National Information Assurance Partnership

Common Criteria Evaluation and Validation Scheme Validation Report

Klas Telecom, Inc.

Klas Voyager

Report Number: CCEVS-VR-VID10767-2017
Dated: September 19, 2017
Version: 1.0

National Institute of Standards and Technology
Information Technology Laboratory
100 Bureau Drive
Gaithersburg, MD 20899

National Security Agency
Information Assurance Directorate
9800 Savage Road STE 6940
Fort George G. Meade, MD 20755-6940

Acknowledgements

Validation Panel

Paul A. Bicknell

MITRE Corporation

Marybeth S. Panock

Kenneth Stutterheim

The Aerospace Corporation

Common Criteria Testing Laboratory

Kenji Yoshino

Ryan Day

UL Verification Services Inc.

San Luis Obispo, CA

Table of Contents

1 Executive Summary

This report documents the NIAP validators' assessment of the CCEVS evaluation of the Klas Voyager Version 1.0 VPN Gateway.

This report is intended to assist the end-users of this product with determining the suitability of this IT product in their environment. End-users should review both the Security Target (ST), which is where specific security claims are made, in conjunction with this Validation Report (VR), which describes how those security claims were evaluated.

The Target(s) of Evaluation (TOE), are the Klas Voyager devices, VoyagerESm and VoyagerSW14 running KlasOS v5.1.0rc7. The TOE is a Network Device that also provides Virtual Private Network Gateway services. The TOE provides the ability to securely encrypt data over WAN links using IPsec and FIPS Approved algorithms. Authentication can be provided locally or over a trusted channel using IPsec or SSH, and all logs can be securely sent to a syslog server. Access Control Lists (ACLs) can filter all types of IP, TCP, and UDP traffic.

This table identifies components that must be present in the Operational Environment to support the operation of the TOE.

Component	Description
VPN Peer	IKEv1 or IKEv2 X.509v3 authentication supporting ECDSA P-256, P-384, or Pre-shared Key Symmetric ciphers: AES-CBC-128, AES-CBC-256, AES-GCM-128, or AES-GCM-256 Integrity algorithms: HMAC-SHA-256 or HMAC-SHA-384 Diffie-Hellman groups: 14, 19, 20, or 24
Syslog Server	RFC 5424 compliant syslog server
NTP Server	NTPv4
Serial Console	VT-100 compatible terminal or emulator
SSH Client	SSHv2 Password, ECDSA P-256, or ECDSA P-384 authentication AES-CBC-128 or AES-CBC-256 encryption HMAC-SHA1, HMAC-SHA2-256, or HMAC-SHA2-512 for message authentication Key exchange using Diffie-Hellman Group 14, ECDH over NIST P-256, or ECDH over NIST P-384

Table 1: Operational Environment Components

2 Identification of the TOE

Table 2 provides information needed to completely identify the product, including:

- The Target of Evaluation (TOE), the fully qualified identifier of the product as evaluated;
- The Security Target (ST), describing the security features, claims, and assurances of the product;
- The conformance result of the evaluation;
- The organizations and individuals participating in the evaluation.

Evaluation Scheme	United States Common Criteria Evaluation Validation Scheme
Evaluated Target of Evaluation	Klas Voyager Hardware: VoyagerESm, VoyagerSW14 Firmware: KlasOS v5.1.0rc7
Protection Profile	collaborative Protection Profile for Network Devices, Version 1.0, Feb. 27, 2015 Network Device Collaborative Protection Profile (NDcPP)/Stateful Traffic Filter Firewall Collaborative Protection Profile (FWcPP) Extended Package VPN Gateway, Version 2.1, March 8, 2017
Security Target	Klas Telecom Voyager Security Target, Version 1.0, September 11, 2017
Dates of Evaluation	March 2017 – September 2017
Conformance Result	Pass
Common Criteria Version	3.1 Revision 4
Common Evaluation Methodology (CEM) Version	CCMB-2012-09-004
Evaluation Technical Report (ETR)	17-3277-R-0028 V1.0
Sponsor/Developer	Klas Telecom, Inc.
Common Criteria Testing Lab (CCTL)	UL Verification Services Inc.
CCTL Evaluators	Kenji Yoshino, Ryan Day
CCEVS Validators	Paul A. Bicknell, Marybeth S. Panock, Kenneth Stutterheim

Table 2: Product Identification

3 Interpretations

The Evaluation Team performed an analysis of the international interpretations of the CC and the CEM and determined that none of the International interpretations issued by the Common Criteria Interpretations Management Board (CCIMB) were applicable to this evaluation.

The TOE is also compliant with all international interpretations with effective dates on or before August 11, 2017.

4 Security Policy

This section contains the product features and denotes which are within the logical boundaries of the TOE. The following Security Functions are supported by the TOE:

- Audit
- Cryptographic Support
- Identification and Authentication
- Security Management
- Protection of the TSF
- Packet Filtering
- TOE Access
- Trusted Path/Channel

4.1 Audit

The TOE generates audit logs for the events specified in FAU_GEN.1 and associates the identity of the user (if applicable) and the time of the event with each audit record.

4.2 Cryptographic Support

The TSF performs the following cryptographic operations:

- DH Group 14
- ECDH P-256 and P-384
- AES-CBC-128, AES-CBC-256, AES-GCM-128, and AES-GCM-256
- ECDSA P-256 and P-384
- RSA 2048 and 3072
- HMAC SHA1, HMAC-SHA2-256, or HMAC-SHA2-512
- CTR_DRBG(AES-256)
- IPsec: IKEv1, IKEv2, and ESP
- SSHv2

The TSF zeroizes all plaintext secret and private cryptographic keys and CSPs once they are no longer required.

4.3 Identification and Authentication

The TOE identifies administrators using a username and password. For authentication over SSH, SSH public-key authentication can be used in lieu of a password.

The TOE supports the use of X.509 certificates for IKE authentication.

4.4 Security Management

The TOE provides secure administrative services for management of general TOE configuration and the security functionality provided by the TOE. All TOE administration occurs via a local console connection. The TOE provides the ability to securely manage:

- All TOE administrative users
- All identification and authentication
- All audit functionality of the TOE
- All TOE cryptographic functionality
- Timestamps maintained by the TOE
- Update to the TOE
- TOE configuration files

Administrators can create configurable login banners to be displayed at time of login and can also define an inactivity timeout to terminate sessions after a set period of inactivity.

4.5 Protection of the TSF

The TOE prevents the reading of secret and private keys. The TOE provides reliable time stamps for itself and synchronizes its time with an NTP server. The TOE runs a suite of self-tests during the initial start-up to demonstrate the correction operation of the TSF. The TOE verifies firmware updates using a digital signature prior to installing those updates.

4.6 Packet Filtering

The TOE filters packets received on the VLAN interfaces. The TOE can be configured to allow or deny the packet based on IP source address, IP destination address, TCP or UDP source port, TCP or UDP destination port.

4.7 TOE Access

The TOE terminates local and remote administrative sessions after a configurable period of inactivity.

Prior to establishing an administrative session, the TOE display a configurable warning banner.

4.8 Trusted Path/Channel

The TOE uses SSH to provide a trusted path for communication with remote administrators. The TOE uses IPsec to provide a trusted channel for communication with trusted IT entities and remote VPN peers.

5 TOE Security Environment

5.1 Secure Usage Assumptions

The following assumptions are made about the usage of the TOE:

A.PHYSICAL_PROTECTION	The network device is assumed to be physically protected in its operational environment and not subject to physical attacks that compromise the security and/or interfere with the device's physical interconnections and correct operation. This protection is assumed to be sufficient to protect the device and the data it contains. As a result, the cPP will not include any requirements on physical tamper protection or other physical attack mitigations. The cPP will not expect the product to defend against physical access to the device that allows unauthorized entities to extract data, bypass other controls, or otherwise manipulate the device.
A.LIMITED_FUNCTIONALITY	The device is assumed to provide networking functionality as its core function and not provide functionality/services that could be deemed as general purpose computing. For example the device should not provide computing platform for general purpose Applications (unrelated to networking functionality).
A.NO_THRU_TRAFFIC_PROTECTION	A standard/generic network device does not provide any assurance regarding the protection of traffic that traverses it. The intent is for the network device to protect data that originates on or is destined to the device itself, to include administrative data and audit data. Traffic that is traversing the network device, destined for another network entity, is not covered by the ND cPP. It is assumed that this protection will be covered by cPPs for particular types of network devices (e.g, firewall).
A.TRUSTED_ADMINISTRATOR	The Security Administrator(s) for the network device are assumed to be trusted and to act in the best interest of security for the organization. This includes being appropriately trained, following policy, and adhering to guidance documentation. Administrators are trusted to ensure passwords/credentials have sufficient strength and entropy and to lack malicious intent when administering the device. The network device is not expected to be capable of defending against a malicious administrator that actively works to bypass or compromise the security of the device.
A.REGULAR_UPDATES	The network device firmware and software is assumed to be updated by an administrator on a regular basis in response to the release of product updates due to known vulnerabilities.
A.ADMIN_CREDENTIALS_SECURE	The administrator's credentials (private key) used to access the network device are protected by the platform on which they reside.
A.CONNECTIONS	It is assumed that the TOE is connected to distinct networks in a manner that ensures that the TOE security policies will be enforced on all applicable network traffic flowing among the attached networks.

5.2 Threats Countered by the TOE

The TOE is designed to counter the following threats:

T.UNAUTHORIZED_ADMINISTRATOR_ACCESS	Threat agents may attempt to gain administrator access to the network device by nefarious means such as masquerading as an administrator to the device, masquerading as the device to an administrator, replaying an administrative session (in its entirety, or selected portions), or performing man-in-the-middle attacks, which would provide access to the administrative session, or sessions between network devices. Successfully gaining administrator access allows malicious

	actions that compromise the security functionality of the device and the network on which it resides.
T.WEAK_CRYPTOGRAPHY	Threat agents may exploit weak cryptographic algorithms or perform a cryptographic exhaust against the key space. Poorly chosen encryption algorithms, modes, and key sizes will allow attackers to compromise the algorithms, or brute force exhaust the key space and give them unauthorized access allowing them to read, manipulate and/or control the traffic with minimal effort.
T.UNTRUSTED_COMMUNICATION_CHANNELS	Threat agents may attempt to target network devices that do not use standardized secure tunneling protocols to protect the critical network traffic. Attackers may take advantage of poorly designed protocols or poor key management to successfully perform man-in-the-middle attacks, replay attacks, etc. Successful attacks will result in loss of confidentiality and integrity of the critical network traffic, and potentially could lead to a compromise of the network device itself.
T.WEAK_AUTHENTICATION_ENDPOINTS	Threat agents may take advantage of secure protocols that use weak methods to authenticate the endpoints – e.g., shared password that is guessable or transported as plaintext. The consequences are the same as a poorly designed protocol, the attacker could masquerade as the administrator or another device, and the attacker could insert themselves into the network stream and perform a man-in-the-middle attack. The result is the critical network traffic is exposed and there could be a loss of confidentiality and integrity, and potentially the network device itself could be compromised.
T.UPDATE_COMPROMISE	Threat agents may attempt to provide a compromised update of the software or firmware which undermines the security functionality of the device. Non-validated updates or updates validated using non-secure or weak cryptography leave the update firmware vulnerable to surreptitious alteration.
T.UNDETECTED_ACTIVITY	Threat agents may attempt to access, change, and/or modify the security functionality of the network device without administrator awareness. This could result in the attacker finding an avenue (e.g., misconfiguration, flaw in the product) to compromise the device and the administrator would have no knowledge that the device has been compromised.
T.SECURITY_FUNCTIONALITY_COMPROMISE	Threat agents may compromise credentials and device data enabling continued access to the network device and its critical data. The compromise of credentials include replacing existing credentials with an attacker's credentials, modifying existing credentials, or obtaining the administrator or device credentials for use by the attacker.
T.PASSWORD_CRACKING	Threat agents may be able to take advantage of weak administrative passwords to gain privileged access to the device. Having privileged access to the device provides the attacker unfettered access to the network traffic, and may allow them to take advantage of any trust relationships with other network devices.
T.SECURITY_FUNCTIONALITY_FAILURE	A component of the network device may fail during start-up or during operations causing a compromise or failure in the

	security functionality of the network device, leaving the device susceptible to attackers.
T.NETWORK_DISCLOSURE	Sensitive information on a protected network might be disclosed resulting from ingress- or egress-based actions.
T. NETWORK_ACCESS	Unauthorized access may be achieved to services on a protected network from outside that network, or alternately services outside a protected network from inside the protected network.
T.NETWORK_MISUSE	Access to services made available by a protected network might be used counter to Operational Environment policies.
T.REPLAY_ATTACK	If malicious or external IT entities are able to gain access to the network, they may have the ability to capture information traversing throughout the network and send them on to the intended receiver.
T.DATA_INTEGRITY	A malicious party attempts to change the data being sent – resulting in loss of integrity.

5.3 Organizational Security Policies

The TOE is designed to fulfill the following OSP:

P.ACCESS_BANNER	The TOE shall display an initial banner describing restrictions of use, legal agreements, or any other appropriate information to which users consent by accessing the TOE.

6 Architectural Information

The TOE is classified as VPN Gateway Network Device for Common Criteria purposes. The TOE is made up of hardware and firmware components.

The TOE consists of KlasOS v5.1.0rc7 and one of the following hardware models:

- VoyagerESm
- VoyagerSW14

KlasOS v5.1.0rc7 is based on Linux Kernel 2.6.31.8.

The VoyagerESm contains 4 FastEthernet ports, 1 GigabitEthernet port, 2 USB ports, 1 VIK slot (removable storage), 1 FXS port and a console port.

The VoyagerSW14 contains 12 FastEthernet ports, 2 GigabitEthernet ports, 1 VIK slot and a console port.
Both hardware models use an ARMv5TE Feroceon Rev0 v5I processor.

7 Documentation

This section details the documentation that is (a) delivered to the customer, and (b) was used as evidence for the evaluation of the Klas Voyager VPN Gateway. In these tables, the following conventions are used:

- Documentation that is delivered to the customer is shown with **bold** titles.
- Documentation that was used as evidence but is not delivered is shown in a normal

typeface.

- Documentation that is delivered as part of the product but was not used as evaluation is shown with a hashed background.

The vendor documents that apply to the CC evaluation are identified below:

7.1 Design Documentation

Document	Revision	Date
Klas Voyager Assurance Questionnaire (625-8315)	1.2	August 2017
Klas Voyager Entropy Design and Analysis	1.6	February 2017

7.2 Guidance Documentation

Document	Revision	Date
Klas Voyager Common Criteria Operational User Guidance	**1.7**	**August 2017**
VOYAGERESm Hardware Reference Guide	**1.0**	**November 2014**
VOYAGERSW14 Hardware Reference Guide	**2.1**	**August 2014**
KlasOS Software Configuration Guide	**4.3.2**	

7.3 Security Target

Document	Revision	Date
Klas Telecom Voyager Security Target	1.0	September 11, 2017

Please note that any other documentation delivered with the product or that may be accessible on-line that is not listed above was not included in the scope of the evaluation, nor was it used to set the product into its evaluated configuration, and therefore should not be relied upon to place the device into the compliant configuration.

8 IT Product Testing

This section describes the testing efforts of the Developer and the Evaluation Team.

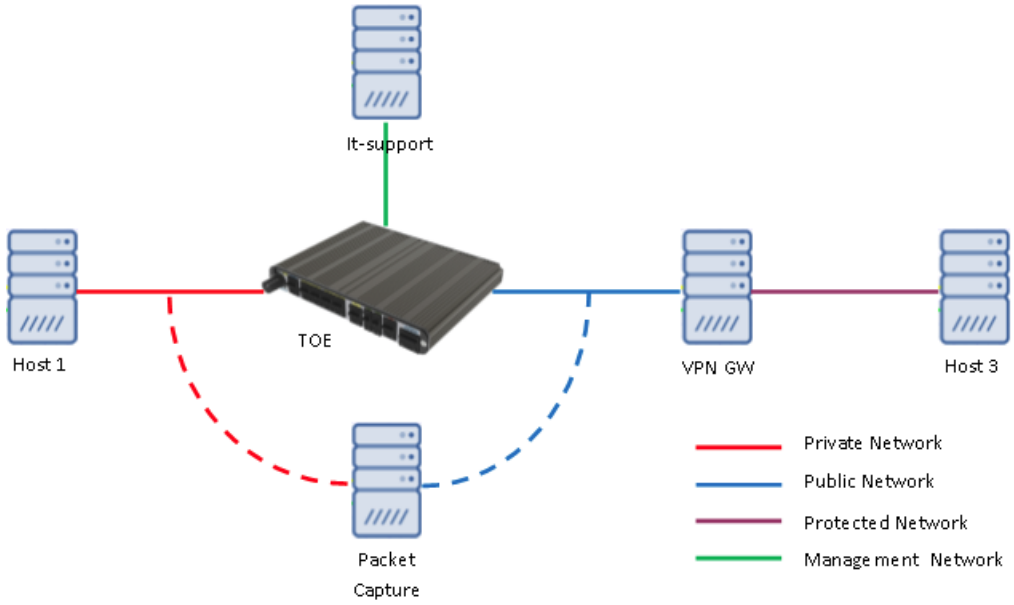
8.1 Evaluation Team Independent Testing

The evaluation team performed the test assurance activities specified in the collaborative

Protection Profile for Network Devices, Version 1.0, Feb. 27, 2015, and the Network Device Collaborative Protection Profile (NDcPP)/Stateful Traffic Filter Firewall Collaborative Protection Profile (FWcPP) Extended Package VPN Gateway, Version 2.1, March 8, 2017. The evaluation team verified that the TOE passed each test.

8.2 Test Environment

The TOE was tested in the following configuration. The evaluation team devised a Test Plan based on the Testing Assurance Activities specified in NDcPP and VPN EP. The evaluation team executed and documented the tests specified in the evaluation sensitive Test Plan. Those results are summarized in the publically available Assurance Activity Report for VID 10767. The evaluated test configuration is below.



8.3 Vulnerability Analysis

A public domain search for potential vulnerabilities was performed. Search terms were limited to the following:

- Klas IKE
- Klas VPN
- Klas IPSec
- Klas SIP
- Klas
- OpenSSH 7.2p2

No potential vulnerabilities were identified that might apply to the TOE. Based on the results, no vulnerabilities existed in the TOE at the time of the evaluation that are exploitable.

8.4 Clarification of Scope

All evaluations (and all products) have limitations, as well as potential misconceptions that need clarifying. This text covers some of the more important limitations and clarifications of this evaluation. Note that:

- As with any evaluation, this evaluation only shows that the evaluated configuration meets the security claims made, with a certain level of assurance - the assurance activities specified in the following,
    - collaborative Protection Profile for Network Devices, Version 1.0, dated February 27, 2015 and the Supporting Document Mandatory Technical Document Evaluation Activities for Network Device cPP, Version 1.0, dated February 27, 2015
    - Network Device Collaborative Protection Profile (NDcPP)/Stateful Traffic Filter Firewall Collaborative Protection Profile (FWcPP) Extended Package VPN Gateway, Version 2.1, March 8, 2017

  and as performed by the evaluation team. All NIAP Technical Decisions related to the protection profile security functional requirements were considered and applied as necessary.
- This evaluation covers only the specific product and software versions identified in this document, and not any earlier or later versions either released or in process.
- This evaluation did not specifically search for, nor attempt to exploit, vulnerabilities that were not “obvious” or vulnerabilities to objectives not claimed in the ST. The CEM defines an “obvious” vulnerability as one that is easily exploited with a minimum of understanding of the TOE, technical sophistication and resources.
- The functionality evaluated is scoped exclusively to the security functional requirements specified in the collaborative Protection Profile for Network Devices, Version 1.0, and the Network Device Collaborative Protection Profile (NDcPP)/Stateful Traffic Filter Firewall Collaborative Protection Profile (FWcPP) Extended Package VPN Gateway, Version 2.1, March 8, 2017 and applicable Technical Decisions. Any additional security related functional capabilities of the TOE were not covered by this evaluation.

9 Results of the Evaluation

The evaluation was carried out in accordance with the Common Criteria Evaluation and Validation Scheme (CCEVS) processes and procedures. The TOE was evaluated against the criteria contained in the Common Criteria for Information Technology Security Evaluation, Version 3.1 Revision 4. The evaluation methodology used by the Evaluation Team to conduct the evaluation is the Common Methodology for Information Technology Security Evaluation, Version 3.1 Revision 4.

UL has determined that the TOE meets the security criteria in the Security Target, which specifies an assurance level of “PP Compliant”. A team of Validators, on behalf of the CCEVS Validation Body, monitored the evaluation. The evaluation was completed in August 2017.

10 Validator Comments/Recommendations

The Target of Evaluation (TOE), are the Klas Voyager devices, VoyagerESm and VoyagerSW14 running KlasOS v5.1.0rc7. No earlier or later versions of hardware and software were evaluated.

Those employing the devices must follow the configuration instructions provided in the Operational Guidance documentation listed above to ensure the evaluated configuration is established and maintained. The functionality evaluated is scoped exclusively to the security functional requirements specified in the Security Target, and only the functionality implemented by the SFR's within the Security Target was evaluated. All other functionality provided by the devices, to include software that was not part of the evaluated configuration, needs to be assessed separately and no further conclusions can be drawn about their effectiveness. The following available services were NOT evaluated:

- DHCP server
- SNMP server
- TFTP server
- VoIP and SIP services
- OSPF and RIP
- 802.1x and RADIUS
- CDP
- DNS server
- Multicast PIM
- IGMP snooping

The devices are capable of utilizing external storage via the VIK slot. This functionality was not tested nor was the interface exercised.

It should be noted that the audit capabilities of the TOE are such that when local audit storage space is full, the current logfile is deleted and a new log file is created. It is suggested that the administrator configure the device to work with a syslog server to ensure log retention.

11 Security Target

Klas Telecom Voyager Security Target, Version 1.0, September 11, 2017.

12 Terms

12.1 Acronyms

CAVP	Cryptographic Algorithm Validation Program
CC	Common Criteria
CSP	Critical Security Parameters
DAC	Discretionary Access Control
EAL	Evaluation Assurance Level

FIPS	Federal Information Processing Standards Publication 140-2
IDS	Intrusion Detection System
IPS	Intrusion Prevention System
I/O	Input/Output
MIB	Management Information Base
NIST	National Institute of Standards and Technology
OCSP	Online Certificate Status Protocol
PP	Protection Profile
SF	Security Functions
SFR	Security Functional Requirements
ST	Security Target
TOE	Target of Evaluation
TSF	TOE Security Functions

13 Bibliography

[1] Common Criteria for Information Technology Security Evaluation – Part 1: Introduction and general model, dated September 2012, Version 3.1 Revision 4, CCMB-2012-09-001.

[2] Common Criteria (CC) for Information Technology Security Evaluation – Part 2: Security functional components, September 2012, Version 3.1, Revision 4, CCMB-2012-09-002.

[3] Common Criteria for Information Technology Security Evaluation – Part 3: Security assurance components, September 2012, Version 3.1, Revision 4, CCMB-2012-09-003.

[4] Common Methodology for Information Technology Security Evaluation – Evaluation methodology, September 2012, Version 3.1, Revision 4, CCMB-2012-09-004.

[5] collaborative Protection Profile for Network Devices, Version 1.0, February 27 2015

[6] Supporting Document Mandatory Technical Document Evaluation Activities for Network Device cPP, Version 1.0, February 2015.

[7] Network Device Collaborative Protection Profile (NDcPP)/Stateful Traffic Filter Firewall Collaborative Protection Profile (FWcPP) Extended Package VPN Gateway, Version 2.1, March 8, 2017.

[8] Assurance Activity Report VID10767, 17-3277-R-0029 V1.0, August 25, 2017

[9] Common Criteria Evaluation Technical Report VID10767, 17-3277-R-0028, Version 1.0, August 25, 2017 <Evaluation Sensitive>

[10] Klas Voyager Common Criteria Operational User Guidance, Version 1.6, August, 2017