National Information Assurance Partnership

Common Criteria Evaluation and Validation Scheme

Validation Report

KlasOS Keel 5.4.0

Report Number: CCEVS-VR-VID11436-2024

Dated: July 16, 2024

Version: 1.0

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

Department of Defense
Attn: NIAP, Suite 6982
9800 Savage Road
Fort Meade, MD 20755-6982

ACKNOWLEDGEMENTS

Validation Team

Daniel Faigin

Marybeth Panock

Mike Quintos

The Aerospace Corporation

Farid Ahmed

Russell Fink

Anne Gugel

Michael Smeltzer

Johns Hopkins University APL

Common Criteria Testing Laboratory

Furukh Siddique

Minal Wankhede

Snehal Gaonkar

Alexander Fannin

Acumen Security, LLC

Table of Contents

1 Executive Summary

This Validation Report (VR) is intended to assist the end user of this product and any security certification Agent for that end user in determining the suitability of this Information Technology (IT) product for their environment. End users should review the Security Target (ST), which is where specific security claims are made, in conjunction with this VR, which describes how those security claims were tested and evaluated and any restrictions on the evaluated configuration. Prospective users should carefully read the Assumptions and Clarification of Scope in Section 5 and the Validator Comments in Section 10, where any restrictions on the evaluated configuration are highlighted.

This report documents the National Information Assurance Partnership (NIAP) assessment of the evaluation of the KlasOS Keel 5.4.0 Target of Evaluation (TOE). It presents the evaluation results, their justifications, and the conformance results. This VR is not an endorsement of the TOE by any agency of the U.S. Government and no warranty of the TOE is either expressed or implied. This VR applies only to the specific version and configuration of the product as evaluated and documented in the ST.

The evaluation was completed by Acumen Security in July 2024. The information in this report is largely derived from the Evaluation Technical Report (ETR) and associated test report, all written by Acumen Security. The evaluation determined that the product is both Common Criteria Part 2 Extended and Part 3 Conformant, and meets the assurance requirements defined in the PP-Configuration for Network Device and Stateful Traffic Filter Firewalls [CFG_NDcPP-FW_v1.4e]: collaborative Protection Profile for Network Devices, Version 2.2e [CPP_ND_V2.2E] and PP-Module for Stateful Traffic Filter Firewalls, Version 1.4e [MOD_CPP_FW_V1.4E].

The Target of Evaluation (TOE) identified in this Validation Report has been evaluated at a NIAP approved Common Criteria Testing Laboratory using the Common Methodology for IT Security Evaluation (Version 3.1, Rev. 5) for conformance to the Common Criteria for IT Security Evaluation (Version 3.1, Rev. 5), as interpreted by the Assurance Activities contained in the aforementioned Protection Profiles. This Validation Report applies only to the specific version of the TOE as evaluated. The evaluation has been conducted in accordance with the provisions of the NIAP Common Criteria Evaluation and Validation Scheme and the conclusions of the testing laboratory in the evaluation technical report are consistent with the evidence provided.

The validation team provided guidance on technical issues and evaluation processes and reviewed the individual work units documented in the ETR and the Assurance Activities Report (AAR). The validation team found that the evaluation showed that the product satisfies all of the functional requirements and assurance requirements stated in the Security Target (ST). Based on these findings, the validation team concludes that the testing laboratory's findings are accurate, the conclusions justified, and the conformance results are correct. The conclusions of the testing laboratory in the evaluation technical report are consistent with the evidence produced.

2 Identification

The CCEVS is a joint National Security Agency (NSA) and National Institute of Standards and Technology (NIST) effort to establish commercial facilities to perform trusted product evaluations. Under this program, security evaluations are conducted by commercial testing laboratories called Common Criteria Testing Laboratories (CCTLs). CCTLs evaluate products against Protection Profile containing Assurance Activities, which are interpretation of CEM work units specific to the technology described by the PP.

The NIAP Validation Body assigns Validators to monitor the CCTLs to ensure quality and consistency across evaluations. Developers of information technology products desiring a security evaluation contract with a CCTL and pay a fee for their product's evaluation. Upon successful completion of the evaluation, the product is added to NIAP's Product Compliance List.

Table 1 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 Protection Profile(s) to which the product is conformant.
- The organizations and individuals participating in the evaluation.

Table 1: Evaluation Identifiers

Item	Identifier
Evaluation Scheme	United States NIAP Common Criteria Evaluation and Validation Scheme
TOE	KlasOS Keel 5.4.0
Protection Profile	• PP-Configuration for Network Device and Stateful Traffic Filter Firewalls [CFG_NDcPP-FW_v1.4e] o collaborative Protection Profile for Network Devices, Version 2.2e [CPP_ND_V2.2E] o PP-Module for Stateful Traffic Filter Firewalls, Version 1.4e [MOD_CPP_FW_V1.4E]
Security Target	KlasOS Keel 5.4.0 Security Target
Evaluation Technical Report	Evaluation Technical Report for KlasOS Keel Version 5.4.0
CC Version	Version 3.1, Revision 5
Conformance Result	CC Part 2 Extended and CC Part 3 Extended
Sponsor	Klas
Developer	Klas
Common Criteria Testing Lab (CCTL)	Intertek Acumen Security Rockville, MD
CCEVS Validators	Daniel Faigin, Marybeth Panock, Mike Quintos, Farid Ahmed, Russel Fink, Anne Gugel, Michael Smeltzer

3 Architectural Information

The TOE is Klas OS Keel 5.4.0 running on the VoyagerVMm, TRX R2 and Voyager VM3.0 platforms (herein referred to as the TOE). It runs the KlasOS Keel firmware combining both connectivity and local compute capabilities. Network connectivity includes ethernet and SDWAN. Computing and firewall capabilities are combined in one unit. This provides users with cloud connectivity when necessary and local processing power for analytics when there is no backhaul. Administration can be performed locally or over a trusted SSH channel.

4 Security Policy

The TOE provides the security functions required by the Collaborative Protection Profile for Network Devices, Version 2.2e and PP-Module for Stateful Traffic Filter Firewall, Version 1.4e. The TOE implements the following security requirements:

- Security Audit (FAU)
- Cryptographic Support (FCS)
- User Data Protection (FDP)
- Firewall (FFW)
- Identification and Authentication (FIA)
- Security Management (FMT)
- Protection of the TSF (FPT)
- TOE Access (FTA)
- Trusted Path/Channels (FTP)

4.1 Security Audit (FAU)

The TOE generates audit events for all start-up and shutdown functions as well as all auditable events specified in ST Table 13 - Security Functional Requirements and Auditable Events. Audit events are also generated for management actions specified in FAU_GEN.1. The TOE stores audit records locally and can export them to an external syslog server using SSHv2 as a tunnel. Each audit record contains the date and time of the event, type of event, subject identity, and other relevant data for the event. Only a security administrator can enable logging to a syslog server.

4.2 Cryptographic Support (FCS)

The cryptographic support used in the TOE are presented in the following table.

Table 2 – TOE Cryptography Implementation

Cryptographic Methods	Usage
FCS_CKM.1 Cryptographic Key Generation	• RSA schemes using cryptographic key sizes of 2048-bit or greater that meet the following: FIPS PUB 186-4, “Digital Signature Standard (DSS)”, Appendix B.3; • ECC schemes using ‘NIST curves’ [selection: P-256, P-384, P-521] that meet the following: FIPS PUB 186-4, “Digital Signature Standard (DSS)”, Appendix B.4; • FFC Schemes using ‘safe-prime’ groups that meet the following: “NIST Special Publication 800-56A Revision 3, Recommendation for Pair-Wise Key

Cryptographic Methods	Usage
	Establishment Schemes Using Discrete Logarithm Cryptography" and [RFC 3526, RFC 7919].
FCS_CKM.2 Cryptographic Key Establishment	• RSA-based key establishment conforming to RSAES-PKCS1-v1_5 as specified in Section 7.2 of RFC 3447, Public-Key Cryptography Standards (PKCS) #1: RSA Cryptography Specifications Version 2.1 • Elliptical curve-based establishment conforming to NIST Special Publication 800-56A Revision 3, "Recommendation for Pair-Wise Key Establishment Schemes Using Discrete Logarithm Cryptography"; • FFC Schemes using "safe-prime" groups that meet the following: 'NIST Special Publication 800-56A Revision 3, "Recommendation for Pair-Wise Key Establishment Schemes Using Discrete Logarithm Cryptography" and [groups listed in RFC 3526].
FCS_CKM.4 Cryptographic Key Destruction	• Refer to ST **Error! Reference source not found.** for Key Zeroization details.
FCS_COP.1/DataEncryption Cryptographic Operations (AES Data Encryption/Decryption)	• AES encryption and decryption conforming to CBC, CTR and GCM as specified in ISO 10116. • AES key size supported is 128 and 256 bits. • AES modes supported are CBC, CTR and GCM.
FCS_COP.1/Hash Cryptographic Operations (Hash Algorithm)	• Cryptographic hashing services conforming to ISO/IEC 10118-3:2004. • Hashing algorithms supported are: SHA-1, SHA-256, SHA-384, and SHA-512. • Message digest sizes supported are: 160, 256, 384, and 512 bits.
FCS_COP.1/KeyedHash Cryptographic Operation (Keyed Hash Algorithm)	• Keyed-hash message authentication conforming to ISO/IEC 9797-2:2011, Section 7 "MAC Algorithm2". • Keyed hash algorithm supported are: HMAC-SHA1, HMAC-SHA-256, HMAC-SHA384, and HMAC-SHA-512 • Key sizes supported are: 160, 256, 384 and 512 bits. • Message digest sizes supported are: 160, 256, 384, and 512 bits.
FCS_COP.1/SigGen Cryptographic Operation (Signature Generation and Verification)	• RSA digital signature algorithm conforming to FIPS PUB 186-4, "Digital Signature Standard (DSS)", Section 5.5, using PKCS #1

Cryptographic Methods	Usage
	v2.1 Signature Schemes RSASSA-PSS and/or RSASSA-PKCS1v1_5; ISO/IEC 9796-2, Digital signature scheme 2 or Digital Signature scheme 3. • RSA key sizes supported are: 2048, 3072, and 4096 bits. • Elliptical curve digital signature algorithm conforming to FIPS PUB 186-4, "Digital Signature Standard (DSS)", Section 6 and Appendix D, Implementing NIST curves ISO/IEC 14888-3, Section 6.4. • Elliptical curve key sizes supported are 256, 384 and 521 bits.
FCS_DTLSC_EXT.1 DTLS Client Protocol without Mutual Authentication	• The TOE supports DTLS version 1.2 for secure communication between TOEs.
FCS_DTLSC_EXT.2 DTLS Client Protocol with Mutual Authentication	• The TOE supports DTLS version 1.2 for secure communication between TOEs using mutual authentication.
FCS_DTLSS_EXT.1 DTLS Server Protocol without Mutual Authentication	• The TOE supports DTLS version 1.2 for secure communication between TOEs.
FCS_DTLSS_EXT.2 DTLS Server Protocol with Mutual Authentication	• The TOE supports DTLS version 1.2 for secure communication between TOEs using mutual authentication
FCS_HTTPS_EXT.1 HTTPS Protocol	• The TOE supports HTTPS using TLS and complies with RFC 2818.
FCS_NTP_EXT.1 NTP Protocol	• The TOE supports NTP v3 and adheres to RFC 1305. • Authentication is performed using SHA-1 as the message digest algorithm.
FCS_RBG_EXT.1 Random Bit Generation	• Random number generation conforming to ISO/IEC 18031:2011 Table C.1 "Security Strength Table for Hash Functions" • The TOE leverages CTR_DRBG(AES) • CTR_DRBG seeded with a minimum of 256 bits of entropy.
FCS_SSHS_EXT.1 SSH Server Protocol	• The TOE supports SSH v2 protocol compliant to the following RFCs:4251, 4252, 4253, 4254, 5656, and 6668. • The TOE supports password-based and public-key-based authentication. • SSH public-key authentication uses ssh-rsa, ecdsa-sha2-nistp256 and ecdsa-sha2-nistp384. • SSH transport uses the following encryption algorithms: aes128-cbc, and aes256-cbc.

Cryptographic Methods	Usage
	• Packets greater than 33,292 bytes in an SSH transport connection are dropped. • SSH transport uses the following data integrity MAC algorithms: hmac-sha1, hmac-sha2-256, hmac-sha384, and hmac-sha2-512 • Key exchange algorithms supported are: diffie-hellman-group14- sha1, ecdh-sha2-nistp256 and ecdh-sha2-nistp384. • The TOE ensures that during SSH connections, the same session keys are used for a threshold of no longer than one hour and no more than one gigabyte of transmitted data.
FCS_TLSS_EXT.1 TLS Server Protocol Without Mutual Authentication	• The TOE supports TLS 1.2 (RFC 5246) for HTTPS connections

4.3 User Data Protection (FDP)

For firewall traffic flowing through the TOE any previous information is made unavailable when a new resource is required to be allocated. This ensure that data is not inadvertently sent to an unintended recipient.

4.4 Firewall (FFW)

The rules allow traffic traversing the TOE to be permitted or dropped and the administrator can choose whether logging occurs when the rule's conditions are met.

4.5 Identification and Authentication (FIA)

All users must be authenticated by the TOE prior to carrying out any administrative actions. The TOE supports password-based and public-key based authentication. An administrator can set a minimum password length on the TOE which must be at least 15 characters.

4.6 Security Management (FMT)

The TOE supports local and remote management of its security functions including:

- Ability to configure the access banner
- Ability to configure the session inactivity time before session termination or locking
- Ability to update the TOE, and to verify the updates using digital signature capability prior to installing those updates
- Ability to configure the authentication failure parameters for FIA_AFL.1
- Ability to start and stop services
- Ability to modify the behavior of the transmission of audit data to an external IT entity
- Ability to manage the cryptographic keys
- Ability to configure the cryptographic functionality

- Ability to re-enable an Administrator account
- Ability to set the time which is used for time-stamps
- Ability to configure NTP
- Ability to configure the reference identifier for the peer
- Ability to manage the TOE's trust store and designate X509.v3 certificates as trust anchors
- Ability to import X.509v3 certificates to the TOE's trust store
- Ability to manage the trusted public keys database
- Ability to configure firewall rules

The administrative user can perform all the above security-related management functions.

4.7 Protection of the TSF (FPT)

The TOE protects all passwords, pre-shared keys, symmetric keys, and private keys from unauthorized disclosure. Passwords are stored as SHA 512 hashes. The TOE executes self-tests during initial start-up to ensure correct operation and enforcement of its security functions. The TOE internally maintains the date and time. An administrator can install software updates to the TOE after they are verified using a digital signature mechanism.

4.8 TOE Access (FTA)

The TOE displays a customizable banner before any administrative session can be established with it. The TOE will terminate local or remote interactive sessions after a specified period of session inactivity configured by an administrator. An administrator can terminate their own interactive local or remote sessions.

4.9 Trusted Path/Channels (FTP)

The TOE supports SSH for secure communications with authorized IT entities such as syslog servers. The TOE supports SSHv2 (remote CLI) for secure remote administration. The TOE also supports DTLS for secure communication between TOEs to support SD-WAN.

5 Assumptions, Threats & Clarification of Scope

5.1 Assumptions

The specific conditions listed in the following subsections are assumed to exist in the TOE's environment. These assumptions include both practical realities in the development of the TOE security requirements and the essential environmental conditions on the use of the TOE.

Table 3 – Assumptions

ID	Assumption
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 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 does not include any requirements on physical tamper protection or other physical attack mitigations. The cPP does 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 a 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 and PP-Modules for particular types of Network Devices (e.g., firewall).

ID	Assumption
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 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. (The paragraph that follows is for x509v3 cert-based authentication. If not relevant, remove) For TOEs supporting X.509v3 certificate-based authentication, the Security Administrator(s) are expected to fully validate (e.g. offline verification) any CA certificate (root CA certificate or intermediate CA certificate) loaded into the TOE's trust store (aka 'root store', ' trusted CA Key Store', or similar) as a trust anchor prior to use (e.g. offline verification).
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.RESIDUAL_INFORMATION	The Administrator must ensure that there is no unauthorized access possible for sensitive residual information (e.g. cryptographic keys, keying material, PINs, passwords etc.) on networking equipment when the equipment is discarded or removed from its operational environment.

5.2 Threats

The following table lists the threats addressed by the TOE and the IT Environment. The assumed level of expertise of the attacker for all the threats identified below is Enhanced-Basic.

Table 4 – Threats

ID	Threat
T.MALICIOUS TRAFFIC	An attacker may attempt to send malformed packets to a machine in hopes of causing the network stack or services listening on UDP/TCP ports of the target machine to crash.

ID	Threat
T.NETWORK_ACCESS	With knowledge of the services that are exported by machines on a subnet, an attacker may attempt to exploit those services by mounting attacks against those services.
T.NETWORK_DISCLOSURE	An attacker may attempt to "map" a subnet to determine the machines that reside on the network, and obtaining the IP addresses of machines, as well as the services (ports) those machines are offering. This information could be used to mount attacks to those machines via the services that are exported.
T.NETWORK_MISUSE	An attacker may attempt to use services that are exported by machines in a way that is unintended by a site's security policies. For example, an attacker might be able to use a service to "anonymize" the attacker's machine as they mount attacks against others.
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_COMPROMISE	Threat agents may compromise credentials and device data enabling continued access to the Network Device and its critical data. The compromise of credentials includes replacing existing credentials with an attacker's credentials, modifying existing credentials, or obtaining the Administrator or device credentials for use by the attacker.
T.SECURITY_FUNCTIONALITY_FAILURE	An external, unauthorized entity could make use of failed or compromised security functionality and might therefore subsequently use or abuse security functions without prior authentication to access, change or modify device data, critical network traffic or security functionality of the device.
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.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

ID	Threat
	Administrator would have no knowledge that the device has been compromised.
T.UNTRUSTED_COMMUNICATION_CHANNELS	Threat agents may attempt to target Network Devices that do not use standardized secure tunnelling 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.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.WEAK_AUTHENTICATION_ENDPOINTS	Threat agents may take advantage of secure protocols that use weak methods to authenticate the endpoints, e.g. a 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.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.

5.3 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 level of assurance for this evaluation is defined within the collaborative Protection Profile for Network Devices, Version 2.2e [CPP_ND_V2.2E] and PP-Module for Stateful Traffic Filter Firewalls, Version 1.4e [MOD_CPP_FW_V1.4E].

- Consistent with the expectations of the Protection Profile, this evaluation did not specifically search for, nor seriously attempt to counter, 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 evaluation of security functionality of the product was limited to the functionality specified in the claimed PPs. Any additional security related functional capabilities included in the product were not covered by this evaluation. See Section 7.2 of this report for product functionality that is not included in the scope of evaluation.

6 Documentation

The following document was provided by the vendor with the TOE for evaluation:

- KlasOS Keel 5.4.0 Operational User Guidance Version 0.4 dated June 2024 (AGD)

To use the product in the evaluated configuration, the product must be configured as specified in the guidance documentation listed above. Consumers are encouraged to download the configuration guide from the NIAP website to ensure the device is configured as evaluated.

7 TOE Evaluated Configuration

7.1 Evaluated Configuration

This section provides an overview of the TOE evaluated configuration and physical boundaries. All TOE models below run the same Klas Keel 5.4.0 binary file.

Table 5 – TOE Models

TOE Model	Specifications
VoyagerVMm (i3) and VoyagerVMm (i5) 	5th Gen Intel® Dual Core i3-5010U (1.8 GHz) Broadwell-U, 8 GB DDR3 RAM Network Ports: 1 x console, 4 x Gb Ethernet Storage: Samsung 850 EVO 256 GB mSATA SSD or Samsung 1TB mSATA SSD
	5th Gen Intel® Quad Core i5-5350U (1.8 GHz) Broadwell-U, 32 GB DDR3 RAM Network Ports: 1 x console, 4 x Gb Ethernet Storage: Samsung 850 EVO 256 GB mSATA SSD or Samsung 1TB mSATA SSD
TRX R2 (4-core) and TRX R2 (8 core) 	Atom™/Denverton C3508 Intel® Atom™ Denverton C3508 4-Core processor with 1.6 GHz clock. 8 GB RAM (upgradeable to 32 GB) Network Ports: 2 x 1 Gb Ethernet 4G/LTE Modems Sierra Wireless EM7455 LTE Cat-6 (B1, B2, B3, B4, B5, B7, B12, B13, B20, B25, B26, B29, B30, B41) Sierra Wireless EM7511 LTE Cat-12 (B1, B2, B3, B4, B5, B7, B8, B9, B12, B13, B14, B18, B19, B20, B26, B29, B30, B32, B41, B42, B43, B46, B48, B66) IEEE802.11 ac/b/g/n 3×3 MIMO Wi-Fi modem with data rates of 1.3 Gb/s downlink in 2.4/5 Ghz bands
	Atom™/Denverton C3708 Intel® Atom™ Denverton C3708 8-Core processor with 1.7 GHz clock. 8 GB RAM (upgradeable to 32 GB) Network Ports: 2 x 1 Gb Ethernet 4G/LTE Modems Sierra Wireless EM7455 LTE Cat-6 (B1, B2, B3, B4, B5, B7, B12, B13, B20, B25, B26, B29, B30, B41) Sierra Wireless EM7511 LTE Cat-12 (B1, B2, B3, B4, B5, B7, B8, B9, B12, B13, B14, B18, B19, B20, B26, B29, B30, B32, B41, B42, B43, B46, B48, B66) IEEE802.11 ac/b/g/n 3×3 MIMO Wi-Fi modem with data rates of 1.3 Gb/s downlink in 2.4/5 Ghz bands
VoyagerVM 3.0	Xeon D-1539

TOE Model	Specifications
	Intel® Xeon Processor D1539 16-Core with 48 or 96 GB RAM Network Ports: 1 x console, 2 x 10 GB SFP, 2 x 1GB ethernet Storage: removable SATA dual SSDs, removable NVMe Voyager Ignition Key (VIK+)
	Xeon D-1559 Intel® Xeon Processor D1559 12-Core with 48 or 96 GB RAM Network Ports: 1 x console, 2 x 10 GB SFP, 2 x 1GB ethernet Storage: removable SATA dual SSDs, removable NVMe Voyager Ignition Key (VIK+)
	Xeon D-1577 Intel® Xeon Processor D1577 16-Core with 48 or 96 GB RAM Network Ports: 1 x console, 2 x 10 GB SFP, 2 x 1GB ethernet Storage: removable SATA dual SSDs, removable NVMe Voyager Ignition Key (VIK+)

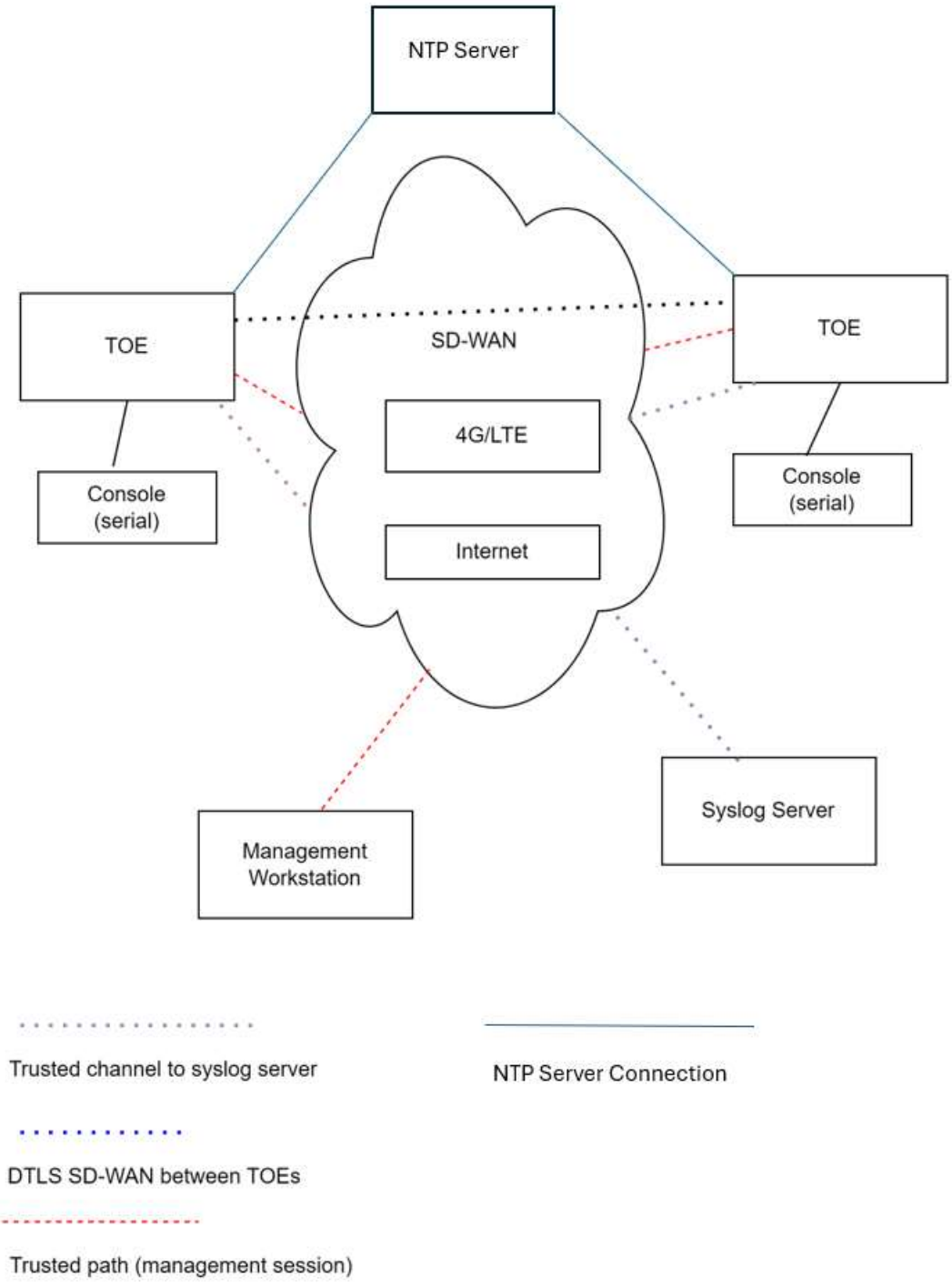

Figure 1 – Representative TOE Deployment

7.1.1 Physical Boundaries

The TOE boundary is the hardware appliance which is comprised of hardware and the KlasOS Keel software component. The TOE hardware models are provided in Table 5 – TOE Models.

The TOE also supports connection to one or more TOEs over a SD-WAN which is protected by DTLS. In the evaluated configuration this connection is not used for TSF data and is used to administer another TOE using SSH over the SD-WAN connection.

The TOE also supports secure connectivity with several other IT environment devices, including the ones identified in Table 3 of the ST.

The TOE implements HTTPS as a limited functionality GUI back to the management workstation. The GUI only offers basic monitoring capabilities and is secured via TLS when an administrator is logged in. Peer certificates are not required for authentication.

7.2 Excluded Functionality

The following product functionality is not included in the CC evaluation:

- SNMP
- Spanning-Tree
- Port Security
- TACACS+
- RADIUS

The TOE has SNMP functionality disabled by default and it should not be enabled for the Common Criteria evaluated configuration.

8 IT Product Testing

This section describes the testing efforts of the developer and the evaluation team. It is derived from information contained in the Evaluation Test Report for KlasOS Keel Version 5.4.0 which is not publicly available. The Assurance Activities Report provides an overview of testing, with the test configuration and tools in Section 4, test cases in Sections 5 and 7, and the prescribed assurance activities in Section 6.

8.1 Developer Testing

No evidence of developer testing is required in the Assurance Activities for this product.

8.2 Evaluation Team Independent Testing

The evaluation team verified the product according to the vendor-provided guidance documentation and ran the tests specified in Collaborative Protection Profile for Network Devices, Version 2.2e [CPP_ND_V2.2E] and PP-Module for Stateful Traffic Filter Firewalls, Version 1.4e [MOD_CPP_FW_V1.4E].

Testing was conducted on the following hardware platforms: VoyagerVMm, TRX R2 and Voyager VM3.0. Testing occurred from May 2023 through July 2024, and took place at Acumen Security offices located at 2400 Research Blvd Suite #395, Rockville, MD 20850.

The Independent Testing activity is documented in the Assurance Activities Report, which is publicly available, and is not duplicated here.

9 Results of the Evaluation

The results of the assurance requirements are generally described in this section and are presented in detail in the proprietary documents: the Detailed Test Report (DTR) and the Evaluation Technical Report (ETR). The reader of this document can assume that activities and work units received a passing verdict.

A verdict for an assurance component is determined by the resulting verdicts assigned to the corresponding evaluator action elements. The evaluation was conducted based upon CC version 3.1 rev 4 and CEM version 3.1 rev 4. The evaluation determined the KlasOS Keel 5.4.0 to be Part 2 extended, and meets the SARs contained in the PP. Additionally the evaluator performed the Assurance Activities specified in the CFG_NDcPP-FW_v1.4e (CPP_ND_V2.2E and MOD_CPP_FW_V1.4E).

9.1 Evaluation of Security Target

The evaluation team applied each ASE CEM work unit. The ST evaluation ensured the ST contains a description of the environment in terms of policies and assumptions, a statement of security requirements claimed to be met by the KlasOS Keel 5.4.0 that are consistent with the Common Criteria, and product security function descriptions that support the requirements. Additionally the evaluator performed an assessment of the Assurance Activities specified in the CFG_NDcPP-FW_v1.4e (CPP_ND_V2.2E and MOD_CPP_FW_V1.4E).

The validator reviewed the work of the evaluation team, and found that sufficient evidence and justification was provided by the evaluation team to confirm that the evaluation was conducted in accordance with the requirements of the CEM, and that the conclusion reached by the evaluation team was justified.

9.2 Evaluation of Development Documentation

The evaluation team applied each EAL 1 ADV CEM work unit. The evaluation team assessed the design documentation and found it adequate to aid in understanding how the TSF provides the security functions. The design documentation consists of a functional specification contained in the Security Target's TOE Summary Specification. Additionally, the evaluator performed the Assurance Activities specified in the CFG_NDcPP-FW_v1.4e (CPP_ND_V2.2E and MOD_CPP_FW_V1.4E) related to the examination of the information contained in the TOE Summary Specification.

The validator reviewed the work of the evaluation team and found that sufficient evidence and justification was provided by the evaluation team to confirm that the evaluation was conducted in accordance with the Assurance Activities, and that the conclusion reached by the evaluation team was justified.

9.3 Evaluation of Guidance Documents

The evaluation team applied each EAL 1 AGD CEM work unit. The evaluation team ensured the adequacy of the user guidance in describing how to use the operational TOE. Additionally, the evaluation team ensured the adequacy of the administrator guidance in describing how to securely administer the TOE. The guides were assessed during the design and testing phases of the evaluation to ensure they were complete. Additionally, the evaluator performed the Assurance Activities specified in the CFG_NDcPP-FW_v1.4e (CPP_ND_V2.2E and MOD_CPP_FW_V1.4E) related to the examination of the information contained in the operational guidance documents.

The validator reviewed the work of the evaluation team and found that sufficient evidence and justification was provided by the evaluation team to confirm that the evaluation was conducted in accordance with the Assurance Activities, and that the conclusion reached by the evaluation team was justified.

9.4 Evaluation of Life Cycle Support Activities

The evaluation team applied each EAL 1 ALC CEM work unit. The evaluation team found that the TOE was identified.

The validator reviewed the work of the evaluation team, and found that sufficient evidence and justification was provided by the evaluation team to confirm that the evaluation was conducted in accordance with the requirements of the CEM, and that the conclusion reached by the evaluation team was justified.

9.5 Evaluation of Test Documentation and the Test Activity

The evaluation team applied each EAL 1 ATE CEM work unit. The evaluation team ran the set of tests specified by the Assurance Activities in the CFG_NDcPP-FW_v1.4e (CPP_ND_V2.2E and MOD_CPP_FW_V1.4E) and recorded the results in a Test Report, summarized in the Evaluation Technical Report and Assurance Activities Report.

The validator reviewed the work of the evaluation team, and found that sufficient evidence was provided by the evaluation team to show that the evaluation activities addressed the test activities in the CFG_NDcPP-FW_v1.4e (CPP_ND_V2.2E and MOD_CPP_FW_V1.4E) , and that the conclusion reached by the evaluation team was justified.

9.6 Vulnerability Assessment Activity

The evaluation team applied each EAL 1 AVA CEM work unit. The evaluation team performed a public search for vulnerabilities, performed vulnerability testing and did not discover any issues with the TOE. The search criteria, the date the search was performed, and a summary of the results can be found in the AAR, Section 6.7. The vulnerability search was last conducted on June 17, 2024.

The validator reviewed the work of the evaluation team, and found that sufficient evidence and justification was provided by the evaluation team to confirm that the evaluation addressed the vulnerability analysis Assurance Activities in the CFG_NDcPP-FW_v1.4e (CPP_ND_V2.2E and MOD_CPP_FW_V1.4E), and that the conclusion reached by the evaluation team was justified.

9.7 Summary of Evaluation Results

The evaluation team's assessment of the evaluation evidence demonstrates that the claims in the ST are met. Additionally, the evaluation team's test activities also demonstrated the accuracy of the claims in the ST.

The validation team's assessment of the evidence provided by the evaluation team is that it demonstrates that the evaluation team performed the Assurance Activities in the CFG_NDcPP-FW_v1.4e (CPP_ND_V2.2E and MOD_CPP_FW_V1.4E), and correctly verified that the product meets the claims in the ST.

10 Validator Comments & Recommendations

The validation team notes that the evaluated configuration is dependent upon the TOE being configured per the configuration guide document listed in Section 6. No other versions of the TOE, either earlier or later, were evaluated.

The functionality evaluated is scoped exclusively to the security functional requirements specified in the Security Target. Other functionality included in the product was not assessed as part of this evaluation. See Section 7.2 of this report for product functionality that is not included in the scope of evaluation.

Additional functionality provided by devices in the operational environment needs to be assessed separately and no further conclusions can be drawn about their effectiveness.

All other items and scope issues have been sufficiently addressed elsewhere in this document.

11 Annexes

Not applicable.

12 Security Target

KlasOS Keel 5.4.0 Security Target Version 1.5, July 5, 2024.

13 Glossary

The following definitions are used throughout this document:

- **Common Criteria Testing Laboratory (CCTL).** An IT security evaluation facility accredited by the National Voluntary Laboratory Accreditation Program (NVLAP) and approved by the CCEVS Validation Body to conduct Common Criteria-based evaluations.
- **Conformance.** The ability to demonstrate in an unambiguous way that a given implementation is correct with respect to the formal model.
- **Evaluation.** The assessment of an IT product against the Common Criteria using the Common Criteria Evaluation Methodology to determine whether or not the claims made are justified; or the assessment of a protection profile against the Common Criteria using the Common Evaluation Methodology to determine if the Profile is complete, consistent, technically sound and hence suitable for use as a statement of requirements for one or more TOEs that may be evaluated.
- **Evaluation Evidence.** Any tangible resource (information) required from the sponsor or developer by the evaluator to perform one or more evaluation activities.
- **Feature.** Part of a product that is either included with the product or can be ordered separately.
- **Target of Evaluation (TOE).** A group of IT products configured as an IT system, or an IT product, and associated documentation that is the subject of a security evaluation under the CC.
- **Validation.** The process carried out by the CCEVS Validation Body leading to the issue of a Common Criteria certificate.
- **Validation Body.** A governmental organization responsible for carrying out validation and for overseeing the day-to-day operation of the NIAP Common Criteria Evaluation and Validation Scheme.

14 Bibliography

The Validation Team used the following documents to produce this Validation Report:

1. Common Criteria for Information Technology Security Evaluation - Part 1: Introduction and general model, Version 3.1 Revision 5, April 2017.
2. Common Criteria for Information Technology Security Evaluation - Part 2: Security functional requirements, Version 3.1 Revision 5, April 2017.
3. Common Criteria for Information Technology Security Evaluation - Part 3: Security assurance requirements, Version 3.1 Revision 5, April 2017.
4. Common Evaluation Methodology for Information Technology Security Evaluation, Version 3.1 Revision 5, April 2017.
5. KlasOS Keel 5.4.0 Security Target, Version 1.5, July 5, 2024.
6. KlasOS Keel 5.4.0 Operational User Guidance, Version 0.4, June 2024.
7. Assurance Activity Report for KlasOS Keel Version 5.4.0, Version 1.5, July 16, 2024.
8. Evaluation Technical Report for KlasOS Keel Version 5.4.0, Version 0.4, July 16, 2024.
9. Vulnerability Assessment for KlasOS Keel 5.4.0, Version 1.2, June 17, 2024.
10. Test Plan for KlasOS Keel 5.4.0 TRX-R2, Version 1.0, July 15, 2024.
11. Test Plan for KlasOS Keel 5.4.0 VM3.0, Version 1.0, July 15, 2024.
12. Test Plan for KlasOS Keel 5.4.0 Voyager VMM, Version 1.0, July 15, 2024.