# National Information Assurance Partnership

# Common Criteria Evaluation and Validation Scheme

# Validation Report

# Persistent Systems LLC, Wave Relay® Devices v1.0

| | |
|---|---|
| **Report Number:** | **CCEVS-VR-VID11509-2025** |
| **Dated:** | **March 27, 2025** |
| **Version:** | **0.1** |

**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

Jerome Myers
Marybeth Panock
Deron Graves

## Common Criteria Testing Laboratory

John Messiha
*Gossamer Security Solutions, Inc.*
*Columbia, MD*

# Table of Contents

# 1 Executive Summary

This report documents the assessment of the National Information Assurance Partnership (NIAP) validation team of the evaluation of Persistent Systems LLC, Wave Relay® Devices v1.0 solution provided by Persistent Systems LLC. It presents the evaluation results, their justifications, and the conformance results. This Validation Report is not an endorsement of the Target of Evaluation by any agency of the U.S. government, and no warranty is either expressed or implied.

The evaluation was performed by the Gossamer Security Solutions (Gossamer) Common Criteria Testing Laboratory (CCTL) in Columbia, MD, United States of America, and was completed in March 2025. The information in this report is largely derived from the Evaluation Technical Report (ETR) and associated test reports, all written by Gossamer Security Solutions. The evaluation determined that the product is both Common Criteria Part 2 Extended and Part 3 Conformant, and meets the assurance requirements of the PP-Configuration for Network Devices, MACsec Ethernet Encryption, and VPN Gateways, Version 1.1, 18 August 2023 (CFG_NDcPP-MACsec-VPNGW_V1.1) which includes the Base PP: collaborative Protection Profile for Network Devices, Version 2.2e, 23 March 2020 (NDcPP22e) with the PP-Module for MACsec Ethernet Encryption, Version 1.0, 02 March 2023 (MACSEC10) and the PP-Module for VPN Gateways, Version 1.3, 16 August 2023 (VPNGW13).

The Target of Evaluation (TOE) is the Persistent Systems LLC, Wave Relay® Devices v1.0.

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). 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 monitored the activities of the evaluation team, provided guidance on technical issues and evaluation processes, and reviewed the individual work units and successive versions of the ETR. 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). Therefore 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.

The technical information included in this report was obtained from the Persistent Systems LLC, Wave Relay® Devices v1.0 Security Target, version 1.0, March 24, 2025 and analysis performed by the Validation Team.

# 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) using the Common Evaluation Methodology (CEM) in accordance with National Voluntary Laboratory Assessment Program (NVLAP) accreditation.

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 Validated Products 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 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** | Persistent Systems LLC, Wave Relay® Devices v1.0<br>(Specific models identified in Section 8) |
| **Protection Profile** | PP-Configuration for Network Devices, MACsec Ethernet Encryption, and VPN Gateways, Version 1.1, 18 August 2023 (CFG_NDcPP-MACsec-VPNGW_V1.1) which includes the Base PP: collaborative Protection Profile for Network Devices, Version 2.2e, 23 March 2020 (NDcPP22e) with the PP-Module for MACsec Ethernet Encryption, Version 1.0, 02 March 2023 (MACSEC10) and the PP-Module for VPN Gateways, Version 1.3, 16 August 2023 (VPNGW13) |
| **ST** | Persistent Systems LLC, Wave Relay® Devices v1.0 Security Target, version 1.0, March 24, 2025 |
| **Evaluation Technical Report** | Evaluation Technical Report for Persistent Systems LLC,Wave Relay® Devices v1.0, version 1.0, March 24, 2025 |
| **CC Version** | Common Criteria for Information Technology Security Evaluation, Version 3.1, rev 5 |
| **Conformance Result** | CC Part 2 extended, CC Part 3 conformant |
| **Sponsor** | Persistent Systems LLC |

| Item | Identifier |
|---|---|
| **Developer** | Persistent Systems LLC |
| **Common Criteria Testing Lab (CCTL)** | Gossamer Security Solutions, Inc.<br>Columbia, MD |
| **CCEVS Validators** | Jerome Myers, Marybeth Panock, Deron Graves |

# 3 Architectural Information

Note: The following architectural description is based on the description presented in the Security Target.

The Target of Evaluation (TOE) is Persistent Systems LLC, Wave Relay® Devices v1.0 running Wave Relay OS 2.2. The TOE provides secure, seamless ethernet connectivity, ensuring global connectivity for users in any location and under any circumstances. By establishing a resilient, secure connectivity fabric, the TOE enables mission-critical communication, regardless of geographical constraints or operational challenges.

## 3.1 TOE Description

The TOE leverages a custom OS called Wave Relay OS that provides a secure operating environment. Available as a hardware network appliance, the TOE supports a wide range of network, wireless and security protocols designed for peer-to-peer MANET networking at OSI Layer 2 and Layer 3. This includes, for instance, the use of multiple layer-3 Gateways in a MANET.

The TOE is capable of securing communication via its ethernet interface with MACsec, IPsec and TLS.  Remote administration utilizes TLS to protect communications to the Wave Relay Device GUI and programmatic interface.

For the purposes of evaluation, the TOE will be treated as a Network Device, IPsec VPN Gateway and MACsec Ethernet Encryption Device. Thus, the security functionality offered by the TOE includes validated secure by design components such as CAVP tested Cryptographic support, Trusted updates, Self Tests, Secure connections, Identification & Authentication, Packet Filtering, and Secure Auditing.

It is important to note that functions outside the scope of NDcPP22e/MACSEC10/VPNGW13 were not evaluated.

## 3.2 TOE Evaluated Platforms

Detail regarding the evaluated configuration is provided in Section 8 below.

## 3.3 TOE Architecture

The Man Portable Unit Generation 5 (MPU5) is a wearable Wave Relay device that can be connected to a wired network and securely communicate with network infrastructure services such as external audit servers, management stations, as well as VPN peers.

The Embedded Module and Embedded Module Lite are Wave Relay embedded devices in a SWaP-timized form factor designed to transform your UAS, UGV platform into a networked asset.

The GVR5 model is a dual band Wave Relay solution, engineered to for tracked and wheeled ground vehicles as well as aircraft.

The Integrated Antenna Series applies the power of Wave Relay directly into an antenna extending the enterprise to the edge of large geographic areas.

The multiple TOE appliance models are designed to support different mission requirements while using the same ARM Cortex-A9 Architecture. NXP i.MX6 series is a family of ARM-based processors designed for a variety of applications balancing power efficiency, performance and flexibility.

While Persistent Systems Wave Relay products can be configured as a collection of independent devices operating in a network, the TOE configuration subject to this evaluation is limited to a single Wave Relay device.

A Persistent Systems Wave Relay device is a network appliance with NXP iMX6 Cortex-A9 CPU running software designed to provide the required capabilities. All Wave Relay Devices include the same validated cryptographic providers that are used to perform cryptographic functions for TLS, IPsec, and MACsec.

- Wave Relay® Kernel Space Crypto Module (HW) version 1.0 (Cert. #A4588)
- Wave Relay® Kernel Space Crypto Module (SW) version 1.0 (Cert. #A4589) All algorithms are supported with PAA and without PAA.
- Wave Relay® User Space Crypto Module version 1.0 (Cert. #A5177). All algorithms are supported with PAA and without PAA

## 3.4 Physical Boundaries

The physical boundaries of the TOE consist of the physical boundaries of the Persistent Systems Wave Relay device.

# 4 Security Policy

This section summaries the security functionality of the TOE:

1. Security audit
2. Cryptographic support
3. Identification and authentication
4. Security management

5. Packet filtering
6. Protection of the TSF
7. TOE access
8. Trusted path/channels

## 4.1 Security audit

The TOE generates audit events for numerous activities including events related to cryptographic functionality, identification and authentication, and administrative actions. The TOE generates a complete audit record including the IP address of the TOE, the event details, and the time the event occurred. The TOE provides the administrator with a local circular audit trail where the TOE overwrites the oldest audit records with the newest audit records when space is full. Audit logs are also sent to a remote syslog server in the environment over TLS encrypted channel.

## 4.2 Cryptographic support

The TOE provides cryptography in support of other TOE security functionality. The TOE provides cryptography in support of secure connections using IPsec, TLS, MACsec and remote administrative management HTTPS/TLS.

## 4.3 Identification and authentication

The TOE allows unauthenticated users to read the login banner, view the TOE identity (DNS name and IP address), view the TOE power level, and view status. The TOE also performs packet filtering operations prior to administrator login. The TOE requires users to be authenticated before all other administrative operations.

The TOE authenticates the administrator prior to granting access to the GUI and programmatic interfaces by accepting a password. The TOE supports the validation of x509v3 certificates for authentication in the context of the TLS and IPsec protocols. These certificates can be ECDSA certificates. The TOE also supports pre-shared key authentication for MACsec and IPsec connections. The TOE checks the revocation status of a certificate using OCSP or CRLs.

## 4.4 Security management

Security management commands are limited to authorized users (i.e., administrators) and available only after they have provided acceptable user identification and authentication data to the TOE. All TOE administration occurs through a TLS/HTTPS session.

## 4.5 Packet filtering

The TOE provides packet filtering and secure IPsec tunneling functionality. The tunnels can be established between the TOE and a VPN peer. An authorized administrator can define the traffic that needs to be protected via IPsec by configuring access lists (permit, deny, log) and applying these access lists to the VPN interfaces.

## 4.6 Protection of the TSF

The TOE provides a variety of means of protecting itself. The TOE performs self-tests and integrity verification that cover the correct operation of the TOE at startup. Any test failures that occur will prevent the TOE from booting to a usable state. It provides functions necessary to securely update the TOE. The TOE includes a hardware clock to ensure reliable timestamps. The TOE's time can be configured manually or by syncing to a remote NTP server. It protects sensitive data such as stored passwords and cryptographic keys so that they are not accessible through the TOE, even to a Security Administrator.

The TOE has the ability detect replay of frames received over the MACsec channel. The detected replayed frames are dropped.

## 4.7 TOE access

The TOE can be configured to display a logon banner before a user session is established. The TOE also enforces inactivity timeouts for local and remote sessions that can be configured by an administrator.

## 4.8 Trusted path/channels

The TOE protects interactive communication with administrators using TLS for GUI and programmatic access. The TLS protocol provides integrity and disclosure protection. If the negotiation of a TLS session fails, the attempted connection will not be established.

The TOE protects communication with network peers, such as an external audit server (syslog server) and a VPN peer using IPsec connections to provide disclosure or modification protections. The TOE can be configured to use MACsec to secure the channel to an external audit server (syslog server) at Layer 2. The TOE can also provide a TLS connection to a controlled network device and validate the X509v3 certificate that is presented by the device.

# 5 Assumptions & Clarification of Scope

***Assumptions***

The Security Problem Definition, including the assumptions, may be found in the following documents:

- collaborative Protection Profile for Network Devices, Version 2.2e, 23 March 2020 (NDcPP22e)
- PP-Module for MACsec Ethernet Encryption, Version 1.0, 02 March 2023 (MACSEC10)
- PP-Module for VPN Gateways, Version 1.3, 16 August 2023 (VPNGW13)

That information has not been reproduced here and the NDcPP22e/MACsec10/VPNGW13 should be consulted if there is interest in that material.

The scope of this evaluation was limited to the functionality and assurances covered in the NDcPP22e/MACsec10/VPNGW13 as described for this TOE in the Security Target. Other functionality included in the product was not assessed as part of this evaluation. All other functionality provided by the devices needs to be assessed separately, and no further conclusions can be drawn about their effectiveness.

***Clarification of scope***

All evaluations (and all products) have limitations, as well as potential misconceptions that need clarification. 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 collaborative Protection Profile for Network Devices and the MACsec and VPNGW Modules and performed by the evaluation team).
- This evaluation covers only the specific device models and software as identified in this document, and not any earlier or later versions released or in process.
- Apart from the Admin Guide, additional customer documentation for the specific VPN Gateway, MACsec Ethernet Encryption models was not included in the scope of the evaluation and therefore should not to be relied upon when configuring or operating the device as evaluated.
- 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 NDcPP22e/MACsec10/VPNGW13 and applicable Technical Decisions. Any additional security related functional capabilities of the TOE were not covered by this evaluation.

# 6 Documentation

The following documents were available with the TOE for evaluation:

- Common Criteria Administrator Guide, Target of Evaluation: Persistent Systems LLC, Wave Relay® Devices v1.0, version 1.0, March 24, 2025

Any additional customer documentation provided with the product, or that is available online was not included in the scope of the evaluation and therefore should not to be relied upon when configuring or operating the device as evaluated.

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 guides from the NIAP website to ensure the device is configured as evaluated.

# 7 IT Product Testing

This section describes the testing efforts of the developer and the Evaluation Team. It is derived from information contained in the proprietary Detailed Test Report for Persistent Systems LLC, Wave Relay® Devices v1.0, version 1.0, March 24, 2025 (DTR), as summarized in the evaluation Assurance Activity Report (AAR).

## 7.1 Developer Testing

No evidence of developer testing is required in the assurance activities for this product.

## 7.2 Evaluation Team Independent Testing

The evaluation team verified the product according to a Common Criteria Certification document and ran the tests specified in the NDcPP22e/MACsec10/VPNGW13 including the tests associated with optional requirements. The AAR, in sections 1.1 lists the tested devices, provides a list of test tools, and has diagrams of the test environment.

# 8 Evaluated Configuration

The TOE is a hardware network appliance available in several models with varying form factors.

| Model | Processor |
|---|---|
| MPU5 (WR-5100) | NXP iMX6 |
| Embedded Module (WR-5200) | NXP i.MX6 |
| Embedded Module Lite (WR-5250) | NXP i.MX6 |
| GVR5 (WR-GVR5-SYS) | NXP i.MX6 |
| Integrated Antenna Series (WR-INT-ANT-SYS) | NXP i.MX6 |

# 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 ETR. The reader of this document can assume that all assurance 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 5 and CEM version 3.1 rev 5. The evaluation determined the Wave Relay® Devices v1.0 TOE to be Part 2 extended, and to meet the SARs contained in the NDcPP22e/MACsec10/VPNGW13.

## 9.1 Evaluation of the Security Target (ASE)

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 Persistent Systems LLC, Wave Relay® Devices v1.0 products that are consistent with the Common Criteria, and product security function descriptions that support the requirements.

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 the Development (ADV)

The evaluation team applied each 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 and Guidance documents. Additionally the evaluator performed the assurance activities specified in the NDcPP22e/MACsec10/VPNGW13 related to the examination of the information contained in the TSS.

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.

## 9.3 Evaluation of the Guidance Documents (AGD)

The evaluation team applied each 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. All of the guides were assessed during the design and testing phases of the evaluation to ensure they were complete.

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.

## 9.4 Evaluation of the Life Cycle Support Activities (ALC)

The evaluation team applied each 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 the Test Documentation and the Test Activity (ATE)

The evaluation team applied each ATE CEM work unit. The evaluation team ran the set of tests specified by the assurance activities in the NDcPP22e/MACsec10/VPNGW13 and recorded the results in a Test Report, summarized in the AAR.

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.

## 9.6 Vulnerability Assessment Activity (VAN)

The evaluation team applied each AVA CEM work unit. The vulnerability analysis is in the Detailed Test Report (DTR) prepared by the evaluator. The vulnerability analysis includes a public search for vulnerabilities. The public search for vulnerabilities did not uncover any residual vulnerability.

The evaluator searched the National Vulnerability Database (https://web.nvd.nist.gov/view/vuln/search) and Vulnerability Notes Database (http://www.kb.cert.org/vuls/) with the following search terms: “Persistent”, “Persistent Systems”, “MPU5”, “WR-5100”, “Man Portable Unit Generation 5”, “Wave Relay”, “Wave Relay OS 2.2”, “Mobile Ad Hoc Networking”, “MANET Radio”, “NXP i.MX 6”, “NXP iMX6 Cortex-A9”, “Wave Relay Kernel Space Crypto Module version 1.0”, “Wave Relay User Space Crypto Module version 1.0”, “OpenSSL 3.1.5”, “StrongSwan 5.9.14”, “wpa_supplicant v2.10”.

The search was performed on March 24, 2025

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.

## 9.7 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 testing 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 followed the procedures defined in the CEM, 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 evaluated configuration instructions in the guidance documents listed in Section 6. No versions of the TOE and software, either earlier or later were evaluated. Please note that 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.

All other concerns and issues are adequately addressed in other parts of this document.

# 11 Annexes

Not applicable

# 12 Security Target

The Security Target is identified as: *Persistent Systems LLC, Wave Relay® Devices v1.0 Security Target, version 1.0, March 24, 2025*.

# 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 components, Version 3.1, Revision 5, April 2017.

[3] Common Criteria for Information Technology Security Evaluation Part 3: Security assurance components, Version 3.1 Revision 5, April 2017.

[4] collaborative Protection Profile for Network Devices, Version 2.2e, 23 March 2020 (NDcPP22e).

[5] PP-Module for MACsec Ethernet Encryption, Version 1.0, 02 March 2023 (MACSEC10).

[6] PP-Module for VPN Gateways, Version 1.3, 16 August 2023 (VPNGW13).

[7] Persistent Systems LLC, Wave Relay® Devices v1.0 Security Target, version 1.0, March 24, 2025 (ST).

[8] Assurance Activity Report for Persistent Systems LLC, Wave Relay® Devices v1.0, version 1.0, March 24, 2025 (AAR).

[9] Common Criteria Administrator Guide Target of Evaluation: Persistent Systems LLC, Wave Relay® Devices v1.0, March 24, 2025 (AGD).

[10] Detailed Test Report for Persistent Systems LLC, Wave Relay® Devices v1.0, version 1.0, March 24, 2025 (DTR).

[11] Evaluation Technical Report for Persistent Systems LLC, Wave Relay® Devices v1.0, version 1.0, March 24, 2025 (ETR).