as identified during the search of vulnerabilities through the developer's evidence. As such, the evaluator created a negative test against the TOE's trusted channel as a penetration test.

Testing configuration

The TOE and the TOE environment were configured according to the [ST], [RFG] and [CGX] guidance documents.

Testing depth

Since the developers performs both positive and negative testing, it was unlikely that vulnerabilities caused by programming errors or bugs would be found and identified by the evaluator. As such, the evaluator attempted to expand the scope of the testing from the perspective of an attacker by verifying the claimed integrity and confidentiality functionality.

Testing results

None of the performed penetration tests revealed any vulnerability in the TOE.

8 Evaluated Configuration

The TOE components below shall be installed and configured in accordance with the TOE guidance listed in this document.

The MVC is intended to be used with the MontaVista Linux Carrier Grade eXpress (CGX) operating system using the ARM processor architecture. So the CGX operating system must be provided as part of the operational environment.

The following platform software components are required for operation of the TOE:

- identification and authentication components
- Linux Kernel Crypto API which provides cryptographic algorithm implementations for the kernel space ESP implementation
- OpenSSL library and PKCS#11 module (SoftHSM by default) which provide cryptographic algorithm implementations for the user space charon-systemd IKEv2 implementation
- Netlink Socket API for maintaining Security Policy Database (SPD) / Security Association Database (SAD) in the kernel space and for communicating from the kernel space IPsec stack to the charon-systemd daemon
- systemd daemon that starts charon-systemd and collects and stores log information
- configuration agent (using libest) that provides user interface for configuration and interfaces to other parts of the user's system

Besides, a hardware/firmware platform compatible with the CGX operating system is required, which has at least one network interface and provides persistent storage for software components, configuration and log data. The evaluated platform hardware is an AGIB A101 board, secure SoC environment (ARM ISA).

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
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.2	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.4	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
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 — MontaVista VPN Client (MVC) Common Criteria Security Target, MontaVista Software LLC, 2025-12-01, document version 2.8, FMV_ID 24FMV5978-38

RFG — Reference Guide MVC 2.0 VPN, MontaVista Software LLC, June 2025, document revision 1, FMV_ID 24FMV5978-30

CGX — Getting Started Guide MVC 2.0 AGIB, MontaVista Software LLC, June 2025, document revision 2, FMV_ID 24FMV5978-30

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