Routing Working Group
Internet-Draft
Intended status: Standards Track
Expires: 7 August 2026

J. E. W. V
Department of the Air Force
S. Kanno
GMO Internet Group, Inc.
3 February 2026

PRISM: Protocol for Routing Intelligent Service Mapping
draft-willman-rtgwg-prism-sdwan-00

Abstract

This document specifies PRISM, an application-aware traffic steering protocol for Software-Defined Wide Area Networks (SD-WAN). PRISM provides deep application identification, per-flow tracking, Service Level Agreement (SLA) enforcement, and policy-based path selection integration with Segment Routing over IPv6 (SRv6).

PRISM is designed as a companion protocol to CONDUIT (Cryptographic Orchestration of Network Distributed Underlay for IPsec Transport), together providing a complete open-standard SD-WAN solution. CONDUIT manages the encrypted tunnel fabric while PRISM provides the application intelligence and policy enforcement.

The protocol is fully programmable via gRPC, supports distributed and centralized deployment models, and mandates a phased transition to Commercial National Security Algorithm Suite 2.0 (CNSA 2.0) cryptographic requirements.

Status of This Memo

This Internet-Draft is submitted in full conformance with the provisions of BCP 78 and BCP 79.

Internet-Drafts are working documents of the Internet Engineering Task Force (IETF). Note that other groups may also distribute working documents as Internet-Drafts. The list of current Internet-Drafts is at https://datatracker.ietf.org/drafts/current/.

Internet-Drafts are draft documents valid for a maximum of six months and may be updated, replaced, or obsoleted by other documents at any time. It is inappropriate to use Internet-Drafts as reference material or to cite them other than as "work in progress."

This Internet-Draft will expire on 7 August 2026.

Table of Contents

1. Introduction

1.1. Problem Statement

Software-Defined Wide Area Networks (SD-WAN) have emerged as a critical technology for enterprises and tactical networks requiring Intelligent traffic management across multiple WAN connections. However, existing SD-WAN solutions are predominantly proprietary, creating several challenges:

Vendor Lock-in: Organizations deploying proprietary SD-WAN solutions become dependent on a single vendor for features, updates, and interoperability.

Limited Interoperability: Proprietary solutions cannot interoperate with equipment from other vendors, limiting deployment flexibility and multi-vendor environments.

Opaque Operation: Closed implementations prevent security auditing and verification of traffic handling behavior.

Cryptographic Limitations: Many commercial SD-WAN products do not support government-mandated cryptographic standards such as CNSA 2.0.

An open-standard SD-WAN protocol would address these limitations by providing a vendor-neutral specification that enables interoperability, permits security auditing, and ensures compliance with required cryptographic standards.

SD-WAN functionality comprises two distinct concerns:

1. Tunnel Fabric Management: Creating, monitoring, and maintaining encrypted tunnels across multiple WAN links. [I-D.conduit-tunnel-fabric] addresses this function.

2. Application-Aware Traffic Steering: Identifying applications, tracking flows, enforcing policies, and selecting optimal paths based on application requirements. This function is addressed by PRISM.

1.2. Relationship to CONDUIT

PRISM and [I-D.conduit-tunnel-fabric] together form a complete open-standard SD-WAN solution with clear separation of responsibilities:

CONDUIT Responsibilities:

* IPsec tunnel lifecycle management (creation, deletion, rekeying)

* Tunnel health monitoring (probing, metrics collection)

* Metric publishing to SRv6/IGP

* IKEv2 security association management

PRISM Responsibilities:

* Application identification (deep packet inspection, heuristics)

* Flow tracking and management

* Policy definition and enforcement

* SLA monitoring and alerting

* Traffic class assignment for SRv6 steering

The relationship can be summarized as: PRISM decides WHAT traffic class each flow belongs to; SRv6 decides WHICH path to use based on Flex-Algo; CONDUIT ensures the paths EXIST and reports their quality.

1.3. Design Goals

PRISM is designed to meet the following goals:

Parameter	Requirement
Flow Scale	10 million concurrent flows per node
Application Signatures	5000+ applications recognized
Classification Latency	Less than 100 microseconds
Policy Scale	100,000 policies per node
SLA Measurement Accuracy	Within 1ms for latency metrics
API Coverage	100% functionality via gRPC
Cryptographic Suite	CNSA 2.0 readiness (phased)

Figure 1

1.4. Scope

This document specifies:

* Application identification mechanisms and signature format
* Flow tracking and management procedures
* Policy framework for traffic steering
* SLA definition and enforcement
* Integration with SRv6 for path selection
* Control protocol for distributed operation
* gRPC API for management and analytics

This document does not specify:

* Tunnel management (covered by [I-D.conduit-tunnel-fabric])
* SRv6 data plane operations (covered by [RFC8986])

* Specific application signatures (maintained separately)

* Deep packet inspection algorithms (implementation-specific)

2. Conventions and Terminology

2.1. Requirements Language

The key words "MUST", "MUST NOT", "REQUIRED", "SHALL", "SHALL NOT", "SHOULD", "SHOULD NOT", "RECOMMENDED", "NOT RECOMMENDED", "MAY", and "OPTIONAL" in this document are to be interpreted as described in BCP 14 [RFC2119] [RFC8174] when, and only when, they appear in all capitals, as shown here.

2.2. Definitions

Application: A network service or program identified by its traffic characteristics, such as Microsoft Teams, Salesforce, or SSH.

Application Category: A grouping of applications with similar characteristics or business purposes, such as "unified communications" or "business critical".

Application Signature: A set of patterns or heuristics used to identify a specific application from its network traffic.

Flow: A unidirectional sequence of packets sharing common identifying characteristics, typically a 5-tuple of protocol, source address, source port, destination address, and destination port.

Session: A bidirectional communication comprising two related flows (forward and reverse directions).

Traffic Class: A classification assigned to flows that maps to specific SRv6 treatment, including path selection and QoS.

SLA (Service Level Agreement): A set of performance thresholds that define acceptable service quality for an application or traffic class.

Policy: A rule that matches traffic based on specified conditions and applies designated actions.

DPI (Deep Packet Inspection): Analysis of packet contents beyond layer 4 headers to identify applications.

PRISM Node: A device implementing the PRISM protocol, typically co-located with a CONDUIT node.

PRISM Controller: A centralized management entity that distributes policies and aggregates analytics from PRISM nodes.

3. Architecture

3.1. System Overview

A PRISM deployment consists of the following components:

PRISM Controller: A centralized or distributed management entity responsible for policy management and distribution, application signature database maintenance, aggregated analytics and reporting, and SLA monitoring dashboard.

PRISM Node: A data plane element deployed at network edges responsible for application identification, flow tracking, and classification, policy enforcement, per-flow metrics collection, and SRv6 traffic class assignment.

CONDUIT Node: Co-located tunnel fabric manager providing IPsec tunnel management and path quality metrics (feeds into SLA calculations).

SRv6 Data Plane: Forwarding plane that executes traffic engineering decisions based on traffic class assignments from PRISM.

3.2. Deployment Models

PRISM supports multiple deployment models:

Distributed Mode: Each PRISM node operates independently. Policies

are configured locally on each node. No central controller required. Suitable for small deployments or disconnected operations.

Centralized Mode: PRISM Controller manages all nodes. Policies are defined centrally and distributed to nodes. Centralized analytics and reporting. Suitable for enterprise deployments.

Hierarchical Mode: Regional controllers manage local nodes. Global controller coordinates regional controllers. Policies can be global, regional, or local. Suitable for large distributed deployments.

Hybrid Mode: Central controller for policy distribution. Local autonomy for real-time decisions. Nodes operate independently if the controller is unreachable. Suitable for tactical/resilient deployments.

4. Application Identification

4.1. Identification Methods

PRISM employs multiple methods to identify applications:

Method	Layer	Description
Port-based	L4	Well-known ports (SSH=22)
Protocol Signature	L7	Pattern matching in payload
TLS/SNI Analysis	L7	Server Name Indication
DNS Correlation	L7	Map DNS queries to flows
Certificate Analysis	L7	X.509 certificate fields
Behavioral Heuristics	L3-L7	Traffic patterns/timing
Machine Learning	L3-L7	Trained classifiers
IP Reputation	L3	Known service IP ranges

Figure 2

Classification proceeds through methods in order of reliability until a confident identification is achieved.

4.2. Encrypted Traffic Analysis

For encrypted traffic (TLS/DTLS), PRISM uses metadata analysis without decryption:

TLS Server Name Indication (SNI): The SNI field in the TLS Client Hello message reveals the intended server hostname, making it the primary method for HTTPS application classification.

Note: The effectiveness of SNI-based identification will diminish as Encrypted Client Hello (ECH) [I-D.ietf-tls-esni] is deployed. Implementations SHOULD prioritize heuristic and behavioral analysis methods (Section 4.1) to maintain classification accuracy for ECH-protected flows.

TLS Certificate Analysis: Server certificates contain identifying

information, including Common Name, Subject Alternative Names, Organization, and Issuer.

JA3/JA3S Fingerprinting: TLS handshake characteristics create unique fingerprints for client and server implementations. Note that JA3 hashes use MD5 for identification purposes only; this does not affect CNSA compliance as no cryptographic protection is derived from these hashes.

Encrypted Traffic Behavioral Analysis: Statistical analysis of

packet sizes, timing, and directionality can identify applications without payload inspection.

PRISM MUST NOT perform TLS interception or decryption. All encrypted traffic analysis is performed on metadata and observable traffic characteristics only.

4.3. Application Categories

Applications are organized into categories for policy management:

Category	Description
unified-communications	Voice, video, messaging (Teams, Zoom, Webex)
business-critical	Core business applications (ERP, CRM, custom apps)
cloud-services	SaaS applications (O365, Salesforce, Workday)
infrastructure	Network services (DNS, NTP, SNMP)
security	Security tools (AV updates, SIEM)
file-transfer	File sharing (SharePoint, Box, FTP)
web-browsing	General web traffic
streaming-media	Video/audio streaming (YouTube, Spotify)
remote-access	VPN, RDP, SSH
unknown	Unclassified traffic

Figure 3

5. Flow Management

5.1. Flow Identification

A composite key identifies flows:

Standard 5-Tuple:

* IP Protocol (8 bits)
* Source IP Address (128 bits for IPv6)
* Destination IP Address (128 bits for IPv6)
* Source Port (16 bits)

* Destination Port (16 bits)

Extended Identifiers (optional):

* VLAN ID

* VRF/VPN ID

* Ingress interface

5.2. Flow Lifecycle

Flows progress through the following states:

NEW: First packet observed. Application identification in progress. Default traffic class applied.

CLASSIFYING: Multiple packets observed. Application identification in progress. May transition to ESTABLISHED once classification confidence exceeds threshold.

ESTABLISHED: Application identified with sufficient confidence. Traffic class assigned based on policy. SLA monitoring is active.

CLOSING: Connection termination detected. Preparing to collect final statistics.

CLOSED: Flow terminated. Final statistics recorded. Entry scheduled for removal after reporting.

6. Policy Framework

6.1. Policy Model

PRISM policies follow a match-action model with the following structure:

* Policy ID: Unique identifier

* Name: Human-readable name

* Priority: Evaluation order (lower = higher priority)

* Match: Conditions that select applicable traffic
* Action: Operations to perform on matching traffic
* Schedule: Optional time-based activation

6.2. Match Conditions

Policies can match on:

* Source/destination IP address or prefix
* Port or port range
* Specific application ID or category
* Application risk level
* Protocol (TCP, UDP, etc.)
* DSCP value
* Time of day
* Ingress interface or zone

6.3. Actions

When a policy matches, the following actions may be applied:

Traffic Class Assignment: Set traffic class (maps to SRv6 color), set DSCP value

Path Selection: Prefer specific path characteristics, avoid specific paths, pin to a specific path

SLA Assignment: Apply SLA profile, set violation actions

Bandwidth Management: Rate limit, bandwidth guarantee

Security: Permit, deny, redirect to inspection

6.4. SLA Definitions

Standard SLA Profiles:

Profile	Latency	Jitter	Loss	Use Case
realtime-voice	150ms	30ms	1%	VoIP
realtime-video	200ms	50ms	1%	Video conferencing
interactive	300ms	100ms	2%	Virtual desktop
transactional	500ms	N/A	0.1%	Database, API
best-effort	N/A	N/A	N/A	General browsing

Figure 4

7. SRv6 Integration

7.1. Traffic Class to SRv6 Color Mapping

PRISM assigns traffic classes that map to SRv6 policy colors:

Traffic Class	Color	Flex-Algo	Description
realtime	100	128	Voice, real-time C2
video	200	129	Video conferencing
interactive	300	128	VDI, interactive apps
business	400	default	Business applications
best-effort	0	default	Default treatment

Figure 5

7.2. Dynamic Path Selection

PRISM influences path selection through traffic class assignment, not direct path manipulation. The sequence is:

1. PRISM classifies flow and assigns traffic class

2. Traffic class maps to SRv6 color

3. SRv6 color maps to SR policy

4. SR policy specifies Flex-Algo or explicit path

5. SRv6 data plane forwards accordingly

This maintains clean separation: PRISM determines the application requirements, SRv6 satisfies them.

8. SLA Monitoring and Enforcement

8.1. SLA Metrics

PRISM monitors:

Latency: End-to-end delay. Measured via TCP timestamps or probes.

Jitter: Variation in packet delay. Calculated per [RFC3550].

Packet Loss: Percentage not delivered. Inferred from TCP

retransmissions.

Throughput: Bytes per second over measurement interval.

8.2. Remediation Actions

When SLA violations are detected:

Alert Only: Generate alert, no corrective action.

Reclassify: Move the flow to a different traffic class.

Path Switch: Signal SRv6 to prefer the alternate path.

Escalate: Notify the external system to take action.

9. Control Protocol

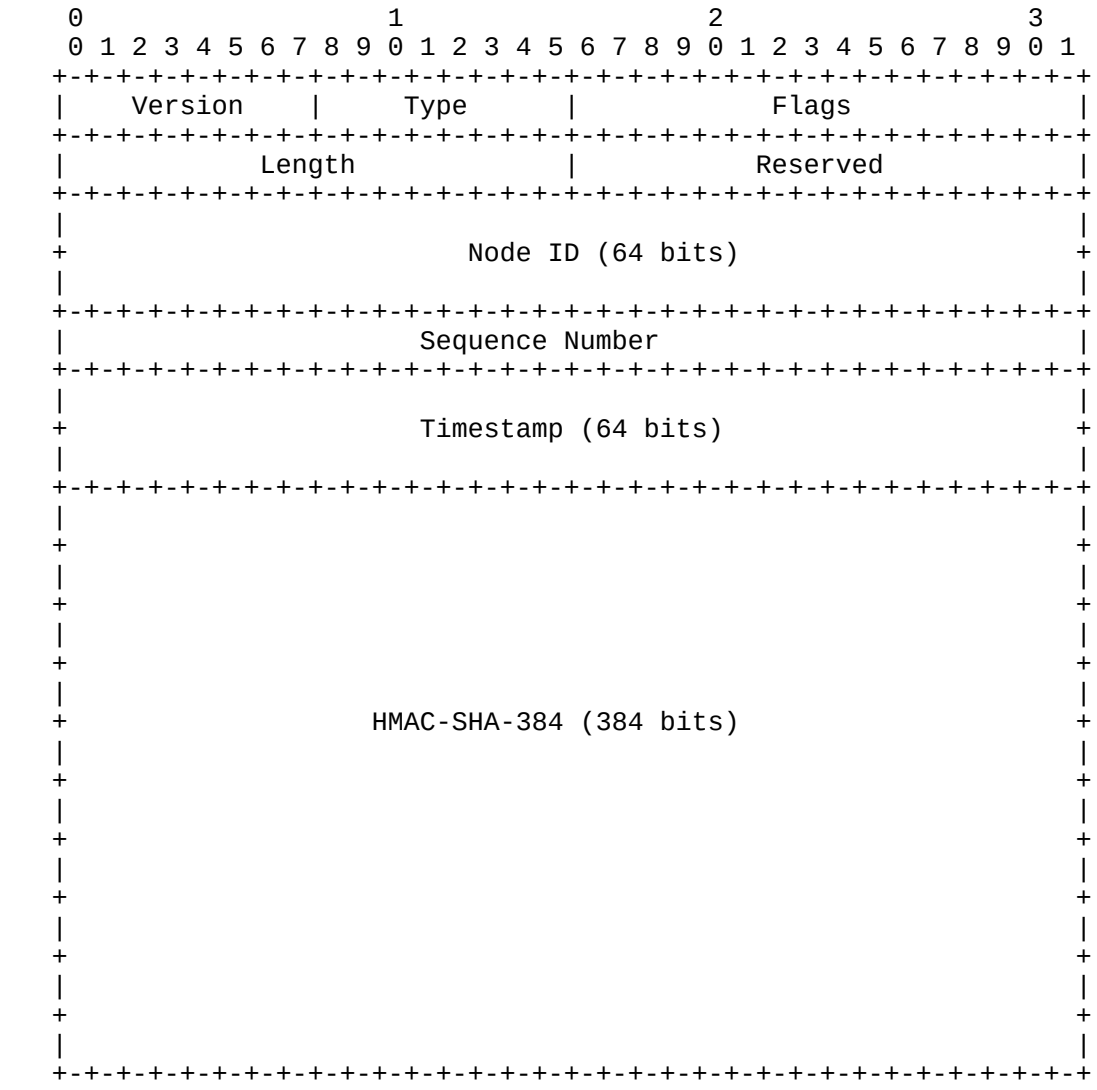
9.1. Transport

PRISM control messages are transported via UDP on port 4796.

PRISM control messages MUST be transported within a CONDUIT encrypted tunnel fabric to ensure confidentiality. Implementations MUST drop PRISM control messages received on unprotected interfaces.

All control messages are authenticated using HMAC-SHA-384.

9.2. Message Header



Total header size: 76 octets
- Version: 8 bits (1 octet)
- Type: 8 bits (1 octet)
- Flags: 16 bits (2 octets)
- Length: 16 bits (2 octets)
- Reserved: 16 bits (2 octets)
- Node ID: 64 bits (8 octets)
- Sequence Number: 32 bits (4 octets)

```
     Timestamp:      64 bits  ( 8 octets)
     HMAC-SHA-384:  384 bits  (48 octets)
```

9.3. Message Types

Value	Name	Description
0x01	HELLO	Node discovery and capability exchange
0x02	HELLO_ACK	Response to HELLO
0x0F	ERROR	Error notification
0x10	POLICY_PUSH	Policy distribution from controller
0x11	POLICY_ACK	Policy receipt acknowledgment
0x20	FLOW_REPORT	Flow statistics report
0x21	FLOW_SYNC	Flow state synchronization (HA)
0x30	SLA_ALERT	SLA violation notification
0x31	SLA_CLEAR	SLA violation cleared
0x40	APP_SIGNATURE	Application signature update

Figure 6

10. gRPC API

PRISM exposes functionality through five gRPC services:

PolicyService: Policy lifecycle management (CRUD for policies, SLA profiles)

ApplicationService: Application signature management

FlowService: Flow visibility and real-time streaming

AnalyticsService: SLA compliance reports and traffic analytics

ConfigService: Node configuration

All gRPC connections MUST use mutual TLS (mTLS). Certificate requirements follow the Phased Transition model defined in Section 11.2. Phase 1 implementations MAY use CNSA 1.0 compliant certificates (ECDSA P-384). Phase 2 implementations SHOULD use hybrid certificates combining ECDSA P-384 and ML-DSA-87. Phase 3 implementations MUST use CNSA 2.0 compliant certificates (ML-DSA-87).

11. Cryptographic Agility and Transition

To ensure long-term security against quantum threats while maintaining operational readiness, PRISM adopts a phased transition strategy aligned with CNSA 2.0 timelines and IETF guidance on Post-Quantum Cryptography [I-D.ietf-pquip-pqc-engineers]. This approach mandates cryptographic agility, enabling seamless updates to algorithms without protocol redesign.

11.1. Cryptographic Agility

PRISM implementations MUST support cryptographic agility. Control plane messages and data plane encapsulations MUST include versioning or algorithm identifiers to allow negotiation of cryptographic suites. Implementations SHOULD be capable of upgrading cryptographic libraries independently of the core protocol logic.

11.2. Phased Transition

The transition to Post-Quantum Cryptography (PQC) is defined in three phases, aligning with the transition models described in [NIST.IR.8547], [ENISA-PQC], and [BSI-PQC], and the timeline mandated by [CNSA2.0]:

Phase 1 (Legacy/Current): Uses CNSA 1.0 algorithms (ECC P-384, AES-256). This phase supports immediate deployment with currently FIPS-validated hardware and software. New deployments SHOULD plan for Phase 2 migration.

Phase 2 (Transitional/Hybrid): Uses hybrid schemes combining CNSA 1.0 and CNSA 2.0 algorithms. Hybrid key exchange (e.g., ECDH P-384 + ML-KEM) and signatures provide "defense in depth" during the transition period. This phase is RECOMMENDED for all systems as PQC libraries become available.

Phase 3 (Target): Uses pure CNSA 2.0 algorithms (ML-KEM, ML-DSA). Mandatory for all new systems by December 31, 2030 (software/firmware and traditional networking equipment) or 2033 (niche equipment), per CNSA 2.0 guidance. The goal is for all NSS to be quantum-resistant by 2035.

11.3. Algorithm Requirements by Phase

Implementations MUST support the algorithms defined for their operating phase:

Algorithm	Phase 1 (Legacy)	Phase 2 (Hybrid)	Phase 3 (Target)
Sym. Enc.	AES-256-GCM	AES-256-GCM	AES-256-GCM
Key Exchange	ECDH P-384	ECDH P-384 + ML-KEM-1024	ML-KEM-1024
Dig. Sig.	ECDSA P-384	ECDSA P-384 + ML-DSA-87	ML-DSA-87
Hashing	SHA-384	SHA-384 / SHA-512	SHA-384 / SHA-512
State Sig. (Firmware)	LMS / XMSS	LMS / XMSS	LMS / XMSS

Figure 7

Note: "ML-KEM" refers to Module-Lattice-Based Key-Encapsulation Mechanism (FIPS 203). "ML-DSA" refers to Module-Lattice-Based Digital Signature Standard (FIPS 204).

11.4. Transport Security

gRPC connections MUST use TLS 1.3. For Phase 1, the TLS_AES_256_GCM_SHA384 cipher suite is REQUIRED. Phase 2 and 3 implementations MUST support PQC-aware TLS cipher suites as they are standardized by the IETF (e.g., [I-D.ietf-tls-hybrid-design], [I-D.ietf-tls-mlkem]). For IPsec compliance (via CONDUIT), implementations MUST support [RFC9370] to enable multiple key exchanges for hybrid PQC.

12. Security Considerations

12.1. Privacy Considerations

PRISM performs deep packet inspection, which raises privacy concerns. PRISM analyzes metadata of encrypted traffic but does not decrypt contents. Organizations SHOULD define data retention policies.

12.2. Application Identification Risks

Sophisticated actors may attempt to evade identification. Implementations SHOULD employ multiple identification methods and provide mechanisms to review classifications.

12.3. Policy Security

Policies MUST be authenticated using HMAC-SHA-384. Policy changes SHOULD require appropriate authorization and be logged for audit.

13. IANA Considerations

13.1. UDP Port Allocation

This document requests the allocation of UDP port 4796 for PRISM control messages.

13.2. Application Category Registry

This document requests the creation of a "PRISM Application Categories." registry with initial values from 0x01 (unified-communications) through 0xFF (unknown).

14. References

14.1. Normative References

[RFC2119] Bradner, S., "Key words for use in RFCs to Indicate Requirement Levels", BCP 14, RFC 2119, DOI 10.17487/RFC2119, March 1997, <https://www.rfc-editor.org/info/rfc2119>.

[RFC3550] Schulzrinne, H., Casner, S., Frederick, R., and V. Jacobson, "RTP: A Transport Protocol for Real-Time Applications", STD 64, RFC 3550, DOI 10.17487/RFC3550, July 2003, <https://www.rfc-editor.org/info/rfc3550>.

[RFC8174] Leiba, B., "Ambiguity of Uppercase vs Lowercase in RFC 2119 Key Words", BCP 14, RFC 8174, DOI 10.17487/RFC8174, May 2017, <https://www.rfc-editor.org/info/rfc8174>.

[RFC8986] Filsfils, C., Ed., Camarillo, P., Ed., Leddy, J., Voyer, D., Matsushima, S., and Z. Li, "Segment Routing over IPv6 (SRv6) Network Programming", RFC 8986, DOI 10.17487/RFC8986, February 2021, <https://www.rfc-editor.org/info/rfc8986>.

[I-D.conduit-tunnel-fabric]
V, J. E. W., "Underlay for IPsec Transport", Work in Progress, Internet-Draft, draft-conduit-tunnel-fabric-00, 30 January 2026, <https://datatracker.ietf.org/doc/html/draft-conduit-tunnel-fabric-00>.

14.2. Informative References

[RFC9460] Schwartz, B., Bishop, M., and E. Nygren, "Service Binding and Parameter Specification via the DNS (SVCB and HTTPS Resource Records)", RFC 9460, DOI 10.17487/RFC9460, November 2023, <https://www.rfc-editor.org/info/rfc9460>.

[NIST.IR.8547]
NIST, "Transition to Post-Quantum Cryptography Standards", November 2024, <https://nvlpubs.nist.gov/nistpubs/ir/2024/NIST.IR.8547.ipd.pdf>.

[ENISA-PQC]
ENISA, "Post-Quantum Cryptography Integration study", October 2022, <https://www.enisa.europa.eu/publications/post-quantum-cryptography-integration-study>.

[BSI-PQC] BSI, "Quantum-safe cryptography fundamentals, current developments and recommendations", 2021, <https://www.bsi.bund.de/SharedDocs/Downloads/EN/BSI/Publications/Brochure/quantum-safe-cryptography.pdf>.

[I-D.ietf-pquip-pqc-engineers]
Banerjee, A., Reddy.K, T., Schoinianakis, D., Hollebeek, T., and M. Ounsworth, "Post-Quantum Cryptography for Engineers", Work in Progress, Internet-Draft, draft-ietf-pquip-pqc-engineers-06, 21 October 2024, <https://datatracker.ietf.org/doc/html/draft-ietf-pquip-pqc-engineers-06>.

[I-D.ietf-tls-hybrid-design]
Stebila, D., Fluhrer, S., and S. Gueron, "Hybrid key exchange in TLS 1.3", Work in Progress, Internet-Draft, draft-ietf-tls-hybrid-design-12, 14 January 2025, <https://datatracker.ietf.org/doc/html/draft-ietf-tls-hybrid-design-12>.

[I-D.ietf-tls-mlkem]
Connolly, D., "ML-KEM Post-Quantum Key Agreement for TLS 1.3", Work in Progress, Internet-Draft, draft-ietf-tls-mlkem-07, 12 February 2026, <https://datatracker.ietf.org/doc/html/draft-ietf-tls-mlkem-07>.

[CNSA2.0] National Security Agency, "Announcing the Commercial National Security Algorithm Suite 2.0", September 2022, <https://media.defense.gov/2022/Sep/07/2003071834/-1/-1/0/CSA_CNSA_2.0_ALGO_FUTURE_QUANTUM_RESISTANT_ALGORITHM_REQUIREMENTS.PDF>.

[I-D.ietf-tls-esni]
Rescorla, E., Oku, K., Sullivan, N., and C. A. Wood, "TLS Encrypted Client Hello", Work in Progress, Internet-Draft, draft-ietf-tls-esni-25, 14 June 2025, <https://datatracker.ietf.org/doc/html/draft-ietf-tls-esni-25>.

[RFC9370] Tjhai, CJ., Tomlinson, M., Bartlett, G., Fluhrer, S., Van Geest, D., Garcia-Morchon, O., and V. Smyslov, "Multiple Key Exchanges in the Internet Key Exchange Protocol Version 2 (IKEv2)", RFC 9370, DOI 10.17487/RFC9370, May 2023, <https://www.rfc-editor.org/info/rfc9370>.

Acknowledgements

The authors thank the networking community for discussions on SD-WAN requirements and open standards approaches.

Authors' Addresses

John Edward Willman V
Department of the Air Force
1800 Air Force Pentagon
Washington, DC 20330
United States of America
Phone: +1 786 994 3023
Email: john.willman.1@us.af.mil
URI: https://www.linkedin.com/in/johnewillmanv

Satoru Kanno
GMO Internet Group, Inc.
Cerulean Tower
26-1 Sakuragaokacho, Tokyo
150-8512
Japan

Email: kanno@gmo-connect.jp
URI: https://www.linkedin.com/in/satoru-kanno/