Ärendetyp: 6
Diarienummer: 21FMV3267-24:1
Dokument ID CSEC2021002

Swedish Certification Body for IT Security

Certification Report - MontaVista VPN Client (MVC) 1.0

Issue: 1.0, 2022-mar-25

Authorisation: Helén Svensson, Lead certifier , CSEC

Table of Contents

1 Executive Summary

The Target of Evaluation (TOE) is MontaVista VPN Client (MVC) 1.0 with buildID 210823084105. 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 open-source 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 is intended to be used with the MontaVista Linux Carrier Grade eXpress (CGX) operating system using the ARM processor architecture.

The TOE is delivered as binary images along with a minimal supporting software platform embodied in the CGX 2.6 deliverable. The TOE is delivered by download from the MontaVista "Zone" at https://support.mvista.com.

The guidance document is delivered as a PDF file on the MontaVista Zone.

No PP claims are being made.

There are ten assumptions being made in the ST regarding the secure usage and operational environment of the TOE. The TOE relies on these to counter one threat and comply with three organisational security policies (OSPs) in the ST. The assumptions, threats and OSPs are described in chapter 4 Assumptions and Clarification of Scope.

The evaluation has been performed by atsec information security AB in Danderyd, Sweden. The evaluation was completed on 2022-03-17. The evaluation was conducted in accordance with the requirements of Common Criteria (CC), version. 3.1 release 5.

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 also accredited by the Swedish accreditation body 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, and by observing site-visit and testing. The certifier determined that the evaluation results confirm the security claims in the Security Target (ST) 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 (FER) produced by atsec information security AB.

2 Identification

Certification Identification	
Certification ID	CSEC2021002
Name and version of the certified IT product	MontaVista VPN Client, Software Version: MVC 1.0, buildID 210823084105
Security Target Identification	MontaVista VPN Client (MVC) Common Criteria Security Target, MontaVista Software, LLC, 2022-03-15, document version 1.0
EAL	EAL 4 + ALC_FLR.2 and AVA_VAN.4.
Sponsor	MontaVista Software, LLC
Developer	MontaVista Software, LLC
ITSEF	atsec information security AB
Common Criteria version	3.1 release 5
CEM version	3.1 release 5
QMS version	2.1.1
Scheme Notes Release	18.0
Recognition Scope	CCRA, SOGIS, EA/MLA
Certification date	2022-03-25

3 Security Policy

The TOE provides the following security services:

- Security audit
- Cryptographic support
- Protection of the TSF
- Trusted channel

3.1 Security audit

Security audit data is generated by strongSwan. StrongSwan generates audit records of IPsec IKEv2 security-relevant events via the systemd logging interface provided by the platform. Audit data (logs) are written to the system journal and can be accessed with systemd tools. The TSF can also be configured to write logs to a file, or to pass logs to the syslog(3) POSIX function.

3.2 Cryptographic support

The MVC implements IPsec ESP protocol to provide confidentiality, data origin authentication, connectionless integrity, and anti-replay service to connections between local and remote networks for both ipv4 and ipv6. Implementation is based on strongSwan and Linux kernel XFRM functionality. Cryptographic algorithm implementations are part of the platform.

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).

The TOE implements cryptographic key establishment and cryptographic key destruction (for session keys). Key generation is implemented by the platform.

3.3 Protection of the TSF

StrongSwan performs crypto tests on startup. The Linux kernel tests cryptographic primitives used by the XFRM module during the system boot.

The TSF self test comprises two parts: test of TSF components and test of the external entities. The self test part is performed by verifying the integrity of the strongSwan configuration using a SHA-256 checksum, but also trigger the invocation of the tests of the external cryptographic functions. 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.

3.4 Trusted channel

The MVC communicates red data (data that is proprietary, sensitive, or otherwise restricted in its distribution) with other compatible trusted peers over a trusted communication channel. This channel is established using the standard protocols for IPsec and IKEv2. All red data is forced flow only through the trusted channel.

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.

4 Assumptions and Clarification of Scope

4.1 Usage and Environmental Assumptions

The Security Target [ST] makes ten assumptions on the usage and on 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 identifies 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 (Data-In-Transit).

The Security Target contains three Organisational Security Policies (OSPs), which have been considered during the evaluation.

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 main guides of installing the TOE into the evaluated configuration is:

- CGX 2.6 Getting Started Guide [GSG]

7 IT Product Testing

7.1 Developer Testing

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.

The testing was performed using the same platform as specified in the [ST].

All tests were successful.

7.2 Evaluator Testing

The evaluator repeated a sample of the developer's testing, covering one test for each TSFI. The evaluator added a test case to verify the cryptographic functionality by using a trusted reference implementation.

The testing was performed using the same platform as specified in the [ST].

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

7.3 Penetration Testing

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.

The TOE and the TOE environment were configured according to the [ST] and the [GSG] guidance document.

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

8 Evaluated Configuration

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	*Component*	*Verdict*
Development	ADV:	
Security architecture description	ADV_ARC.1	PASS
Complete functional specification	ADV_FSP.4	PASS
Implementation representation of the TSF	ADV_IMP.1	PASS
Basic modular 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
Production support, acceptance procedures and automation	ALC_CMC.4	PASS
Problem tracking CM coverage	ALC_CMS.4	PASS
Delivery procedures	ALC_DEL.1	PASS
Identification of security measures	ALC_DVS.1	PASS
Developer defined life-cycle model	ALC_LCD.1	PASS
Well-defined development tools	ALC_TAT.1	PASS
Flaw reporting procedures	ALC_FLR.2	PASS
Security Target evaluation	ASE:	PASS
Conformance claims	ASE_CCL.1	PASS
Extended components definition	ASE_ECD.1	PASS
ST introduction	ASE_INT.1	PASS
Security objectives	ASE_OBJ.2	PASS
Derived security requirements	ASE_REQ.2	PASS
Security problem definition	ASE_SPD.1	PASS
TOE summary specification	ASE_TSS.1	PASS
Tests	ATE:	PASS
Analysis of coverage	ATE_COV.2	PASS
Testing: basic design	ATE_DPT.1	PASS
Functional testing	ATE_FUN.1	PASS
Independent testing - sample	ATE_IND.2	PASS
Vulnerability assessment	AVA:	PASS
Methodical vulnerability analysis	AVA_VAN.4	PASS

10 Evaluator Comments and Recommendations

None.

11 Glossary

API	Application Programming Interface
ARM	Advanced RISC Machine
CC	Common Criteria for Information Technology Security Evaluation Version 3.1r5
CGL	Carrier Grade Linux (standard working group) CGL 5.0 standard
CGX	MontaVista Linux Carrier Grade eXpress operating system
charon-systemd	IKE daemon for use with systemd
CEM	Common Methodology for Information Technology Security, document describing the methodology used in Common Criteria evaluations
DIT	Data-In-Transit
EAL	Evaluation Assurance Level
ESP	Encapsulating Security Payload
IKE	Internet Key Exchange
IKEv2	Internet Key Exchange version 2
IPsec	Internet Protocol security (protocols)
IPv4	Internet Protocol version 4
IPv6	Internet Protocol version 6
IT	Information Technology
ITSEF	IT Security Evaluation Facility, test laboratory licensed to operate within a evaluation and certification scheme
libest	library offering EST client and server functions
MVC	MontaVista VPN Client
netlink	Linux kernel interface used for communication between kernel and user space processes and between user space processes
PKCS #11	Public-Key Cryptography Standards API to create and manipulate cryptographic tokens
platform	Hardware, firmware, operating system, and utilities that provide the IT environment within which the TOE runs
POSIX	Portable Operating System Interface (standard)
PP	Protection Profile
red data	data that is proprietary, sensitive, or otherwise restricted in its distribution
RFC	Request For Comments (standards)
RISC	Reduced Instruction Set Computer (ISA)
RNG	Random Number Generator (or Generation)
SA	Security Association

SAD	Security Associations Database
SHA	Secure Hash Algorithm
SPD	Security Policy Database
SSL	Secure Sockets Layer
ST	Security Target
strongSwan	a multiplatform IPsec implementation available under GNU GPL
subject	a process operating on behalf of a user
systemd	system and service manager for Linux operating systems
TOE	Target of Evaluation
TSF	TOE Security Functions
user	Person employing the VPN service
Virtual Private Network	a method employing encryption to provide secure access to a remote computer over the Internet (or other unsecure network)
VPN	Virtual Private Network
XFRM	Transform (Transformation)
X.509	Standard defining the format of public key certificates

12 Bibliography

ST	MontaVista VPN Client (MVC) Common Criteria Security Target, MontaVista Software, LLC, 2022-03-15, document version 1.0
GSG	CGX MontaVista Linux Carrier Grade Express 2.6 Getting Started Guide AGIB, MontaVista Software, LLC., 2021-10, document version Rev 6
CCpart1	Common Criteria for Information Technology Security Evaluation, Part 1, version 3.1 revision 5, CCMB-2017-04-001
CCpart2	Common Criteria for Information Technology Security Evaluation, Part 2, version 3.1 revision 5, CCMB-2017-04-002
CCpart3	Common Criteria for Information Technology Security Evaluation, Part 3, version 3.1 revision 5, CCMB-2017-04-003
CC	CCpart1 + CCpart2 + CCpart3
CEM	Common Methodology for Information Technology Security Evaluation, version 3.1 revision 5, CCMB-2017-04-004
SP-002	SP-002 Evaluation and Certification, CSEC, 2021-10-26, document version 34.0
SP-188	SP-188 Scheme Crypto Policy, CSEC, 2021-10-26, document version 12.0

Appendix A Scheme Versions

During the certification project, the following versions of the quality management system (QMS) have been applicable since the certification application was registered.

QMS 1.24.1 valid from 2020-12-03

QMS 1.25 valid from 2021-06-17

QMS 2.0 valid from 2021-11-24

QMS 2.1 valid from 2022-01-26

QMS 2.1.1 valid from 2022-03-09

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 CSEC QMS 2.1.1".

The certifier concluded that, from QMS 1.24.1 to the current QMS 2.1.1, there are no changes with impact on the result of the certification.

A.1 Scheme Notes

- Scheme Note 15 – Testing
- Scheme Note 16 - Additional planning requirements
- Scheme Note 18 - Highlighted Requirements on the Security Target
- Scheme Note 22 - Vulnerability assessment
- Scheme Note 25 - Use of CAVP-tests in CC evaluations
- Scheme Note 27 - ST requirements at the time of application for certification
- Scheme Note 28 - Updated procedures for application, evaluation ad certification
- Scheme Note 31 - New procedures for site visit oversight and testing oversight