Mplify Standard

Mplify 174

Product Attributes and Use Cases for Quantum-Safe Services

April 2026

Disclaimer

The information in this publication is freely available for reproduction and use by any recipient and is believed to be accurate as of its publication date. Such information is subject to change without notice and Mplify Alliance (Mplify) is not responsible for any errors. Mplify does not assume responsibility to update or correct any information in this publication. No representation or warranty, expressed or implied, is made by Mplify concerning the completeness, accuracy, or applicability of any information contained herein and no liability of any kind shall be assumed by Mplify as a result of reliance upon such information.

The information contained herein is intended to be used without modification by the recipient or user of this document. Mplify is not responsible or liable for any modifications to this document made by any other party.

The receipt or any use of this document or its contents does not in any way create, by implication or otherwise:

a) any express or implied license or right to or under any patent, copyright, trademark or trade secret rights held or claimed by any Mplify member which are or may be associated with the ideas, techniques, concepts or expressions contained herein; nor
b) any warranty or representation that any Mplify members will announce any product(s) and/or service(s) related thereto, or if such announcements are made, that such announced product(s) and/or service(s) embody any or all of the ideas, technologies, or concepts contained herein; nor
c) any form of relationship between any Mplify member and the recipient or user of this document.

Implementation or use of specific Mplify standards, specifications, or recommendations will be voluntary, and no Member shall be obliged to implement them by virtue of participation in Mplify Alliance. Mplify is a non-profit international organization to enable the development and worldwide adoption of agile, assured and orchestrated network services. Mplify does not, expressly or otherwise, endorse or promote any specific products or services.

Table of Contents

List of Tables

1 List of Contributing Members

The following members of Mplify participated in the development of this document and have requested to be included in this list.

- aconnic
- Arqit
- Capvion
- FiberCop
- MaiaEdge
- RAD
- Sparkle

2 Abstract

Quantum computing introduces new threats that can compromise widely deployed cryptographic mechanisms across telecommunications networks. Service Providers must therefore plan the transition toward quantum-safe architectures while ensuring continuity with existing Mplify service models.

This document defines the **attributes**, **taxonomy**, and **use cases** required to describe, provision, and operate automated **Quantum-Safe Network Services** across Layer 1, Layer 2, Layer 3, and overlay environments.

The work focuses on the **service-level behaviour** of quantum-safe connectivity, including authentication models, key-management modes, crypto-agility, orchestration requirements, and multi-domain considerations, while remaining agnostic to specific cryptographic algorithms or vendor implementations. The document also aligns with global initiatives from NIST, ETSI, ITU and other SDOs to ensure interoperability and coherent migration paths.

This contribution enables automated, scalable, and interoperable quantum-safe services across heterogeneous infrastructures and provides the foundation for future evolution of secure, orchestrated, and post-quantum networking.

3 Terminology and Abbreviations

This section defines the terms used in this document. In many cases, the normative definitions to terms are found in other documents. In these cases, the third column is used to provide the reference that is controlling, in other Mplify or external documents.

Term	Definition	Reference
Automated Key Management (AKM)	A method of managing cryptographic keys where generation, distribution, storage and rotation are performed through a controller or orchestrator that automate the full lifecycle and avoids any manual process.	This document
Crypto-agility	The ability of a system or protocol to switch between different cryptographic schemes or key agreement methods with minimal impact on operations or overall system architecture.	This document
ETSI GS QKD 014 [Interface]	An interface specification developed by ETSI to support interoperability between QKD equipment and key management systems.	ETSI GS QKD 014
ETSI GS QSC 004 [Interface]	An interface developed by ETSI for post-quantum cryptography components, including crypto brokers and orchestrators.	ETSI GS QSC 004
Hybrid Encryption	A cryptographic approach that combines a least one PQC approach with another encryption scheme which may include a traditional non-quantum secure cryptographic method. Examples: i) multiple key encapsulation mechanisms with DH/PQC/PPK - RFC9370 ii) use of PPK from an out of band such as SKO / QKD for the PPK with IKEv2 for quantum secure IPsec – RFC8784 Further clarity on “Post-Quantum/Traditional” hybrid cryptographic terminology may be referenced in RFC9794 authored by the NCSC.	RFC8784 RFC9370 RFC9794
Manual Key Management (MKM)	A method of managing cryptographic keys where distribution, storage and/or change are performed manually, through operational procedures outside of system-based automation. Key provisioning is static (e.g. pre-shared keys) and updated on a scheduled basis with manual key fill.	This document

Term	Definition	Reference
Network Integrated Key Agreement (NIKA)	A key management mode (KMD) in which PKA-based cryptographic session keys are negotiated using key agreement mechanisms implemented within network protocols and controlled by the network.	This document
Key Management	The process of generating, distributing, storing, and revoking cryptographic keys in a secure manner across a network or system.	NIST SP 800-57
Key Management Mode (KMD)	A service attribute to indicate how keys are managed for a given quantum-safe connection for intra-operator or between different operators	This document
Overlay Key Agreement (OKA)	A key management mode (KMD) in which cryptographic session keys are established by an overlay key agreement system, independent of network control, and derived using quantum key distribution (QKD) or post-quantum algorithms (PKA). The resulting keys are securely provisioned to service endpoints for use in data-plane encryption.	This document
Public Key Infrastructure (PKI)	A system of hardware, software, policies, and procedures needed to create, manage, distribute, and revoke digital certificates and public keys.	RFC 5280
Quantum Computing	A paradigm of computing based on the principles of quantum mechanics, using quantum bits (qubits) to process information.	ETSI GR QSC 001
Post-quantum Algorithm (PQA)	NIST has released its first Post-Quantum Cryptography (PQC) standards, which include Post-Quantum Algorithms (PQA) for encryption and digital signatures designed to be resistant to future quantum computers. The three initial standards are: ML-KEM (CRYSTALS-Kyber) for key encapsulation, ML-DSA (CRYSTALS-Dilithium) for general digital signatures, and SLH-DSA (SPHINCS+) for stateless hash-based digital signatures. NIST has also identified other algorithms like FALCON and HQC for future standardization and has a process in place to evaluate and adopt new proposals.	FIPS203/204/205

Term	Definition	Reference
Post-Quantum Cryptography (PQC)	Post-Quantum Cryptography (PQC) primarily refers to new cryptographic algorithms (PQAs) designed to be secure against attacks from both classical and quantum computers. It also covers schemes which are based on symmetric cryptographic primitives and methods such as Pre-Shared Post-Quantum Keys which are already resilient against the same Quantum Threat. For defence in depth, and for implementation agility, PQC can be used with Hybrid Encryption and network protocols which can ingest quantum-secure key material on a purely symmetric basis.	ETSI GS QSC 001
Quantum Key Distribution (QKD)	A method of secure key exchange that uses quantum mechanics principles to detect eavesdropping and guarantee confidentiality of key material.	ETSI GS QKD 014

Term	Definition	Reference
Quantum-Safe Network Service	A network service that integrates mechanisms to protect data in transit against present and future quantum computing threats.	This document
Quantum Threat	The risk posed by sufficiently powerful quantum computers on data encrypted with current Public Key Cryptography (PKC), making data vulnerable in transit, in use and at rest. [PKC methods at risk rely on the difficulty of one of three mathematical problems which are solvable by Shor's algorithm or possible alternatives: the integer factorization problem, the discrete logarithm problem or the elliptic-curve discrete logarithm problem.]	ETSI GR QSC 001
Symmetric Key Orchestration (SKO)	A quantum-safe method for securely establishing and managing symmetric keys at authenticated endpoints without relying on traditional Public Key Cryptography (PKC) or transfer of session keys across the network.	This document
Secure Key Integration Protocol (SKIP)	A solution for managing symmetric key injection and policies between security endpoints and orchestration systems.	IETF draft-cisco-skip-01
Store Now, Decrypt Later (SNDL)	A threat scenario where encrypted data is stored today by an attacker and decrypted in the future once quantum capabilities are available. May also be termed Harvest Now, Decrypt Later (HNDL).	ETSI GR QSC 001
Symmetric Encryption	Encryption using the same key for both encryption and decryption processes, often considered more quantum-resilient than asymmetric alternatives.	NIST SP 800-5

Table 1 – Terminology

Abbreviation	Definition	Reference
AKM	Automated Key Management	
ETSI	European Telecommunications Standards Institute	
EVC	Ethernet Virtual Connection	
e2e	End to end [service]	
IETF	Internet Engineering Task Force	
KMD	Key Management Mode	
KEM	Key Encapsulation Mechanism	
m2m	Machine to Machine	
MKA	MACsec Key Agreement	IEEE 802.1x - 2010
MKM	Manual Key Management	
NIKA	Network Integrated Key Agreement	
OKA	Overlay Key Agreement	
p2p	Point to point [topology]	
p2m	Point to multi-point [topology]	
PKI	Public Key Infrastructure	
PKC	Public Key Cryptography	
PQC	Post-Quantum Cryptography	
QEVC	Quantum-Safe Ethernet Virtual Connection	
QKD	Quantum Key Distribution	
QIPVC	Quantum-Safe IP Virtual Connection	
QOVC	Quantum-Safe Operator Virtual Connection	
QSN	Quantum-Safe Network	
SNDL	Store Now, Decrypt Later	
SKO	Symmetric Key Orchestration	
SKIP	Symmetric Key Integration Protocol	
SP	Service Provider	

Table 2 – Abbreviations

4 Compliance Levels

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 (RFC 2119 [1], RFC 8174 [2]) when, and only when, they appear in all capitals, as shown here. All key words must be in bold text.

Items that are **REQUIRED** (contain the words **MUST** or **MUST NOT**) are labeled as **[Rx]** for required. Items that are **RECOMMENDED** (contain the words **SHOULD** or **SHOULD NOT**) are labeled as **[Dx]** for desirable. Items that are **OPTIONAL** (contain the words **MAY** or **OPTIONAL**) are labeled as **[Ox]** for optional**.**

5 Numerical Prefix Conventions

This document uses the prefix notation to indicate multiplier values as shown in Table 3.

Decimal		Binary	
Symbol	**Value**	**Symbol**	**Value**
k	10^3	Ki	2^{10}
M	10^6	Mi	2^{20}
G	10^9	Gi	2^{30}
T	10^{12}	Ti	2^{40}
P	10^{15}	Pi	2^{50}
E	10^{18}	Ei	2^{60}
Z	10^{21}	Zi	2^{70}
Y	10^{24}	Yi	2^{80}

Table 3 – Numerical Prefix Conventions

6 Introduction

Quantum computing is emerging as a material risk to the cryptographic mechanisms currently used to secure telecommunications networks. Today's widely deployed asymmetric algorithms, such as those used in TLS, IPsec, MACsec control planes, or PKI-based authentication, are expected to become vulnerable to future large-scale quantum attacks. This creates both immediate and long-term challenges: the *Store-Now-Decrypt-Later (SNDL)* threat, the need for crypto-agile infrastructures, and the requirement for service providers to plan a controlled migration path toward post-quantum security.

The purpose of this document is to define a consistent set of **service attributes**, **taxonomy**, and **use cases** for *Quantum-Safe Mplify Network Services*.

The document provides a service-level abstraction that enables Mplify members to describe, provision, automate, and operate quantum-safe services across multiple technologies, vendors, and administrative domains. It focuses on how quantum-safe capabilities are expressed and consumed at the service layer, rather than defining cryptographic algorithms, which remain under the remit of other SDOs such as NIST and ETSI.

This work extends Mplify service models across Layer 1, Layer 2, Layer 3, and overlay constructs, within and between service provider networks, ensuring alignment with existing standards such as MEF 10.4, MEF 51.1, MEF 63, MEF 64, MEF 69.1, and MEF 70.2.

It also considers interoperability with emerging post-quantum interfaces (e.g., ETSI GS QKD 014, ETSI GS QSC 004) and supports heterogeneous key-management paradigms, including Manual Key Management (MKM), Automated Key Management (AKM), Symmetric Key Orchestration (SKO), and QKD-based approaches.

The introduction of Quantum-Safe service attributes supports a range of deployment scenarios, single-provider, multi-provider, and overlay, as well as different technology paths including PQC-only, hybrid classical+PQC, or hybrid PQC+QKD. This ensures that service providers can adopt quantum-safe protections incrementally while maintaining interoperability with legacy environments.

By standardizing terminology, attributes, and classification frameworks, this document provides the foundation for a consistent industry approach to quantum-safe networking. It supports the evolution of operator and enterprise services toward crypto-agile, automated, and quantum-resilient architectures.

7 Product Model vs Service Model

This section clarifies the distinction between the **product perspective** exposed commercially to customers and the **service perspective** that defines the technical behavior and interoperability of Quantum-Safe Network Services within the Mplify framework.

In the context of the Mplify LSO framework, **Products are transacted** in the business systems layer (e.g., via Cantata/Sonata business interactions), while **Services are implemented and orchestrated** in the operations systems layer and below. As a result, information needed to buy/sell a product differs from information needed to configure and operate the service.

7.1 Product Model

From a commercial standpoint, Quantum-Safe capabilities are typically abstracted into simple, high-level attributes that can be exposed in product catalogs, ordering systems, or customer-facing portals.
These attributes enable customers to request a quantum-safe capability without needing to understand the underlying cryptographic mechanisms, key-management models, or orchestration processes.
Therefore, the product model is intentionally minimal and focuses on a small set of agreement points between buyer and seller.

7.1.1 Product Offering concepts

This document uses the following product concepts consistent with Mplify product modeling:

- **Product Specification**: describes a class of items that are sold (here: "Quantum-Safe capability applied to Mplify Network Services").
- **Product Offering**: an externally facing commercial realization derived from a Product Specification, typically constraining the allowed values of Product Attributes and associating commercial terms (e.g., tier, pricing model).
- **Product Offering Configuration**: an identifiable set of Product Attribute values selected/negotiated for a specific purchase instance.

7.1.2 Quantum-Safe Product Offering archetypes

Quantum-Safe capability is typically offered as an add-on or embedded feature within existing connectivity and security products. For clarity of applicability, three generic Product Offering archetypes are identified:

- **PO-A: Quantum-Safe Underlay Connectivity**
  Quantum-safe capability embedded in Layer 1/2/3 connectivity products (e.g., Wavelength/Capacity, Carrier Ethernet, IP Services/Internet Access). PO-A is selected by buyers who require cryptographic protections embedded directly within the transport service itself, with lifecycle and policy enforcement managed by the Service Provider. This model centralizes responsibility for cryptographic posture within the underlay infrastructure and minimizes customer operational complexity. Where the service spans multiple administrative domains, the Service Provider is accountable for coordinating cross-domain profile alignment and lifecycle enforcement consistent with the agreed Product Offering configuration.

- **PO-B: Quantum-Safe Overlay Service**
  Quantum-safe capability delivered via overlay constructs (e.g., SD-WAN overlay models). PO-B enables quantum-safe protection through overlay constructs that may be controlled by the Service Provider, the Customer, or a third-party overlay orchestrator. In this model, cryptographic lifecycle authority may reside outside the transport underlay. Buyers selecting PO-B typically require deployment flexibility or independence from underlay implementation constraints; responsibility boundaries for cryptographic posture and assurance evidence MUST therefore be made explicit in the Product Offering configuration.

- **PO-C: Quantum-Safe End-to-End / Cross-Domain**
  Quantum-safe capability delivered end-to-end across multiple administrative domains, including federated delivery models. PO-C supports end-to-end quantum-safe delivery across multiple administrative domains. This model requires clearly defined orchestration authority, cross-domain cryptographic profile alignment, and agreed assurance evidence exchange between participating providers (e.g., via LSO-based contracts). In federated models, a lead Service Provider may assume responsibility for enforcing consistent lifecycle and cryptographic policy across domains, while partner providers operate domain-level controls and supply the required compliance evidence.

These archetypes are technology-agnostic; detailed realization is defined by the Service Model and the use cases.

7.1.3 Quantum-Safe Product Attributes

While a simple "quantum-safe: yes/no" flag can exist in commercial offers, the working group has identified the need for a **small but expressive** attribute set that enables differentiation (tiers/options) without leaking service mechanisms. This section defines a canonical set of Product Attributes aligned with this document's structure and contributions received.

Product Attribute	Purpose (buyer intent)	Typical applicability
Quantum-Safe Level	Selects the requested quantum-safe posture/tier	PO-A, PO-B, PO-C
Key Lifecycle Profile	Selects the requested lifecycle/rotation posture	PO-A, PO-B, PO-C
Delivery Model	Selects the commercial delivery scope across administrative domains	PO-C (optional for PO-A/PO-B)
Assurance Profile	Selects the requested assurance/reporting posture	PO-A, PO-B, PO-C

Table 4 – Product attributes

The Product Attributes below are defined in a relatively formal way because the goal is to enable automation of business interactions using Mplify LSO APIs (POQ, Quote, Product Order, Product Inventory), while maintaining a clear separation from service realization.

Each Product Attribute value MUST map to a defined service-level realization profile within the Seller's framework. Sellers SHALL ensure that agreed Product Attribute values correspond to consistent service-level behaviors, including key lifecycle enforcement, orchestration authority, and assurance posture—particularly in federated (PO-C) scenarios and when Enhanced assurance is selected.

Quantum-Safe Level Product Attribute

The value of this Product Attribute indicates the requested quantum-safe posture as a buyer-facing tier. It is technology-agnostic and does not mandate a specific cryptographic mechanism.

Name: Quantum-Safe Level

Value: One of:

- **None**
- **Hybrid** (e.g., hybrid transition posture)
- **PQC-only**

Product Offering	**Quantum-Safe Level implication)**
PO-A	Underlay cryptographic posture enforced by the Service Provider.
PO-B	Overlay cryptographic posture enforced by the overlay authority (SP, Customer, or third party).
PO-C	Cross-domain cryptographic profile alignment required across participating administrative domains.

Table 5 – Quantum-Safe Implications for Product Offering

Applicable Use Cases / Product Offering archetypes: PO-A, PO-B, PO-C

Requirements:

- The Quantum-Safe Level Product Attribute **MAY** be exposed as a single yes/no abstraction in catalogs; if so, it **MUST** map deterministically to one of the values above (e.g., yes → Hybrid or PQC-only).
- The Quantum-Safe Level Product Attribute **MUST NOT** mandate a specific technology (e.g., "QKD") at product level; technology choice remains a service-level realization decision.
- If Quantum-Safe Level = None, the Seller **MAY** treat other quantum-safe product attributes as "not applicable" for realization

Key Lifecycle Profile Product Attribute

The value of this Product Attribute indicates the requested lifecycle posture for key rotation and crypto-agility outcomes, without exposing the detailed operational mechanics. It represents a commercial selection of a provider-defined lifecycle profile.

Name: Key Lifecycle Profile

Value: One of:

- **Standard** (provider default lifecycle posture for the selected Quantum-Safe Level)
- **Enhanced** (stronger lifecycle posture, e.g., tighter rotation and/or policy/event-driven rekey as realized at service level to be agreed between seller and buyer)

In federated (PO-C) scenarios, participating providers SHALL ensure that lifecycle enforcement aligns with the agreed Product Offering configuration across domains.

In overlay (PO-B) models, lifecycle enforcement authority MAY reside outside the underlay provider.

Applicable Use Cases / Product Offering archetypes: PO-A, PO-B, PO-C

Requirements:

- If Quantum-Safe Level ≠ None, the Key Lifecycle Profile Product Attribute **SHOULD** be supported to enable tiering (e.g., "Enhanced Key Rotation" as a commercial upgrade).
- The Key Lifecycle Profile Product Attribute **MUST** remain technology-agnostic; detailed cadence, triggers, and operational workflows are service-level behavior.

Delivery Model Product Attribute

The value of this Product Attribute indicates the commercial delivery scope and administrative domain model under which the seller provides the end-to-end quantum-safe capability.

Name: Delivery Model

Value: One of:

- **Single Provider**
- **Federated Multi-Provider**
- **Overlay (Provider-Agnostic)**

Governance and accountability implications: The Delivery Model attribute defines commercial responsibility boundaries.
• In Single Provider scenarios, the provider owns full cryptographic lifecycle authority.
• In Federated Multi-Provider scenarios, authority and assurance obligations must be explicitly coordinated across domains.
• In Overlay scenarios, orchestration authority may reside with the overlay operator or Customer.

Applicable Use Cases / Product Offering archetypes: Mandatory for PO-C; optional for PO-A/PO-B

Requirements:

- For PO-C offerings, the Delivery Model Product Attribute **MUST** be supported because it materially affects commercial responsibility boundaries (end-to-end commitment vs federated delivery vs overlay).
- The Delivery Model Product Attribute **MUST NOT** define service-level orchestration authority details; those are specified by the service model (e.g., lead-provider authority, federation enforcement rules).

Assurance Profile Product Attribute

The value of this Product Attribute indicates the requested assurance/reporting posture visible to the buyer. It selects a provider-defined assurance profile without defining telemetry schemas.

Name: Assurance Profile

Value: One of:

- **Basic**
- **Enhanced** (e.g., extended reporting and compliance-oriented evidence as defined by the provider)

Quantum-safe assurance focus: In a quantum-safe context, assurance is not generic SLA. Enhanced assurance may include cryptographic posture reporting, lifecycle visibility, and (in federated scenarios) cross-domain evidence exchange and attestations.

Product Offering	**Assurance emphasis**
PO-A	Underlay cryptographic posture visibility.
PO-B	Overlay cryptographic status visibility.
PO-C	Cross-domain evidence exchange and attestation.

Table 6 – Assurance for Product offering

Applicable Use Cases / Product Offering archetypes: PO-A, PO-B, PO-C

Requirements:

- If Quantum-Safe Level ≠ None, the Assurance Profile Product Attribute **SHOULD** be supported to enable differentiated assurance and reporting options.
- Assurance Profile **MUST** remain technology-agnostic at product level; specific service assurance/telemetry behaviors remain service-level definition.

7.1.4 Product attribute usage in business interactions

Product Attributes are exchanged and agreed as part of business interactions including Product Offering Qualification (POQ), Quote, Product Order, and Product Inventory. A Product Offering defines constraints on allowed values, and a Product Offering Configuration is the selected set of attribute values. The Seller determines feasibility and may propose close alternatives.

Product Attribute	PO-A	PO-B	PO-C
Quantum-Safe Level	Enforced in underlay	Enforced in overlay	Must align across domains
Key Lifecycle Profile	SP-driven	Overlay-driven	Cross-domain synchronized
Delivery Model	Single-domain	Overlay-controlled	Federated governance
Assurance Profile	SP reporting	Overlay reporting	Cross-domain assurance

Table 7 – Product Attributes for different offers

7.2 Service Model

The primary focus of this document is the **service model**, which describes how a Quantum-Safe Network Service behaves, interacts with other Mplify services, and is orchestrated across single-provider or multi-provider environments.

The service model includes:

- Service-level attributes (e.g., authentication method, encryption type, Key Management Mode)
- Key-management behavior across MKM, AKM, SKO, QKD, NIKA, OKA or hybrid models
- Control-plane and data-plane cryptographic protections
- Topology and layer classification (L1/L2/L3/Overlay)
- Interoperability rules within and between administrative domains
- Automation and LSO integration requirements
- Service assurance and lifecycle considerations

These characteristics define how a quantum-safe connection is established, maintained, and operated across the network, and represent the core technical deliverables of W174.

7.3 Relationship Between the Two Models

The **product model** provides the minimal customer-facing abstraction, whereas the **service model** specifies the complete technical behaviour needed to realize the product.

Product attributes express **customer intent** (e.g., Quantum-Safe Level, Key Lifecycle Profile, Delivery Model, Assurance Profile). Service-level attributes define the **cryptographic realization**, **key management and lifecycle behavior**, **orchestration authority**, and **assurance/telemetry** required to deliver that intent across single-provider, multi-provider, and overlay scenarios.

While a product may expose a single "quantum-safe" attribute, multiple service-level attributes are involved in enabling that capability, such as key-management mode, orchestration behaviour, cryptographic transitions, and node roles.

In summary:

- **Product model:** simple commercial abstraction (buyer intent) via a small number of Product Attributes.
- **Service model:** detailed technical definition of how the quantum-safe capability is delivered, automated, and assured across the network.

This separation ensures ease of consumption for customers while providing the necessary rigor for implementation, interoperability, and automation inside the Mplify ecosystem, and prevents use cases from reverting to product-level shorthand when describing service behavior.

8 Mplify Product and Service applicability

This section identifies the Mplify product areas expected to be impacted by the W174 *Product Attributes and Use Cases for Quantum-Safe Services*.
The objective is to clarify where Mplify W174 quantum-safe service concepts, attributes, and use cases apply within the existing Mplify product taxonomy, and where no direct applicability exists.
Mplify W174 defines a consistent service-level abstraction for quantum-safe network services, including service attributes, key management modes, crypto-agility, orchestration authority, and representative use cases across Layer 1, Layer 2, Layer 3, and overlay service constructs. These concepts apply to selected Mplify product areas as described below.

8.1 Product areas directly addressed by W174 use cases

The following Mplify product areas have a direct mapping to the W174 quantum-safe use case framework and attribute taxonomy.

8.1.1 Carrier Ethernet (Profiles and Use Cases)

W174 applies to Carrier Ethernet services through the definition of Quantum-Safe Ethernet Virtual Connection (QEVC) and Quantum-Safe Operator Virtual Connection (QOVC) use cases. These use cases extend existing Ethernet service constructs with quantum-safe attributes, including key management mode, crypto-agility, and service orchestration considerations. Supported topologies include point-to-point (p2p), multipoint-to-multipoint (m2m), and point-to-multipoint (p2m), where specified.

8.1.2 Wavelength / Capacity (Profiles and Use Cases)

Mplify W174 applies to Layer 1 connectivity through Quantum-Safe Layer 1 Virtual Connection (QL1VC) use cases.
These use cases address quantum-safe service requirements for wavelength or capacity-based services, including p2p and p2m topologies, and define relevant service attributes related to key lifecycle management, crypto-agility, and orchestration authority.

8.1.3 IP Services and Internet Access (Profiles and Use Cases)

Mplify W174 applies to IP-based connectivity through Quantum-Safe IP Virtual Connection (QIPVC) use cases.
QIPVC use cases cover single-provider, multi-provider, and overlay service scenarios, and support p2p, m2m, and p2m topologies. The W174 attribute framework enables consistent specification of quantum-safe properties for IP services, including policy, key management, and lifecycle aspects.

8.1.4 Cloud Connectivity (Profiles and Use Cases)

Mplify W174 includes Cloud Access variants of quantum-safe services, addressing connectivity between customer sites, service provider networks, and cloud service environments.
These variants apply to both Layer 2 and Layer 3 services (e.g., QEVC Cloud Access and QIPVC Cloud Access) and leverage the same quantum-safe attribute framework defined in W174. Detailed Cloud Access use cases are identified as TBD and subject to further refinement.

8.1.5 SD-WAN (Profiles and Use Cases)

Mplify W174 quantum-safe use cases and attributes are applicable to overlay service constructs such as SD-WAN.
In these scenarios, quantum-safe capabilities are applied to overlay connectivity and access services, aligned with existing overlay service framework conventions. W174 does not redefine overlay service models but provides a common attribute and use-case reference for quantum-safe behavior within such services.

8.1.6 Network-as-a-Service (Profiles and Use Cases)

Mplify W174 attributes are applicable to NaaS service constructs where connectivity services are ordered, configured, and assured through standardized APIs and automated lifecycle management.
In this context, W174 supports the specification of quantum-safe service properties in NaaS environments, including orchestration authority, federation, crypto-agility, and service assurance considerations.

8.1.7 Satellite Services (Profiles and Use Cases)

Mplify W174 is applicable to Satellite connectivity services where satellite networks are used to deliver end-to-end connectivity subject to quantum threats.
In these scenarios, W174 applies to the service behaviour and service attributes of the quantum-safe connectivity (e.g., key management mode, crypto-agility, orchestration authority), independent of the underlying transmission medium.
Satellite transport may be used as a standalone domain or as part of hybrid terrestrial–satellite connectivity.
Where applicable, these scenarios align with the W174 use case families for Layer 1, Layer 2, Layer 3, and overlay services.

8.2 Product areas not directly impacted by W174

The following Mplify product areas are not directly impacted by W174, as they do not represent quantum-safe services and do not expose quantum-safe service attributes.

8.2.1 Cross-Connection (XConn)

Cross-Connection Products, as defined in Mplify standards, represent physical connectivity constructs used to interconnect External Interfaces at the infrastructure level.

W174 does not introduce quantum-safe service attributes, use cases, or extensions specific to Cross-Connection Products. Cross-Connections do not provide encryption, key management, or crypto-agility capabilities and therefore are not considered Quantum-Safe Services.
A Cross-Connection may be used as an underlying physical enabler within an end-to-end Quantum-Safe Service defined in W174 (e.g., QL1VC, QEVC, QIPVC), but no W174 attributes or use cases are directly applicable to the Cross-Connection Product itself.

8.2.2 IaaS/Edge Compute

IaaS and Edge Compute products primarily provide compute, storage, and virtualization resources rather than network connectivity services.
Mplify W174 specifies attributes and use cases for Quantum-Safe Network Services (e.g., Layer 1, Layer 2, Layer 3, and overlay connectivity). Therefore, IaaS/Edge Compute products are not directly impacted by W174.
Quantum-safe requirements for accessing or interconnecting IaaS/Edge resources are addressed through the underlying quantum-safe connectivity services defined in this document.

8.2.3 Device Physical & Environmental

Device Physical & Environmental product areas focus on physical infrastructure characteristics (e.g., facilities, power, physical access, environmental conditions) and hardware-related constraints.
These product areas do not expose service-level cryptographic behaviour (e.g., key management mode, crypto-agility, encryption profiles) and are not considered Quantum-Safe Network Services. As such, they are not directly impacted by Mplify W174.

8.2.4 SAI

Service Access Interface (SAI) defines a consolidated set of service attributes for the access interface (UNI) that can be used across multiple frame-based connectivity Service Families (e.g., Subscriber Ethernet, Operator Ethernet, Subscriber IP, SD-WAN, Broadband Access).
Mplify W174 does not define or modify UNI/service-attribute structures for access interfaces. Instead, W174 specifies product attributes and use cases for quantum-safe connectivity services. Therefore, SAI is not directly impacted by W174; any use of SAI to describe access-interface characteristics in the context of quantum-safe services is handled by the applicable service-attribute standards and is outside the scope of this document.

9 Use Case Framework

The Use Case Framework outlines how Mplify-defined network services can evolve to withstand future quantum threats by leveraging post-quantum algorithms (PQA), Quantum Key Distribution (QKD), and crypto agility.
The use cases are organized by the underlying Mplify service type (EVC, OVC, IPVC, L1VC) and by the service topology (Point-to-Point, Multipoint-to-Multipoint, Point-to-Multipoint, and Cloud Access).
Each use case specifies the connection scope (single hop or end-to-end) and whether the service spans one or multiple network providers. Each use case identifies the cryptographic profile(s) applicable to Mplify-defined network services, including the authentication and authorization mechanisms, the type of encryption employed, the Key Management Mode (KMD), the key authority, the key-renewal model, and any replay-protection requirements.

10 Deployment Consideration

The deployment of quantum-safe network services requires attention to architecture, interoperability, and operational management. The following considerations are key for ensuring secure, scalable, and future-proof implementations.

Crypto-Agility. To stay ahead of evolving cryptographic threats and standards, architectures should be designed to support on-demand updates of cryptographic algorithms, hybrid cryptography deployments, and flexible key management modes, helping services remain secure and adaptable without major infrastructure changes.

Hybrid Encryption. Combining post-quantum algorithms (PQA) with classical cryptographic algorithms, or with Quantum Key Distribution (QKD) enables a smooth migration path. Hybrid approaches are particularly important in inter-domain or multi-vendor environments, to simplify interoperability.

QKD Usage. Quantum Key Distribution (QKD) can be deployed in environments where physical infrastructure, security requirements, or regulatory constraints justify its use. QKD deployment should be evaluated against operational complexity, cost, and integration with existing key management frameworks.

Service Orchestration. Key lifecycle management should be integrated with Mplify's LSO APIs and policy controllers. This integration supports automated, scalable management of key generation, distribution, rotation, and revocation across network services.

Network Protocol Interoperability. Quantum-safe mechanisms must be compatible with established protocols such as IPsec, TLS, and MACsec, and ensure seamless interworking across vendors and service provider domains.

Service Interoperability. To achieve a quantum-safe service interoperability across multiple domains and vendors, it is essential to have a common cryptographic profile in place.

11 Use Cases for Quantum-Safe Services

This section provides representative use cases for Quantum-Safe Network Services, consolidating contributions from multiple industry stakeholders. The goal is to describe how Mplify-defined network services can evolve to withstand future quantum threats, leveraging post-quantum cryptography (PQC), crypto-agile key management, and Quantum Key Distribution (QKD).

Each use case includes:

- Current practices in service deployment and encryption
- Proposed quantum-safe enhancements
- Layer and topology classification
- Key exchange, management, and orchestration considerations.

Note (product vs service): In W174, product attributes capture customer intent (e.g., quantum-safe level, delivery model, assurance profile), while the use cases in this chapter describe the **service-level realization** (crypto profile selection, key management mode and authority, lifecycle handling, and assurance/telemetry). Therefore, "quantum-safe" in the use cases refers to service behavior rather than a binary label.

Note:
The use cases described in this document adopt naming conventions that align with existing MEF standards. Specifically, definitions for EPL, EVPL, EPLAN, EVPLAN, EPTREE, and EVPTREE services are consistent with **MEF 6.3 (Subscriber Ethernet Service Definitions)**, **MEF 51.1 (Operator Ethernet Service Definitions)**, and **MEF 64 (Operator Layer 1 Service Attributes and Services)**.
Quantum Safe Overlay services, such as Quantum Safe SD-WAN and Quantum Safe Access to SASE, align with **MEF 70.2 (SD-WAN Service Attributes and Service Framework)**.

11.1 Use Case Taxonomy

Attribute	Options
Authentication	Asymmetric, Symmetric static, Symmetric dynamic
Authorization	Service configuration, Policy based
Service Layer	Layer 1, Layer 2, Layer 3, Overlay
Topology	Point-to-Point, Point-to-Multipoint, Multipoint
Traffic Type	Unicast, Multicast, Broadcast
Directionality	Unidirectional, Bidirectional
Scope	Single-hop, End-to-End
Peers	Intra-provider, Inter-provider
Encryption Type	Symmetric, Asymmetric, Hybrid
Key Distribution	Static, Dynamic, Orchestrated (e.g., SKA, QKD)
Replay Protection	Optional, Mandatory
Key Renewal Period	Time period

Table 8 – Use Case Taxonomy

11.1.1 Use Case Structure (Informative)

To enable consistent comparison across service layers and service families, each use case in Chapter 11 follows a common structure. This structure standardizes the level of detail and does not constrain technology choice or implementation.

Each use case SHOULD include the following sections:

- **Commercial Context / Buyer Value**
- **Overview**
- **Current Practice**
- **Quantum-Safe Implementation**
- **Key Management Mode and administrative authority**
- **Control-plane vs data-plane protection**
- **Assurance and telemetry considerations**
- **Classification summary**

11.1.2 Common Attributes for Use Cases (Informative)

In addition to use-case-specific details, the following common attributes are used throughout Chapter 11 to ensure consistent service-level descriptions.

Classification attributes: Service Layer; Topology; Scope; Peers.
Security behaviour attributes: Authentication; Authorization; Encryption Type; Replay Protection; Key Distribution; Key Renewal Period/Cadence.
Service model attributes (explicit per use case): Key Management Mode (KMD), **Key Orchestration Authority**, **Assurance & Telemetry (minimum set)**.

Each use case in Chapter 11 SHOULD explicitly state Key Management Mode, Key Orchestration Authority, and a minimum Assurance & Telemetry set to preserve service-level behaviour description.

11.2 Quantum-Safe Layer-1 Virtual Connection (QL1VC)

Commercial Context / Buyer Value
This use case supports organizations with long-term confidentiality obligations, where data must remain secure well beyond today's technology lifecycle. Quantum-safe network services reduce the risk that encrypted traffic captured today can be decrypted in the future, helping governments and regulated industries meet long-term security, compliance, and sovereignty requirements.

The commercial value lies in shifting quantum risk mitigation into the network service itself, removing the need for customers to retrofit cryptographic protection later. Buyers procure this service to meet regulatory durability requirements, sovereign security mandates, and internal risk governance objectives without redesigning applications or operational processes.

Overview:
This use case describes a quantum-safe Layer 1 virtual connection for wavelength/capacity services, where confidentiality is primarily achieved through line-rate optical encryption and quantum-safe enhancements focus on crypto-agile key lifecycle orchestration and control/management plane hardening

Current Practice:
Layer-1 services such as EPL are typically secured at the optical layer through hardware-based encryption, most commonly AES-256 in GCM mode. Keys are often provisioned statically or managed via centralized controllers. Confidentiality is reinforced by dedicated wavelengths or fiber paths, but key lifecycle management is limited in flexibility and scalability.

Quantum-Safe Implementation:
QL1VC introduces quantum-safe enhancements to optical connectivity by keeping AES-256 line-rate encryption but replacing static key handling with **crypto-agile orchestration**. Key management can be automated using **Symmetric Key Orchestration (SKO)**, ensuring frequent, dynamic key rotation. For management and control planes, **post-quantum cryptographic algorithms** (e.g., Kyber for key establishment, Dilithium for authentication) are applied. In ultra-sensitive or regulated deployments (e.g., defense, financial networks), **Quantum Key Distribution (QKD)** may be integrated to provide physical-layer key exchange with forward secrecy. The QL1VC therefore enables a future-proofed, interoperable model for secure Layer-1 services that can evolve in line with quantum-resilient standards.

Key Management Mode and administrative authority:
Key management can be manual in legacy deployments or automated through orchestrated key lifecycle mechanisms (e.g., SKO). The key orchestration authority resides with the Service Provider for single-provider services and may be federated to a Lead Service Provider for end-to-end services spanning multiple administrative domains.

Control-plane vs data-plane protection:
Data-plane protection retains line-rate symmetric encryption. Control and management planes are protected using quantum-resilient and crypto-agile mechanisms for authentication and key establishment, consistent with the selected Key Management Mode.

Assurance and telemetry considerations:
Assurance includes visibility into the applied cryptographic profile, key rotation status, and service health indicators relevant to the Layer 1 connection. In multi-domain scenarios, assurance may include evidence/attestations needed to validate compliance with agreed crypto profiles and lifecycle policies.

Classification:

- **Layer:** 1 (optical)
- **Topology:** Point-to-Point
- **Encryption:** AES-256-GCM at line rate, PQC-secured control plane, optional QKD for key delivery
- **Key Management:** Manual (legacy), Automated (crypto-agile, SKO/QKD)
- **Applicable References:** MEF 63, MEF 64

11.3 Quantum-Safe Ethernet Virtual Connection point-to-point (QEVC p2p)

Commercial Context / Buyer Value
This use case applies to enterprises that rely on private, deterministic network connections to support sensitive operational or business-critical activities. Quantum-safe Ethernet services help ensure that data exchanged between sites remains confidential over its full lifecycle, supporting compliance with evolving security regulations while avoiding future network redesigns caused by cryptographic obsolescence.

The value proposition is not stronger encryption per se, but future-proof trust: enterprises avoid future forced migrations caused by cryptographic obsolescence while retaining familiar Ethernet service semantics. Service Providers benefit from offering a differentiated Carrier Ethernet service aligned with emerging compliance expectations.

Overview:
This use case describes a Layer 2 point-to-point Ethernet Virtual Connection delivered as a Mplify E-Line service between two endpoints, and outlines quantum-safe enhancements for onboarding, key lifecycle, and service assurance while retaining symmetric data-plane encryption

Current Practice:
Layer 2 EPL services rely on logical isolation and MACsec for confidentiality and integrity. VLANs are used for segmentation; key management is often static or pre-shared.

Quantum-Safe Implementation:
- Enhance MACsec with post-quantum key agreement (e.g., Kyber-based MKA).
- Secure control plane protocols like 802.1X using PQC digital signatures.
- Crypto-agile L2 switches support seamless cryptographic updates.
- Optional QKD for high-assurance intra-metro EVCs.

Key Management Mode and administrative authority:
Key management behaviour is explicitly defined through the Key Management Mode (manual vs automated and/or orchestrated key lifecycle mechanisms). The key orchestration authority resides with the Service Provider for single-provider services and may be federated to a Lead Service Provider for end-to-end services spanning multiple administrative domains. Where an overlay model is used, orchestration authority may be owned by the customer or a third party providing the overlay security function.

Control-plane vs data-plane protection:
Data-plane protection retains symmetric encryption where MACsec is employed. Control and management planes (including onboarding and policy/orchestration interfaces) are protected using quantum-resilient and crypto-agile mechanisms consistent with the selected Key Management Mode.

Assurance and telemetry considerations:
Assurance includes visibility into the applied cryptographic profile, key rotation/rekey status, and service health indicators relevant to the EVC. In multi-domain scenarios, assurance may

include evidence/attestations needed to validate adherence to the agreed crypto profile and lifecycle policy across domains.

Classification summary:
Layer: 2
Topology: Point-to-Point
Scope: Single-hop or End-to-End (depending on delivery model)
Peers: Intra-provider or Inter-provider (where federated)

11.4 Quantum-Safe Operator Virtual Connection point-to-point (QOVC p2p)

Commercial Context / Buyer Value

This use case addresses multi-operator services where responsibility for security spans multiple service providers. Quantum-safe operator connections enable customers to procure end-to-end services with clear accountability and consistent long-term security posture across provider boundaries, reducing supply-chain risk and simplifying governance for cross-border or regulated deployments.

Quantum-safe QOVC p2p enables lead providers to offer contractual, auditable assurances that cryptographic protections meet defined quantum-resilience and key-lifecycle standards across all participating domains. Buyers select this service to reduce systemic supply-chain risk, satisfy cross-border security requirements, and simplify vendor accountability.

Overview

This use case describes a Layer-2 point-to-point virtual connection delivered by an operator to interconnect two customer endpoints (CE–A ↔ CE–B). The scope covers three delivery models:

1. Single-provider, single-hop L2 service within one SP domain (e.g., MEF E-Line over an access/aggregation network).
2. End-to-end multi-provider L2 service orchestrated by a lead SP across federated SP domains (e.g., inter-AS EVPN-VPWS / MPLS VPWS handoffs).
3. Overlay L2 p2p service where a third party or the customer secures L2 over an underlying transport (e.g., CE-to-CE MACsec across a provider-transparent path or L2 pseudowire).

Current Practice

The prevailing implementation typically relies on one or more of the following:

- MACsec (IEEE 802.1AE) on CE–PE or CE–CE links, using AES-GCM-128/256 with XPN (Extended Packet Numbering) for high-latency/long-haul links. MKA (802.1X/802.1Q) distributes Secure Association Keys; onboarding often uses PKI or PSKs. EAPoL transparency may be required if keys are exchanged end-to-end.
- Provider L2VPNs (MPLS VPWS or EVPN-VPWS) securing only the transport/core with hop-by-hop controls; payload L2 frames are not encrypted unless MACsec is applied at edges.
- Overlay encryption at higher layers (e.g., IPsec) is sometimes used to protect L2 payloads tunneled across the provider; however, that shifts the protection to L3 and may defeat some L2 operational goals (e.g., true L2 transparency).

Operational challenges include manual provisioning, infrequent key rotation, heterogeneous trust across NNI handoffs, and limited telemetry for crypto posture across federated domains. These are analogous to the L3 case you documented, but at L2 the key/EAPoL transparency and MACsec scale (per-port/VLAN) are the most common pain points.

Quantum-Safe Implementation

The control and management plans in p2p services can be enhanced by employing Crypto-agility across control, management, and data planes (ability to rotate algorithms/profiles without service disruption):

- Post-Quantum Cryptography (PQC) for device/endpoint authentication (Use PQC certificates/signatures (e.g., Dilithium) for CE/PE identity, RADIUS/EAP-TLS(-PQC) during 802.1X onboarding, or controller-driven zero-touch provisioning with PQC-backed trust) and key establishment (replace or hybridize classical ECDH with PQC KEM (Kyber) for distributing MKA CAKs/SAKs. For provider-hosted L2VPNs, use PQC in the EVPN/VPWS control plane (e.g., TLS with PQC ciphersuites) and for NNI trust between SPs) modes during transition.
- Automated Symmetric Key Orchestration (SKO) to drive frequent, policy-based rotation of MACsec SAKs (or overlay keys), abstracting key lifecycles from transport specifics.
- Overlay L2 encryption (when used): If a CE-to-CE L2 overlay requires a control handshake (e.g., key controllers), secure that channel with PQC KEM + PQC signatures.

If higher assurance is required, QKD can feed entropy or key material into SKO/MKA. In p2p topologies this is simpler than p2m but still constrained by fiber loss, distance, and trusted-repeater placement. When used, QKD keys are injected to the key-server, which then derives/distributes MACsec SAKs at a configurable cadence.

For the three different delivery models:

Single-Provider, Single-Hop L2 p2p

- **Security**: CE↔PE MACsec with MKA can be upgraded using PQC-enhanced onboarding (802.1X + PQC certs) and SKO-driven SAK rotation (e.g., sub-hour cadences).
- **Replay protection:** MACsec sequence enforcement with XPN (Extended Packet Numbering) strict anti-replay windows.

End-to-End Multi-Provider L2 p2p

- **Security:**
  - PE edge MACsec (per SP policy) can be upgraded with PQC-anchored CAK/SAK distribution.
  - Inter-SP control-plane (BGP EVPN) can be protected via PQC-enabled TLS or IPsec with hybrid IKEv2; SKO federated to enforce rotation SLAs across domains.
- **Federation:** Lead SP orchestrator defines crypto profiles, minimum PQC levels, and rotation cadence; partner SPs attest compliance (evidence/telemetry).

Overlay L2 p2p (Provider-Agnostic)

- **Security:** End-to-end MACsec (or L2-over-L3 with additional encapsulation if required) can be upgraded with PQC-based enrollment and centralized SKO.

Lifecycle and failure considerations: Layer 3 services rely on IPsec/IKE behavior; therefore quantum-safe service definitions SHOULD account for key renewal coordination, negotiation failure handling, and inter-domain interoperability during rekey events. In multi-provider delivery, these lifecycle rules SHOULD be consistently applied across domains to avoid partial or divergent security posture.

Key Management Mode and administrative authority:
Key management behaviour is explicitly defined through the selected Key Management Mode, supporting manual, automated, and orchestrated lifecycle models. In single-provider delivery, the Service Provider acts as the key orchestration authority for the service. In multi-provider end-to-end delivery, a Lead Service Provider may define the end-to-end crypto profile and key lifecycle policy, while partner providers execute local enforcement within their administrative domains under federation rules and agreed assurance obligations. In overlay delivery models, orchestration authority may be owned by the customer or a third party providing the overlay security function. The key authority governs the end-to-end cryptographic profile and key-lifecycle policy for the service. For single-provider delivery, this is the SP; for multi-provider delivery, this is typically the lead SP (SP'), with partner domains operating under agreed federation rules; for overlay delivery, it is the overlay operator.

Control-plane vs data-plane protection:

For Layer 3 services, control-plane protection covers session establishment/negotiation, while data-plane protection covers payload encryption; these MAY rely on different mechanisms, depending on the selected crypto profile and key management mode.
Data-plane protection is provided by symmetric encryption mechanisms appropriate to the Layer 2 service realization (e.g., edge link encryption and/or overlay encryption), while allowing quantum-resilient and crypto-agile onboarding and key establishment. Control and management planes (including service provisioning, orchestration interfaces, and inter-domain coordination across NNIs) are protected using quantum-resilient and crypto-agile mechanisms consistent with the selected Key Management Mode.

Assurance and telemetry considerations:
Assurance includes visibility into the applied cryptographic profile, key rotation/rekey status, replay protection posture, and service health indicators. For multi-provider services, assurance SHOULD include evidence/attestations that partner domains comply with the agreed crypto profile and lifecycle policy, plus telemetry sufficient to support end-to-end SLA reporting for security posture (e.g., algorithm profile in use, last successful rekey timestamp, and compliance flags).

The following table presents a comparison table for Quantum-Safe Operator Virtual Connection point-to-point (QOVC p2p) on Layer 2, covering attributes across Single Provider, Multiple Provider, and Overlay configurations.

Attribute	**Single Provider**	**Multiple Provider**	**Overlay**
Service Layer	L2	L2	L2
Topology	p2p	p2p	p2p
Scope	Single-hop	End-to-end	End-to-end
Peers	Intra-provider	Inter-provider	Provider-agnostic
Data Encryption	MACsec (AES-GCM, XPN)	MACsec at edges; optional core	MACsec CE-to-CE
Replay Protection	Mandatory (MACsec)	Mandatory	Mandatory
Authentication	PQC / PKI / PSK	PQC / PKI / PSK	PQC / PKI / PSK
Key Renewal Cadence	Configurable (e.g., ≤60 min)	Configurable & federated	Configurable (customer-defined)
Key Distribution	SP-hosted SKO / MKA	Lead-SP SKO across domains	Customer/TP SKO
Key Authority	SP	Lead SP (with partner attestations)	TP / Customer
Control-Plane Protection	PQC-TLS to devices	PQC-TLS + inter-SP controls	

Table 9 – QOVC p2p Attributes

11.5 Quantum-Safe IP Virtual Connection point-to-point (QIPVC p2p)

Commercial Context / Buyer Value
This is expected to be one of the earliest and most widely adopted commercial quantum-safe services.

This use case supports enterprises and public institutions that depend on IP connectivity for critical communications and data exchange. Quantum-safe IP services reduce long-term exposure to cryptographic failure by ensuring that encrypted traffic remains confidential over time, allowing organizations to meet regulatory expectations without modifying applications or internal IT architectures.

The commercial driver is risk transfer: customers offload cryptographic evolution, algorithm transitions, and key-lifecycle complexity to the service provider. For regulated industries, this use case supports long-term compliance with financial, healthcare, and government security requirements.

Overview:
Layer 3 point to point vcs may be delivered as diverse service types; we will consider three variations in this use case discussion.

1. A p2p single-hop vc within a single service provider's (SP) network.

2. A p2p e2e service which is delivered to the customer by a lead service provider (SP') and spans two or more service providers' (SP*) networks.

3. A p2p e2e customer service which is delivered by a service provider or third-party as an overlay and may be network provider agnostic.

Note: It is assumed that an intra-provider multi-hop service exhibits similar characteristics to (1) for the purposes of this use case discussion.

Current Practice:
It is proposed that the generalized current practice typically involves the use of IPSec, IKEv2 key derivation based on classic non-quantum-safe algorithms utilizing PKI or PSKs for authentication. Key delivery may be manual (PSK implementations); key rotation cadence may be infrequent and non-automated in the significant majority of cases.

Quantum-Safe Implementation:
As general principle, the control and management planes may be enhanced by employing post-quantum cryptographic algorithms and crypto-agile paradigms, for example adopting Kyber for KEM and Dilithium for digital sig authentication.
An emergent consideration for PQC implementations with typically higher assurance needs, is whether QKD provides additional qualities in the delivery of key material/entropy to complement PQA or hybrid approaches to cryptography. This might offer options for either 'full

QKD' for the entire end to end service, or presence of QKD within the core network to the POP with a complimentary PQC approach for the last mile delivery to the Customer.

Note: subject to further technical advancement optical QKD (fiber / OTA) services are subject to several constraining factors including, i) transmission loss over distance (fiber/OTA) ii) direct line of sight between optical receivers (OTA), iii) the QKD bit rate may not suffice the re-keying rate for high throughput data plane services. Items (i) & (ii) can be absolved with the use of trusted repeaters which will affect the threat model.

The use of QKD requires direct line of sight between optical receivers and may require the use of trusted repeater. All previous points may affect the maximum distance between the end point.

Note: For the purposes of this use-case discussion, it is assumed that the definition of quantum-safe customer facing services will be technology-agnostic. Hence, there is no requirement for specific quantum-safe technologies (e.g. QKD) to be specified within the service definition or by orchestrators during provisioning workflows.
Regardless of the service type, the introduction of automated key management using Symmetric Key Orchestration (SKO) delivers agile, dynamic key rotation and permits a flexible key rotation cadence to be specified by the service provider (i.e. potentially more frequent).
However, depending on the scope and type of service, the overarching key orchestration authority may differ, and cascading orchestration may be required within sub-domains that are owned by multiple SPs' (where the e2e service is delivered by domain artefacts delivered by in-house orchestration and network configuration systems). This may lead to federation, workflow and assurance considerations for the SP' that is accountable for delivering the quantum-safe end-to-end service to the customer.

Key Management Mode and administrative authority:
Key management behavior is explicitly defined through the selected Key Management Mode, supporting manual, automated, and orchestrated lifecycle models. In single-provider delivery, the Service Provider is the key orchestration authority. In multi-provider end-to-end delivery, a Lead Service Provider may define end-to-end crypto profiles and key lifecycle policies, while partner providers enforce domain-level key operations under federation rules. In overlay delivery models, orchestration authority may be owned by the customer, a third party, or the service provider depending on who operates the overlay security function.

Control-plane vs data-plane protection:
Data-plane protection uses symmetric encryption (e.g., IPsec and/or edge link encryption where applicable). Control and management planes (including tunnel establishment, provisioning, policy/orchestration interfaces, and inter-domain coordination) are protected using quantum-resilient and crypto-agile mechanisms consistent with the selected Key Management Mode, enabling quantum-resilient key establishment and rekey operations to be expressed as a service behavior.

Assurance and telemetry considerations:
Assurance includes visibility into tunnel/session health, configured cryptographic profiles, key rotation/rekey status, and compliance with lifecycle policies. In multi-provider services, assurance SHOULD include end-to-end compliance reporting across domains, including

evidence/attestations as required and telemetry that supports security posture SLAs (e.g., profile identifiers, rekey cadence compliance, and per-domain compliance indicators).

Attribute	**Single Provider**	**Multiple Provider**	**Overlay**
Service Layer	Layer 3	Layer 3	Layer 3
Topology	p2p	p2p	p2p
Scope	Single Hop	End-2-End	End-2-End
Peers	Intra-Provider	Inter-provider	Provider-Agnostic
Encryption Type	Symmetric	Symmetric	Symmetric
Replay Protection	Mandatory	Mandatory	Mandatory
Authentication			
Key Renewal Cadence	Configurable	Configurable	Configurable
Key Distribution	SP Static/Orch	SP' Orchestrated	Orchestrated
Key Authority	SP	SP'	TP / SP' / Customer
Authentication	PQC / PKI / PSK	PQC / PKI / PSK	PQC / PKI / PSK

Table 10 – QIPVC p2p Attributes

11.6 Quantum-Safe Ethernet Virtual Connection multipoint (QEVC m2m)

Commercial Context / Buyer Value
This use case is relevant for organizations operating distributed environments where multiple sites exchange sensitive data with each other. Quantum-safe multipoint Ethernet services help reduce the risk that a future cryptographic break compromises large portions of the network, supporting long-term resilience, operational continuity, and regulatory compliance in distributed enterprise and infrastructure environments.

Buyers value centralized, policy-driven key management and crypto-agility at scale, avoiding manual key coordination across numerous sites. This use case is particularly relevant to utilities, transportation operators, and industrial enterprises with distributed operational networks.

Overview:
This use case describes a Layer 2 multipoint Ethernet Virtual Connection (e.g., Mplify E-LAN semantics) enabling any-to-any connectivity among multiple endpoints, and introduces quantum-safe enhancements for scalable key distribution/rotation and multi-site assurance.

Current Practice:
E-LAN and EVPL services provide multipoint connectivity. Security is handled via MACsec, VLANs, ACLs, and segmentation at L2 switching nodes.

Quantum-Safe Implementation:
- Apply MACsec with PQC key exchange at customer and provider edges.
- Use TLS/IPsec with PQC for protocols like LDP and BGP.
- Enable crypto-agile policy enforcement per EVC or VLAN.
- Integrate QKD for symmetric key generation in short-distance secure topologies.

Key Management Mode and administrative authority:
Key management behavior is defined through the Key Management Mode, supporting manual, automated, and orchestrated lifecycle models suitable for multipoint scenarios. The key orchestration authority resides with the Service Provider for single-provider services and may be federated to a Lead Service Provider for multi-provider end-to-end delivery. Where an overlay model is used, orchestration authority may be owned by the customer or a third party.

Control-plane vs data-plane protection:
Data-plane protection retains symmetric encryption where MACsec is employed. Control and management planes (including provisioning/orchestration interfaces and any inter-domain coordination) are protected using quantum-resilient and crypto-agile mechanisms consistent with the selected Key Management Mode.
Assurance and telemetry considerations:
Assurance includes visibility into crypto profile compliance, key rotation/rekey status, and service health. For multipoint services, assurance SHOULD scale across sites/endpoints and include operational visibility and compliance reporting across the multipoint group.

Classification summary:
Layer: 2
Topology: Multipoint
Scope: Single-hop or End-to-End (depending on delivery model)
Peers: Intra-provider or Inter-provider (where federated)

11.7 Quantum-Safe Operator Virtual Connection multipoint (QOVC m2m)

Commercial Context / Buyer Value
This use case applies to complex, federated network services delivered by multiple operators. Quantum-safe multipoint operator services allow customers to obtain consistent long-term security assurances across all participating providers, enabling procurement of multi-domain services without inheriting the weakest-link security risk.

The commercial value lies in assured federation: the lead provider offers measurable guarantees on cryptographic behavior, key rotation cadence, and compliance evidence across all participating operators. This enables procurement of multi-provider services without assuming weakest-link security risk.

Overview
This use case describes a Layer-2 multipoint-to-multipoint (mp2mp) virtual connection where any site can communicate with any other site at L2, aligned with MEF E-LAN semantics or EVPN broadcast domain constructs. The scope covers three delivery models:

- Single-provider, single-hop mp2mp within one SP domain (all sites on the same operator network).
- End-to-end multi-provider mp2mp orchestrated by a lead SP across federated SP domains (inter-AS EVPN/MPLS handoffs).
- Overlay mp2mp delivered by a third party or the customer over provider-agnostic transport (e.g., CE-driven MACsec across a transparent E-LAN).

Current Practice
The prevailing implementation typically relies on one or more of the following:

- MACsec (IEEE 802.1AE) with MKA secures L2 segments on CE–PE or CE–CE links. For mp2mp, operators typically adopt per-port or per-VLAN MACsec policies, using XPN (Extended Packet Numbering) for long-haul/high-speed links. Onboarding is commonly via 802.1X/EAP with PKI or PSKs; if CE-to-CE MACsec spans the provider, EAPoL transparency may be required.
- Provider L2VPNs (e.g., EVPN E-LAN, VPLS) offer any-to-any L2 connectivity. Transport/control planes may be protected within the provider, while payload L2 frames remain unencrypted unless MACsec is enabled at edges.
- Overlay encryption (e.g., IPsec) is sometimes used but shifts protection to L3, which can undermine L2 transparency goals and complicate BUM handling. Manual onboarding and infrequent key rotation are common; at mp2mp scale, key distribution and replay protection are challenging due to many-to-many patterns.

Quantum-Safe Implementation
The control and management plans in mp2mp services can be enhanced by employing:

- Crypto-agility across control, management, and data planes to rotate/upgrade algorithms without downtime.

- Post-Quantum Cryptography (PQC): use Dilithium for signatures (device/endpoint identity) and Kyber for key encapsulation (session establishment). Support hybrid (classical + PQC) during transition.
- Automated Symmetric Key Orchestration (SKO): centralized distribution and frequent rotation of MACsec SAKs (and any overlay keys) via policy-based cadences—critical at mp2mp scale.
- EVPN control-plane security: protect inter-SP and intra-SP EVPN/BGP sessions using PQC-capable TLS/IPsec profiles; enforce profiles on NNIs for federated services.
- Mp2mp with QKD is complex due to distribution topology and key-rate constraints; trusted repeaters or hub-and-spoke relay may be needed. In practice, QKD feeds entropy/key material to SKO, which then implements group or pairwise keying policies suitable for mp2mp. QKD is strictly optional; the service remains technology-agnostic.

For the three different delivery models:

Single-Provider, Single-Hop L2 mp2mp

Data Plane: MACsec on CE–PE links (or CE–CE if provider allows EAPoL transit) with XPN and strict replay windows. For multi-homed CEs, ensure consistent policies across ports.

Control/Management: PQC-protected TLS to devices; SKO orchestrates per-link or group SAKs with staggered rotations to avoid synchronized re-key storms.

End-to-End Multi-Provider L2 mp2mp

Security: Edge MACsec can be upgraded with PQC-assisted MKA; choose pairwise (site↔site) or group SAKs (site↔domain) per policy. Inter-SP control-plane protected via PQC-TLS/IPsec; federated SKO enforces rotation SLAs and validates compliance via telemetry.

Assurance: Lead SP defines crypto profiles (algorithms, parameters, rotation cadence) and requires partner attestations/evidence.

Overlay L2 mp2mp (Provider-Agnostic)

Security: End-to-end MACsec can be upgraded with PQC onboarding and customer-owned SKO; providers guarantee transport SLA only.

Key Management Mode and administrative authority:

Key management behavior is explicitly defined through the selected Key Management Mode, supporting manual, automated, and orchestrated lifecycle models suitable for multipoint-to-multipoint services. In single-provider delivery, the Service Provider is the key orchestration authority. In multi-provider end-to-end delivery, a Lead Service Provider may define the end-to-end crypto profile and key lifecycle policy (including group vs pairwise keying posture), while partner providers enforce domain-level key operations under federation rules. In overlay delivery models, orchestration authority may be owned by the customer or a third party operating the overlay security function.

Control-plane vs data-plane protection:

For Layer 3, control-plane protection covers tunnel/session establishment and negotiation (e.g., IKE), while data-plane protection covers payload encryption; different cryptographic mechanisms MAY be applied per the selected crypto profile and Key Management Mode
Data-plane protection relies on symmetric encryption mechanisms appropriate to the Layer 2 realization (e.g., edge encryption and/or overlay encryption), while supporting quantum-resilient

and crypto-agile onboarding and key establishment. Control and management planes (including provisioning/orchestration interfaces, and intra- and inter-domain control protocols such as EVPN/BGP sessions and NNI coordination) are protected using quantum-resilient and crypto-agile mechanisms consistent with the selected Key Management Mode.

Assurance and telemetry considerations:
Assurance includes visibility into crypto profile compliance, key rotation/rekey status, and service health across the multipoint group. For multi-provider services, assurance SHOULD include per-domain compliance indicators, evidence/attestations where required, and telemetry that supports end-to-end reporting (e.g., group membership/keying policy state, last rekey timestamps per site or per policy unit, and compliance flags across domains).

The following table presents a comparison table for Quantum-Safe Operator Virtual Connection multipoint-to-multipoint (QOVC mp2mp) on Layer 2, covering attributes across Single Provider, Multiple Provider, and Overlay configurations.

Attribute	Single Provider	Multiple Provider	Overlay
Service Layer	L2	L2	L2
Topology	mp2mp (any-to-any)	mp2mp (any-to-any)	mp2mp (any-to-any)
Scope	Single-hop	End-to-end	End-to-end
Peers	Intra-provider	Inter-provider	Provider-agnostic
Data Encryption	MACsec (AES-GCM, XPN)	MACsec at edges; optional in core	MACsec CE-to-CE
Replay Protection	Mandatory	Mandatory	Mandatory
Authentication	PQC / PKI / PSK	PQC / PKI / PSK	PQC / PKI / PSK
Key Renewal Cadence	Configurable (policy-driven)	Configurable & federated	Configurable (customer-defined)
Key Distribution	SP SKO / MKA (pairwise or group)	Lead-SP SKO (federated)	Customer/TP SKO
Key Authority	SP	Lead SP (partner attestations)	TP / Customer
Control-Plane Protection	PQC-TLS to devices	PQC-TLS/IPsec across NNIs	PQC-TLS to CE controllers

Table 11 – QOVC m2m Attributes

11.8 Quantum-Safe IP Virtual Connection multipoint (QIPVC m2m)

Commercial Context / Buyer Value
This use case supports organizations with highly interconnected IP networks, such as global enterprises, research networks, and public agencies. Quantum-safe IP multipoint services help ensure that internal communications remain confidential and trustworthy over time, reducing the need for repeated security redesigns as cryptographic standards evolve.

The buyer value is operational continuity: organizations avoid repeated redesigns of VPN architectures as cryptographic standards evolve, while maintaining scalable multipoint connectivity with predictable security behavior.

Overview:
This use case describes a Layer 3 multipoint IP virtual connection enabling secure connectivity among multiple sites (e.g., any-to-any VPN service models), and addresses quantum-safe behaviors for tunnel establishment, key lifecycle, and compliance reporting at multipoint scale.

Current Practice:
Routing-based VPN services use IPsec tunnels, L3 segmentation, and classical key exchange. Security relies on MPLS isolation and ACLs.

Quantum-Safe Implementation:

- Replace IKE with PQC-based key exchange (e.g., Kyber + Dilithium).
- Adopt ETSI QSVPN models for centralized key orchestration and hybrid crypto.
- Use crypto-agile VPN appliances supporting QRNG and PQC readiness.
- Optional QKD in high-regulatory environments (e.g., financial, national).

Lifecycle and failure considerations: Layer 3 multipoint services rely on coordinated IPsec/IKE lifecycle behavior across multiple tunnels/endpoints. Quantum-safe service behavior SHOULD account for staged/controlled rekey, negotiation failure handling, and inter-domain interoperability so that lifecycle events do not result in partial or inconsistent protection across the multipoint set.

Key Management Mode and administrative authority:
Key management behavior is explicitly defined through the Key Management Mode (manual vs automated and/or orchestrated lifecycle mechanisms). The key orchestration authority resides with the Service Provider for single-provider services and may be federated to a Lead Service Provider for end-to-end multipoint services spanning multiple administrative domains. For QIPVC m2m, the key authority is the administrative domain accountable for the end-to-end crypto profile and key-lifecycle policy across all endpoints. For single-provider delivery this is the SP; for multi-provider end-to-end delivery this is typically the lead SP (SP'), with partner domains operating under federation rules. Where an overlay model is used, orchestration authority may be owned by the customer or a third party providing the overlay security function.

Control-plane vs data-plane protection:
Control and management planes (including orchestration interfaces and any inter-domain coordination) are protected using quantum-resilient and crypto-agile mechanisms consistent with the selected Key Management Mode. Data-plane protection retains symmetric encryption where IPsec is employed, while allowing quantum-resilient key establishment and rekey operations to be expressed as service behavior.

Assurance and telemetry considerations:
Assurance includes visibility into key rotation/rekey status, tunnel/session health, and compliance with configured cryptographic profiles and lifecycle policies. In multipoint services, assurance SHOULD scale across endpoints/sites, providing per-site and per-tunnel (where applicable) operational visibility and compliance reporting.

Classification summary:
Layer: 3
Topology: Multipoint
Scope: Single-hop or End-to-End (depending on delivery model)
Peers: Intra-provider, Inter-provider, or Provider-agnostic (overlay)

11.9 Quantum-Safe Layer 1 Virtual Connection point-to-multipoint (QL1VC p2m)

Commercial Context / Buyer Value
This use case addresses scenarios where a central organization distributes sensitive data to multiple locations over long periods. Quantum-safe Layer-1 distribution services help protect centrally sourced data against future decryption risks, supporting compliance and data-sovereignty requirements in government, financial, and critical infrastructure use cases.

The service is typically procured by government agencies, financial data distributors, and critical infrastructure operators with asymmetric traffic patterns and strict confidentiality mandates.

Overview:
This use case describes a quantum-safe Layer 1 point-to-multipoint virtual connection and the service-level behaviors required to support crypto-agile key lifecycle management and quantum-resilient control/management plane protection, while retaining line-rate symmetric data-plane encryption.

Current Practice:
E-Tree services ensure root-to-leaf connectivity, prohibiting leaf-to-leaf traffic. Security includes optical encryption (L1), MACsec (L2), and IPsec (L3) with static keys.

Quantum-Safe Implementation:

- MACsec or IPsec tunnels enhanced with PQC-based key exchange (MKA or IKEv2).
- PQC-secured control plane using TLS 1.3 for BGP-EVPN, SPB, or LDP.
- Crypto-agile infrastructure supports per-service policies.
- QKD used optionally for centralized key distribution from root to leaf.

Key Management Mode and administrative authority:
Key management behavior is defined through the Key Management Mode (manual vs automated and/or orchestrated lifecycle mechanisms). The key orchestration authority resides with the Service Provider for single-provider services and may be federated to a Lead Service Provider for end-to-end services spanning multiple administrative domains.

Control-plane vs data-plane protection:
Data-plane protection retains symmetric encryption where applied at Layer 1. Control and management planes (including provisioning and orchestration interfaces, and any relevant control protocols used to realize the service) are protected using quantum-resilient and crypto-agile mechanisms consistent with the selected Key Management Mode.

Assurance and telemetry considerations:
Assurance includes visibility into the applied crypto profile, key lifecycle status (e.g., rotation/rekey adherence), and service health. For rooted point-to-multipoint scenarios, assurance SHOULD scale across Leaves and include visibility into policy compliance for rooted multipoint constraints (e.g., Root-to-Leaf behavior).

Classification summary:
Layer: 1
Topology: Point-to-Multipoint
Scope: Single-hop or End-to-End (depending on delivery model)
Peers: Intra-provider or Inter-provider (where federated)

11.10 Quantum-Safe IP Virtual Connection point-to-multipoint (QIPVC p2m)

Commercial Context / Buyer Value
This use case applies to hub-and-spoke network models such as branch connectivity, centralized systems, and distributed service delivery. Quantum-safe IP point-to-multipoint services reduce long-term exposure by ensuring that encrypted communications remain secure across all endpoints throughout their operational lifetime.

Commercially, this enables scalable secure distribution while preserving operational simplicity. Buyers benefit from policy-driven key lifecycle management and future-proof cryptographic assurances without per-site customization.

Overview:
Layer 3 **point-to-multipoint virtual connections** (vcs) may be delivered across a variety of service configurations. This use case considers three primary variations:

1. A p2m single-hop virtual connection within a single service provider's (SP) network, where the central node communicates with multiple endpoints.
2. A p2m e2e service orchestrated by a lead service provider (SP') that spans multiple service providers' (SP*) networks to reach distributed customer endpoints.
3. A p2m overlay service delivered by a third-party or service provider, potentially agnostic to the underlying network infrastructure.

Note: For this use case, intra-provider multi-hop p2m services are assumed to exhibit similar characteristics to (1).

Current Practice:
The prevailing implementation typically relies on **IPSec** with IKEv2 for key exchange, using classical cryptographic algorithms (AES (128/256-bit), SHA-2 for integrity). Authentication is commonly based on PKI or pre-shared keys (PSKs), with manual key provisioning and infrequent rotation cycles, especially in static deployments. In Dynamic multipoint VPN (DMVPN) or SD-WAN architectures, IKEv2 is used to establish individual tunnels between a central hub and multiple spokes and each of them forms a separate IKEv2 Security Association (SA) with the hub. This is not true multicast, but rather multiple unicast tunnels managed efficiently. In the third scenario each endpoint (spoke) establishes a secure tunnel with the central node (hub) and IPsec ensures end-to-end encryption across the overlay, even if it spans multiple networks or providers. In addition, **MACsec** could also be used to secure Layer 3 services encrypting traffic between customer edge (CE) and provider edge (PE) devices. As encryption uses AES-GCM (128 or 256-bit) with XPN (Extended Packet Numbering) for high-speed WAN links and for point-to-multipoint configurations adopts VLAN-level MACsec. It requires transparent forwarding of EAPoL packets (for keys exchange) across SP networks and coordination between SPs to support transparent MACsec forwarding.

Quantum-Safe Implementation:

As a general principle, the control and management plans in p2m services can be enhanced by employing post-quantum cryptographic algorithms and crypto-agile paradigms. For example, Kyber may be adopted for key encapsulation mechanisms (KEM) and Dilithium for digital signature authentication, ensuring quantum resilience across all endpoints in the multipoint topology.

In p2m scenarios, a key challenge is the secure and efficient distribution of cryptographic keys to multiple receivers. Automated key management using Symmetric Key Orchestration (SKO) becomes even more critical, as it enables dynamic, scalable key rotation and group key management. The service provider can specify flexible key rotation cadences, potentially increasing frequency to address the larger attack surface inherent in multipoint connections.

For deployments requiring higher assurance, Quantum Key Distribution (QKD) may be considered to deliver key material or entropy to multiple endpoints. However, QKD in p2m topologies introduces additional complexity, such as the need for trusted repeaters or star/topology-specific key relay mechanisms. Constraints like transmission loss (fiber/OTA), direct line-of-sight requirements, and QKD bit rate limitations become more pronounced as the number of endpoints increases. Trusted repeaters can help mitigate some of these issues but may also impact on the overall threat model and maximum feasible distance between endpoints.

It is important to note that, for the purposes of this use-case discussion, quantum-safe customer-facing services are assumed to be technology-agnostic. There is no requirement for specific quantum-safe technologies (e.g., QKD) to be mandated within the service definition or by orchestrators during provisioning workflows.

Finally, in p2m environments, automated key management via Symmetric Key Orchestration (SKO) enables dynamic, configurable key rotation. The overarching key orchestration authority may differ depending on the service scope. Cascading orchestration may be required within sub-domains managed by multiple service providers (SPs), due to the increased complexity of QKD in multipoint topologies, especially when delivering end-to-end services across federated domains. This necessitates careful consideration of federation, workflow, and assurance processes for the SP accountable for the quantum-safe end-to-end service.

Lifecycle note: In multi-provider p2m delivery, lifecycle rules (rekey coordination, failure handling, and interoperability) SHOULD be explicitly stated to avoid partial protection across spokes during negotiation or rekey events.

Key Management Mode and administrative authority:

Key management behavior is explicitly defined through the selected Key Management Mode, supporting manual, automated, and orchestrated lifecycle models suitable for point-to-multipoint delivery. In single-provider delivery, the Service Provider is the key orchestration authority. In multi-provider end-to-end delivery, a Lead Service Provider may define the end-to-end crypto profile and key lifecycle policy (including hub-and-spoke keying posture and rekey cadence), while partner providers enforce domain-level key operations under federation rules. In overlay delivery models, orchestration authority may be owned by the customer, a third party, or the service provider depending on who operates the overlay security function.

Control-plane vs data-plane protection:

Data-plane protection uses symmetric encryption (e.g., IPsec and/or edge link encryption where applicable). Control and management planes (including hub/spoke tunnel establishment, provisioning, policy/orchestration interfaces, and inter-domain coordination) are protected using quantum-resilient and crypto-agile mechanisms consistent with the selected Key Management

Mode, enabling quantum-resilient key establishment and scalable rekey operations to be expressed as service behavior.

Assurance and telemetry considerations:
Assurance includes visibility into session health, configured cryptographic profiles, key rotation/rekey status, and compliance with lifecycle policies across all spokes/leaves. For multi-provider services, assurance SHOULD include end-to-end compliance reporting and telemetry that scales across endpoints (e.g., per-spoke rekey status, cadence compliance indicators, and per-domain compliance flags).

The following table presents a comparison table for Quantum-Safe IP Virtual Connection point-to-multipoint (QIPVC p2m) on Layer 3, covering attributes across Single Provider, Multiple Provider, and Overlay configurations.

Attribute	**Single Provider**	**Multiple Provider**	**Overlay**
Service Layer	Layer 3	Layer 3	Layer 3
Topology	p2m	p2m	p2m
Scope	Single Hop	End-2-End	End-2-End
Peers	Intra-Provider	Inter-provider	Provider-Agnostic
Encryption Type	Symmetric	Symmetric	Symmetric
Replay Protection	Mandatory	Mandatory	Mandatory
Authentication	PQC / PKI / PSK	PQC / PKI / PSK	PQC / PKI / PSK
Key Renewal Cadence	Configurable	Configurable	Configurable
Key Distribution	SP Static/Orch	SP' Orchestrated	Orchestrated
Key Authority	SP	SP'	TP / SP' / Customer

Table 12 – QIPVC p2m Attributes

11.11 Quantum-Safe Ethernet Virtual Connection point-to-multipoint (QEVC p2m)

Commercial Context / Buyer Value
This use case supports organizations that require controlled, directional data distribution at Layer 2, often in regulated or operational environments. Quantum-safe rooted Ethernet services help maintain confidentiality and compliance over time while preserving strict traffic-flow policies and service behavior.

The value proposition is secure distribution with controlled trust boundaries, enabling compliance with sector-specific requirements (e.g., utilities, transport, public safety) without introducing overlay complexity.

Overview:
This use case describes a Layer 2 rooted point-to-multipoint Ethernet Virtual Connection (aligned with E-Tree semantics), where a Root communicates with multiple Leaves and Leaf-to-Leaf traffic is restricted, and applies quantum-safe service attributes to key lifecycle and orchestration.

Current Practice:
Layer 2 point-to-multipoint connectivity is typically delivered using rooted multipoint Ethernet service constructs (e.g., E-Tree semantics), where a Root endpoint communicates with multiple Leaf endpoints, and Leaf-to-Leaf communication is restricted by the service behavior. Confidentiality and integrity, when required, are commonly implemented via link-layer encryption (e.g., MACsec) on Customer Edge to Provider Edge segments, or through operational controls and traffic isolation mechanisms (e.g., VLAN separation and access policies). Keying is frequently based on classical onboarding and key agreement methods, with manual or limited automation for key rotation, and crypto-agility is not consistently expressed as a service-level characteristic.

Quantum-Safe Implementation:
QEVC p2m applies W174 quantum-safe service attributes to rooted multipoint Layer 2 services. The service retains symmetric data-plane encryption where used, and aligns service establishment and lifecycle with quantum-resilient and crypto-agile objectives. Key management behavior is explicitly defined through the Key Management Mode, including policy-driven key rotation cadence and rekey triggers that scale across multiple Leaf endpoints. Where MACsec is employed, onboarding and control-plane protection can be enhanced using post-quantum or hybrid approaches for authentication and key establishment, while maintaining symmetric encryption for the data plane. Symmetric Key Orchestration (SKO) (or equivalent orchestrated key lifecycle mechanisms) supports scalable distribution and rotation policies suitable for rooted multipoint services (e.g., per-leaf keying or group-oriented keying policies, as applicable), under an explicit orchestration authority. In multi-domain scenarios, federation rules determine how orchestration responsibilities, cryptographic profiles, and lifecycle obligations are enforced across administrative boundaries. QKD may be used as an optional key material source where operationally feasible, without being mandated by the service definition.

Key Management Mode and administrative authority:
Key management behavior is explicitly defined through the selected Key Management Mode,

supporting manual, automated, and orchestrated lifecycle models suitable for rooted point-to-multipoint services. In single-provider delivery, the Service Provider is the key orchestration authority. In multi-domain delivery, a Lead Service Provider may define end-to-end crypto profiles and lifecycle policies, while partner domains enforce domain-level key operations under federation rules. In overlay delivery models, orchestration authority may be owned by the customer or a third party operating the overlay security function.

Control-plane vs data-plane protection:
Data-plane protection retains symmetric encryption where applied for the Layer 2 service realization (e.g., edge link encryption and/or overlay encryption), while supporting quantum-resilient and crypto-agile onboarding and key establishment. Control and management planes (including provisioning/orchestration interfaces and any inter-domain coordination) are protected using quantum-resilient and crypto-agile mechanisms consistent with the selected Key Management Mode.

Assurance and telemetry considerations:
Assurance includes visibility into crypto profile compliance, key rotation/rekey status, and service health across the rooted multipoint set. Assurance SHOULD scale across Leaves and include telemetry sufficient to support security posture reporting (e.g., profile identifiers, last successful rekey timestamps per Leaf or per policy unit, and compliance indicators).

Classification:

- **Layer:** 2
- **Topology:** Point-to-Multipoint (rooted multipoint)
- **Scope:** Single-hop or End-to-End (depending on delivery model)
- **Peers:** Intra-provider or Inter-provider (where federated)
- **Security objective:** Quantum-resilient/hybrid authentication and key establishment; symmetric data-plane encryption where applicable; crypto-agility
- **Key lifecycle:** Policy-driven rotation and rekey triggers; orchestration authority defined; scalable keying across multiple Leaves
- **Notes:** Service behaviour enforces rooted-multipoint constraints (e.g., Leaf-to-Leaf restrictions) independent of the security profile.

11.12 Quantum-Safe Operator Virtual Connection point-to-multipoint (QOVC p2m)

Commercial Context / Buyer Value

This use case addresses federated hub-and-spoke services delivered across multiple service providers. Quantum-safe operator services allow customers to rely on a single accountable provider for long-term security posture, reducing governance complexity while ensuring compliance across all delivery domains.

The commercial driver is accountability: a single lead provider assumes responsibility for cryptographic posture, lifecycle enforcement, and compliance evidence across all domains, simplifying procurement and governance for the customer**.**

Overview

This use case describes a Layer-2 point-to-multipoint (p2m) virtual connection where one root (hub) endpoint communicates with multiple leaf (spoke) endpoints at L2 (e.g., MEF E-Tree service semantics or VLAN-scoped distribution). The scope covers three delivery models:

1. Single-provider, single-hop p2m within one SP domain (hub and all leaves on the same operator network).
2. End-to-end multi-provider p2m orchestrated by a lead SP across federated SP domains to reach distributed leaves.
3. Overlay p2m delivered by a third party or the customer over provider-agnostic transport (e.g., CE-driven MACsec across a transparent p2m L2 service).

Current Practice

The prevailing implementation typically relies on one or more of the following:

- MACsec (802.1AE) with MKA is commonly used to protect L2 traffic on CE–PE or CE–CE adjacencies. For p2m, operators often apply MACsec per access VLAN or per leaf port. XPN is used for long-haul/high-speed links. Onboarding leverages 802.1X/EAP with PKI or PSKs; EAPoL transparency can be required when keys are exchanged end-to-end through the provider cloud.
- Provider L2VPNs (e.g., EVPN E-Tree, MPLS E-Tree, or VLAN-based replication) deliver hub-and-spoke traffic separation (root→leaf allowed; leaf→leaf restricted) but typically secure only the transport/control planes unless MACsec is enabled at edges.
- Overlay encryption at higher layers (IPsec) is sometimes used to protect payloads but shifts protection to L3 and may not preserve pure L2 transparency goals for p2m. Manual provisioning and infrequent key rotation remain common, and scalability challenges grow with the number of leaves (key distribution, replay windows, telemetry).

Quantum-Safe Implementation

The control and management plans in p2m services can be enhanced by employing:

- **Crypto-agility**: Ability to change/upgrade algorithms and rotate keys without service downtime.

- **PQC in control/management planes**: Use Dilithium (signatures) for device identity and Kyber (KEM) for session establishment in onboarding and control channels (CE/PE identities validated with PQC certificates; EAP-TLS(PQC) or controller-assisted ZTP). Hybrid (classical+PQC) is supported during transition. Replacement or hybridization of ECDH with PQC KEM (Kyber) to derive the MKA CAK/SAKs, enabling rapid, frequent rotations across many leaves can add PQC value.
- **Automated Symmetric Key Orchestration (SKO)**: Centralized service that distributes/rotates MACsec SAKs (and any overlay keys) on policy-based schedules; crucial at p2m scale.
- **P2m with QKD** is more complex than p2p: star/distribution models or trusted repeaters may be needed, and limits on distance/bit-rates apply. In practice, QKD feeds key material or entropy into SKO, which then performs scalable group keying (e.g., per-leaf SAKs or group SAKs for root→leaf traffic). QKD remains optional; the service definition stays technology-agnostic.

For the three different delivery models:

Single-Provider, Single-Hop L2 p2m

- **Data Plane: MACsec** at CE–PE (or CE–CE if the provider allows EAPoL transit) can be upgraded with XPN (Extended Packet Numbering) and strict replay windows.
- **Control/Management:** PQC-protected TLS channels between orchestrator/NMS and devices; SKO distributes per-leaf or group SAKs with staggered rotations to avoid bursts.

End-to-End Multi-Provider L2 p2m

- **Security:**
    - Edge **MACsec** can be upgraded with PQC-assisted MKA; per-leaf SAKs or hub-group SAKs as policy dictates.
    - **Inter-SP control-plane** (e.g., EVPN) can be protected via PQC-enabled TLS/IPsec; federated SKO enforces rotation SLAs and policy conformity across domains.

Overlay L2 p2m (Provider-Agnostic)

- **Security: End-to-end MACsec** can be upgraded with PQC onboarding and SKO owned by the customer/TP; providers deliver only transport SLA.

Key Management Mode and administrative authority:

Key management behaviour is explicitly defined through the selected Key Management Mode, supporting manual, automated, and orchestrated lifecycle models suitable for rooted point-to-multipoint services. In single-provider delivery, the Service Provider is the key orchestration authority. In multi-provider end-to-end delivery, a Lead Service Provider may define end-to-end crypto profiles and lifecycle policies (including per-leaf vs group keying posture), while partner providers enforce domain-level key operations under federation rules. In overlay delivery models, orchestration authority may be owned by the customer or a third party operating the overlay security function.

Control-plane vs data-plane protection:
Data-plane protection relies on symmetric encryption mechanisms appropriate to the Layer 2 service realization (e.g., edge link encryption and/or overlay encryption), while supporting quantum-resilient and crypto-agile onboarding and key establishment. Control and management planes (including provisioning/orchestration interfaces, intra- and inter-domain control protocols, and NNI coordination where applicable) are protected using quantum-resilient and crypto-agile mechanisms consistent with the selected Key Management Mode.

Assurance and telemetry considerations:
Assurance includes visibility into crypto profile compliance, key rotation/rekey status, and service health across the rooted multipoint set. For multi-provider services, assurance SHOULD include evidence/attestations where required and telemetry that supports end-to-end security posture reporting (e.g., rekey cadence compliance, per-domain compliance indicators, and per-leaf/group keying state visibility as applicable).

The following table presents a comparison table for Quantum-Safe Operator Virtual Connection point-to-multipoint (QOVC p2m) on Layer 2, covering attributes across Single Provider, Multiple Provider, and Overlay configurations.

Attribute	**Single Provider**	**Multiple Provider**	**Overlay**
Service Layer	L2	L2	L2
Topology	p2m (root→leaves)	p2m (root→leaves)	p2m (root→leaves)
Scope	Single-hop	End-to-end	End-to-end
Peers	Intra-provider	Inter-provider	Provider-agnostic
Data Encryption	MACsec (AES-GCM, XPN)	MACsec at edges; optional in core	MACsec CE-to-CE
Replay Protection	Mandatory	Mandatory	Mandatory
Authentication	PQC / PKI / PSK	PQC / PKI / PSK	PQC / PKI / PSK
Key Renewal Cadence	Configurable (policy-driven)	Configurable & federated	Configurable (customer-defined)
Key Distribution	SP SKO / MKA (per-leaf or group)	Lead-SP SKO (federated)	Customer/TP SKO
Key Authority	SP	Lead SP (with partner attestations)	TP / Customer
Control-Plane Protection	PQC-TLS to devices	PQC-TLS/IPsec across NNIs	PQC-TLS to CE controllers

Table 13 – QOVC p2m Attributes

11.13 Quantum-Safe Ethernet Virtual Connection Cloud Access (QEVC Cloud Access)

Commercial Context / Buyer Value
This use case applies to enterprises connecting private environments to cloud platforms using Layer-2 services. Quantum-safe Cloud Access helps ensure that data exchanged with cloud environments remains confidential over its full lifecycle, supporting regulatory, audit, and data-protection obligations without requiring changes to cloud workloads.

The value lies in aligning cloud connectivity with future regulatory and audit expectations, ensuring that network-level protections evolve without requiring changes to cloud workloads or enterprise security models.

Overview:
This use case describes a Layer 2 Cloud access connectivity service between a customer site and a Cloud on-ramp/exchange port, and defines quantum-safe service behaviors for key management mode, orchestration authority, and multi-domain assurance.

Current Practice:
Layer 2 Cloud connectivity is commonly delivered as an Ethernet service between a Customer site and a Cloud on-ramp or Cloud exchange port. Service separation is typically enforced through VLANs and Layer 2 service delimitation. Confidentiality and integrity may be provided via link-layer encryption (e.g., MACsec) on selected segments, or may rely primarily on service isolation and operational controls. Keying and key rotation are often constrained by operational practices and/or device capabilities, and crypto-agility is not consistently expressed as a service characteristic.

Quantum-Safe Implementation:
QEVC Cloud Access applies quantum-safe service attributes to Layer 2 Cloud connectivity. The service retains symmetric data-plane encryption where used, and aligns service establishment and lifecycle with quantum-resilient and crypto-agile security objectives. Quantum-safe behavior includes policy-driven key lifecycle management (e.g., rotation cadence and rekey triggers), key management mode selection, and explicit orchestration authority for the end-to-end service. Where the service spans multiple administrative domains (e.g., access + exchange + cloud on-ramp), the service definition identifies the orchestration model and responsibilities for key lifecycle and policy enforcement across domain boundaries. The use case remains transmission-medium agnostic and focuses on service-level behavior rather than vendor- or platform-specific mechanisms.

Key Management Mode and administrative authority:
Key management behavior is explicitly defined through the selected Key Management Mode, supporting manual, automated, and orchestrated lifecycle models for Cloud connectivity. The key orchestration authority resides with the Service Provider for single-provider delivery. Where Cloud on-ramp, exchange, and access segments span multiple administrative domains, a Lead Service Provider (or designated orchestration entity) may define end-to-end crypto profiles and

lifecycle policies, while domain providers enforce local key operations under agreed federation rules.

Control-plane vs data-plane protection:
Data-plane protection retains symmetric encryption where applied for the Layer 2 realization. Control and management planes (including provisioning/orchestration interfaces and inter-domain coordination across access/exchange/on-ramp domains) are protected using quantum-resilient and crypto-agile mechanisms consistent with the selected Key Management Mode.

Assurance and telemetry considerations:
Assurance includes visibility into the crypto profile in use, key rotation/rekey status, and service health indicators relevant to Cloud connectivity. In multi-domain delivery, assurance SHOULD include per-domain compliance indicators and telemetry sufficient to support end-to-end reporting (e.g., profile identifiers, last rekey timestamps, and compliance flags across domains).

Classification:

- **Layer:** 2
- **Topology:** Cloud Access
- **Scope:** End-to-End
- **Peers:** Intra-provider or Inter-provider (depending on Cloud on-ramp model)
- **Security objective:** Quantum-resilient key establishment/lifecycle + crypto-agility; symmetric data-plane encryption where applicable
- **Key lifecycle:** Policy-driven rotation and rekey triggers; orchestration authority defined

11.14 Quantum-Safe IP Virtual Connection Cloud Access (QIPVC Cloud Access)

Commercial Context / Buyer Value
This use case supports organizations adopting hybrid and multi-cloud strategies. Quantum-safe IP Cloud Access reduces the risk that encrypted connectivity to cloud platforms becomes insecure over time, enabling enterprises to meet long-term compliance and security requirements while maintaining architectural flexibility.

The commercial benefit is risk mitigation at scale: enterprises avoid future forced migrations of VPN, routing, or security architectures as cryptographic standards evolve.

Overview:
This use case describes a Layer 3 Cloud access connectivity service from customer sites to Cloud environments (e.g., VPN/private connectivity delivery models), and introduces quantum-safe behaviors for key establishment/rekey, crypto-agility, and end-to-end orchestration across domains.

Current Practice:
Layer 3 Cloud connectivity is commonly delivered via IP connectivity services from Customer sites to Cloud environments using IPsec-based VPNs, routed private connectivity, or managed IP VPN services. Key establishment frequently relies on classical IKEv2 key exchange and authentication methods (e.g., PKI- or PSK-based). Key rotation and lifecycle management may be supported, but crypto-agility and quantum-resilient key establishment are not consistently addressed as service characteristics.

Quantum-Safe Implementation:
QIPVC Cloud Access applies quantum-safe service attributes to Layer 3 Cloud connectivity. The service retains symmetric encryption for the data plane while ensuring that key establishment and rekey operations can be quantum-resilient and crypto-agile. This includes support for hybrid approaches that combine a well-established classical key exchange with post-quantum key establishment to provide a migration path while maintaining conservative security posture. Policy-driven key rotation (including rekey cadence and event-driven rekeys) is treated as a service behaviour, coordinated by the defined orchestration authority. For multi-domain delivery models (e.g., Customer access + transit/interconnect + Cloud), the service definition identifies how orchestration and responsibilities for key lifecycle, policy enforcement, and inter-domain coordination are handled end-to-end.
Key Management Mode and administrative authority:
Key management behavior is explicitly defined through the selected Key Management Mode, supporting manual, automated, and orchestrated lifecycle models for Cloud connectivity. The key orchestration authority resides with the Service Provider for single-provider delivery. Where the service spans multiple domains (e.g., customer access + transit/interconnect + Cloud), a Lead Service Provider (or designated orchestration entity) may define end-to-end crypto profiles and lifecycle policies, while domain providers enforce local key operations under agreed federation rules.

Control-plane vs data-plane protection:
Data-plane protection retains symmetric encryption for the service realization (e.g., IPsec/TLS as applicable) while enabling quantum-resilient and crypto-agile key establishment and rekey operations to be expressed as service behavior. Control and management planes (including provisioning/orchestration interfaces and inter-domain coordination) are protected using quantum-resilient and crypto-agile mechanisms consistent with the selected Key Management Mode.

Assurance and telemetry considerations:
Assurance includes visibility into session health, crypto profile compliance, and key rotation/rekey status relevant to Cloud connectivity. In multi-domain delivery, assurance SHOULD include per-domain compliance indicators and telemetry sufficient to support end-to-end reporting (e.g., profile identifiers, rekey cadence compliance, and compliance flags across domains).

Classification:

- **Layer:** 3
- **Topology:** Cloud Access
- **Scope:** End-to-End
- **Peers:** Intra-provider or Inter-provider (depending on delivery model)
- **Security objective:** Quantum-resilient/hybrid key establishment + symmetric data-plane encryption + crypto-agility
- **Key lifecycle:** Policy-driven rotation and rekey triggers; orchestration authority defined
- **Notes:** Hybrid key exchange modes may be used to support transition without weakening security posture

11.15 Quantum-Safe Overlay / SD-WAN

Commercial Context / Buyer Value

This use case is designed for organizations seeking scalable, managed security across diverse network underlays. Quantum-safe overlay services allow enterprises to transfer long-term cryptographic risk to the service provider, ensuring continuous protection as cryptographic standards evolve and reducing the operational burden of managing security changes internally, while customers consume quantum-resilient connectivity as a managed outcome aligned with zero-trust and automation strategies**.**

Overview:
This use case describes a quantum-safe SD-WAN/overlay service where edge devices establish secure tunnels over one or more underlay networks, and focuses on quantum-resilient authentication/key establishment, orchestrated key lifecycle, and fleet-scale assurance.

Current Practice:
SD-WAN services are delivered as overlays where edge devices establish secure tunnels over one or more underlay networks (e.g., Internet, private IP). Security typically relies on IPsec/TLS-based tunnels with controller-driven provisioning and classical authentication and key exchange. Key rotation may be supported, but operational policies and heterogeneous device capabilities can limit consistent key lifecycle management and crypto-agility across the fleet.

Quantum-Safe Implementation:
Quantum-Safe Overlay / SD-WAN applies W174 quantum-safe service attributes to overlay tunnel establishment and lifecycle, aligned with the SD-WAN service framework. The overlay retains symmetric encryption for the data plane while enabling quantum-resilient and crypto-agile authentication and key establishment for tunnel setup and rekey. Orchestrated key lifecycle management becomes a first-class service behaviour: policy-driven rotation cadence, rapid rekey events, and lifecycle enforcement across a large set of SD-WAN edges are coordinated under a defined orchestration authority. Because SD-WAN overlays commonly traverse third-party underlays, the service definition explicitly separates overlay quantum-safe obligations from underlay responsibilities, while still allowing the overlay to incorporate underlay assurances where available.

Key Management Mode and administrative authority:
Key management behavior is explicitly defined through the selected Key Management Mode, supporting automated and orchestrated lifecycle models typical of SD-WAN. The key orchestration authority is typically the SD-WAN orchestrator/controller (operated by the Service Provider or a managed third party), with policy-driven lifecycle enforcement across the SD-WAN edge fleet. Where customers operate their own controller, orchestration authority may reside with the customer.

Control-plane vs data-plane protection:
Data-plane protection retains symmetric encryption for overlay tunnels, while enabling quantum-resilient and crypto-agile authentication and key establishment for tunnel setup and rekey.

Control and management planes (including controller-to-edge communications, provisioning workflows, and API interfaces) are protected using quantum-resilient and crypto-agile mechanisms consistent with the selected Key Management Mode.

Assurance and telemetry considerations:
Assurance includes fleet-scale visibility into crypto profile compliance, key rotation/rekey status, and tunnel health across SD-WAN edges. Assurance SHOULD include telemetry suitable for operational governance (e.g., profile identifiers, last rekey timestamps per edge/tunnel policy, and compliance flags), and may incorporate underlay assurance inputs where available without shifting responsibility for overlay security obligations.

Classification:

- **Layer:** Overlay
- **Topology:** Typically multipoint; may include p2p variants
- **Scope:** End-to-End (overlay endpoints)
- **Peers:** Underlay-provider agnostic (overlay over third-party underlays)
- **Security objective:** Quantum-resilient/hybrid key establishment + symmetric data-plane encryption + crypto-agility
- **Key lifecycle:** Controller/orchestrator-driven, policy-based, fleet-scale

11.16 Satellite (Quantum-Safe Satellite Connectivity)

Commercial Context / Buyer Value

This use case applies to organizations that depend on satellite connectivity for remote access, resilience, or mobility. Quantum-safe satellite services help ensure that sensitive data transmitted over satellite links remains confidential over time, supporting long-term security and compliance requirements even in operationally constrained environments.

The commercial value lies in extending quantum-safe assurances to the most operationally challenging domains, demonstrating end-to-end security consistency across terrestrial and non-terrestrial networks.

Overview:
This use case describes quantum-safe connectivity services traversing satellite transport domains (often realized as overlays), and defines quantum-safe behaviors for key lifecycle orchestration and assurance adapted to satellite constraints such as long RTT and intermittent connectivity.

Current Practice:
Satellite connectivity is used for access and backhaul in remote, mobile, and resilience-driven scenarios. Security is commonly implemented at higher layers (e.g., IPsec/TLS overlays) or via selected link-layer mechanisms, with classical key exchange and operationally constrained key rotation. Satellite operational characteristics (e.g., long RTT, intermittent connectivity, bandwidth constraints, terminal limitations) can lead to conservative key lifecycle practices and limited crypto-agility.

Quantum-Safe Implementation:
Satellite connectivity scenarios are addressed by applying W174 quantum-safe service attributes to services that traverse satellite transport domains. The service retains symmetric encryption for the data plane while enabling quantum-resilient and crypto-agile authentication and key establishment, including support for hybrid migration approaches where needed. Policy-driven key lifecycle management is adapted to satellite constraints (e.g., scheduled rotation windows, resilient rekey handling under intermittent connectivity, and operational safeguards). The service definition identifies the orchestration authority and key lifecycle responsibilities across satellite access, gateways, and any terrestrial segments, including inter-provider coordination where multiple operators contribute to end-to-end delivery.

Key Management Mode and administrative authority:
Key management behavior is explicitly defined through the selected Key Management Mode, supporting manual, automated, and orchestrated lifecycle models adapted to satellite operational constraints. The key orchestration authority resides with the Service Provider for single-provider delivery. Where the service spans satellite access, gateways, and terrestrial segments across multiple operators, a Lead Service Provider may define end-to-end crypto profiles and lifecycle policies, while partner providers enforce local key operations under federation rules.

Control-plane vs data-plane protection:
Data-plane protection retains symmetric encryption for the service realization while enabling quantum-resilient and crypto-agile authentication and key establishment. Control and management planes (including provisioning/orchestration interfaces and inter-operator coordination where applicable) are protected using quantum-resilient and crypto-agile mechanisms consistent with the selected Key Management Mode, accounting for satellite latency and intermittency constraints.

Assurance and telemetry considerations:
Assurance includes visibility into crypto profile compliance, key rotation/rekey status, and service health indicators relevant to satellite delivery. Assurance SHOULD support operationally adapted reporting (e.g., scheduled rekey windows, last successful rekey timestamp, and compliance flags), and in multi-operator scenarios include per-domain compliance indicators sufficient to support end-to-end security posture reporting.

Classification:

- **Layer:** Commonly Layer 3 (overlay/IPsec); may support Layer 2 constructs depending on service realization
- **Topology:** p2p and multipoint (e.g., hub-and-spoke)
- **Scope:** End-to-End
- **Peers:** Intra-provider or Inter-provider (common in satellite ecosystems)
- **Security objective:** Quantum-resilient/hybrid key establishment + symmetric data-plane encryption + crypto-agility
- **Key lifecycle:** Policy-driven and operationally adapted; orchestration authority defined

11.17 Representative Use Case Summary

Use Case	Mplify Product	Layer	Topology	Current Encryption	Current Key Management	Quantum-Safe Cryptography	Key Management Mode
QL1VC	Wavelength / Capacity	L1	Point-to-Point	Optical (minimum AES-256-GCM)	Manual, Automted	PQC SKO, QKD, hybrid mode	Manual, Automated, OKA
QEVC p2p	Carrier Ethernet	L2	Point-to-Point	MACsec (minimum AES-256-GCM)	Manual, Automated	PQC SKO, QKD, hybrid mode	Manual, Automated, NIKA, OKA
QOVC p2p	Carrier Ethernet	L2	Point-to-Point	MACsec (minimum AES-256-GCM)	Manual, Automated	PQC SKO, QKD, hybrid mode	Manual, Automated, NIKA, OKA
QIPVC p2p	IP Services / Internet Access	L3	Point-to-Point	IPsec, MACsec	Manual, Automated	PQA, PQC SKO, QKD, hybrid mode	Manual, Automated, NIKA, OKA
QEVC m2m	Carrier Ethernet	L2	Multipoint	MACsec (minimum AES-256-GCM)	Manual, Automated	PQC SKO, QKD, hybrid mode	Manual, Automated, NIKA, OKA
QOVC m2m	Carrier Ethernet	L2	Multipoint	MACsec (minimum AES-256-GCM)	Manual, Automated	PQC SKO, QKD, hybrid mode	Manual, Automated, NIKA, OKA
QIPVC m2m	IP Services / Internet Access	L3	Multipoint	IPsec, MACsec	Manual, Autometed	PQA, PQC SKO, QKD, hybrid mode	Manual, Automated, NIKA, OKA
QL1VC p2m	Wavelength / Capacity	L1	Point-to-Multipoint	Optical (minimum AES-256-GCM)	Manual, Automted	PQC SKO, QKD, hybrid mode	Manual, Automated, OKA
QIPVC p2m	IP Services / Internet Access	L3	Point-to-Multipoint	IPsec, MACsec	Manual, Autometed	PQA, PQC SKO, QKD, hybrid mode	Manual, Automated, NIKA, OKA
EVC (Rooted-Multipoint) OVC (Rooted-Multipoint) QEVC p2m	Carrier Ethernet	L2	Point-to-Multipoint	MACsec (minimum AES-256-GCM)	Manual, Automated	PQC SKO, QKD, hybrid mode	Manual, Automated, NIKA, OKA
QOVC p2m	Carrier Ethernet	L2	Point-to-Multipoint	MACsec (minimum AES-256-GCM)	Manual, Automated	PQC SKO, QKD, hybrid mode	Manual, Automated, NIKA, OKA
QEVC Cloud Access)	Cloud Connectivity	L2	Cloud Access	MACsec (minimum AES-256-GCM)	Manual, Automated	PQC SKO, QKD, hybrid mode	Manual, Automated, NIKA, OKA
QIPVC Cloud Access	Cloud Connectivity	L3	Cloud Access	IPsec, TLS	Manual, Autometed	PQA, PQC SKO, QKD, hybrid mode	Manual, Automated, NIKA, OKA
Quantum Safe Overlay / SD-WAN	SD-WAN	L3	Multipoint	IPsec, TLS	Manual, Automated	PQA, PQC SKO, QKD, hybrid mode	Manual, Automated

							, NIKA, OKA
Satellite	Satellite	L1-L3	Point-to-Point, Multipoint	IPsec, TLS, MACsec	Manual, Automated	PQA, PQC SKO, QKD, hybrid mode	Manual, Automated , NIKA, OKA

Table 14 – Representative Use Case Summary

12 SDO Dependencies

The evolution toward quantum-safe networking introduces significant challenges and opportunities for Mplify services and Lifecycle Service Orchestration (LSO) frameworks. All proposed solutions in this document are going to be developed in collaboration with relevant standardization bodies to ensure:

- **Interoperability:** Mplify service definitions remain compatible with evolving IEEE MACsec specifications.
- **Forward Compatibility:** Solutions anticipate future quantum-safe cryptographic requirements.
- **Global Harmonization:** Avoid conflicting specifications across industry standards.

This implies that Mplify must proactively engage with global and regional standardization bodies like NIST, ETSI, ITU, TM Forum, IEEE, CEN-CENELEC, ISO/IEC, NQI, NMI-Q to establish service assurance in a quantum-enabled ecosystem.

As today specs developments:

ETSI (European Telecommunications Standards Institute) – TC QT (Technical Committee Quantum Technologies) is mainly focused on Quantum communications and networking, including Quantum Key Distribution (QKD), post-quantum cryptography, and integration with classical telecom systems through the EuroQCI (European Quantum Communication Infrastructure) initiative and development of specifications for secure quantum-enhanced communication infrastructure and interoperability across sectors.

CEN-CENELEC – JTC 22" Quantum Technologies and Focus Group on Quantum Technologies (FGQT) is focused on European standardization for quantum technologies, including quantum communication and cryptography, coordinating with ETSI and ISO/IEC JTC (Joint Technical Committee) 1 to align European connectivity standards with global frameworks and delivering use cases for quantum networking and secure communications.

IEEE Standards Association has defined protocols and architectures for quantum networking and hybrid quantum-classical systems through **IEEE P1913 (**Software-Defined Quantum Communication (SDQC) protocol for dynamic configuration of quantum endpoints in networks), and **IEEE P1943** (Post-Quantum Network Security standards).

ISO/IEC JTC 1 – WG 14 (Quantum Information Technology) has developed Global standards for quantum computing and communication, including interoperability frameworks for quantum networking.

National Quantum Coordination Bodies such as U.S. **National Quantum Initiative (NQI)** and its Advisory Committee **(NQIAC)** are focused on quantum networking strategies and international cooperation.

NMI-Q (National Metrology Institutes Quantum Initiative) focused on measurement standards and interoperability for quantum communication and networking technologies, through global metrology standards.

NIST (National Institute of Standards and Technology) leads U.S. efforts on post-quantum cryptography and contributes to global quantum standards readiness coordinating with ANSI (American National Standards Institute) and industry consortia like QED-C (Quantum Economic Development Consortium).

12.1 Impacts of these standardization activities on Mplify Quantum Safe initiative

- **ETSI**'s work on Quantum Key Distribution (QKD) and secure communication protocols directly influences encryption models for Mplify services. Mplify EVC-based services (E-LINE, E-LAN, E-TREE) rely on deterministic QoS and service classification, which must remain intact when quantum-safe encryption is introduced. ETSI standards will guide how QKD integrates with LSO APIs and service orchestration frameworks, ensuring secure key exchange without disrupting existing operational models.
- **CEN-CENELEC** offers Mplify the opportunity to align service definitions and operational models with EU regulatory and interoperability requirements. Hybrid cryptographic transitions—where classical and quantum-safe algorithms coexist—must be supported in Mplify's LSO architecture to maintain backward compatibility while meeting European security mandates.
- **IEEE**'s work on MACsec (802.1AE) and 802.1X authentication is critical for Mplify services. Current MACsec implementations encrypt VLAN tags, which conflict with Mplify's need for VLAN visibility for EVC classification and QoS enforcement. IEEE initiatives like SDQC (Software-Defined Quantum Communication) and post-quantum security standards will shape how Mplify adapts MACsec for quantum-safe environments—potentially requiring modified frame formats and enhanced key agreement protocols.
- **ISO/IEC** provides global interoperability frameworks for quantum communication systems. Mplify must ensure its service definitions and LSO APIs align with these reference architectures to support cross-domain quantum networking. This alignment is essential for global carriers implementing Mplify services over quantum-secure links, ensuring consistent service behavior across regions.
- **The U.S. National Quantum Initiative** influences domestic carrier Ethernet compliance and security policies. Mplify services deployed in U.S. networks must adhere to NQI guidelines for quantum-safe cryptography and secure networking. This includes ensuring that Mplify orchestration frameworks can integrate with national quantum networking strategies without compromising interoperability.
- Metrology standards from **NMI-Q** support performance validation and SLA assurance for quantum-safe links. Mplify's service assurance models will need to incorporate quantum-specific metrics (e.g., QKD key generation rates, quantum channel integrity) to maintain accurate SLA reporting and compliance in hybrid networks.

Standardization Body	Key Standards / Initiatives	Impact on Mplify
ETSI (TC QT)	Quantum communications & networking; Quantum Key Distribution (QKD); EuroQCI initiative	Shapes encryption models for Mplify services; Guides QKD integration with LSO APIs; Ensures secure key exchange without disrupting operations
CEN-CENELEC (JTC 22, FGQT)	European quantum technology standards; Quantum Communication Use Cases; Coordination with ETSI and ISO/IEC	Aligns Mplify with EU regulatory/interoperability requirements; Supports hybrid cryptographic transitions; Ensures backward compatibility
IEEE Standards Association	MACsec (802.1AE), 802.1X; IEEE P1913 (SDQC); IEEE P1943 (Post-Quantum Network Security)	Impacts MACsec and VLAN visibility for Mplify EVC classification; Shapes adaptation of MACsec for quantum-safe environments; May require modified frame formats
ISO/IEC JTC 1 – WG 14	Global quantum computing & communication standards; Quantum Communication Reference Architecture	Provides interoperability frameworks for quantum networking; Ensures Mplify service definitions and APIs align globally; Supports cross-domain quantum networking
NQI (U.S. National Quantum Initiative)	National Quantum Networking Strategy; Policy and standards alignment	Influences U.S. carrier Ethernet compliance: Ensures Mplify orchestration aligns with national quantum security policies
NMI-Q (National Metrology Institutes Quantum Initiative)	Global metrology standards for quantum links; Performance validation metrics	Supports SLA assurance and performance validation for quantum-secure Mplify services; Incorporates quantum-specific metrics

Table 15 – Impacts of different SDOs' activities on Mplify Quantum Safe initiative

Coordination with international standards bodies is essential to maintain consistency and avoid fragmentation through Mplify Quantum Standards Task Force to coordinate engagement with ETSI, IEEE, ISO/IEC, and regional bodies to Initiate joint working groups with IEEE for MACsec adaptation and ETSI for QKD integration and publish Mplify Quantum Interoperability Guidelines to support carriers and service providers during the transition.

13 References

[1] IETF RFC 2119, *Key words for use in RFCs to Indicate Requirement Levels*, by Scott Bradner, March 1997

[2] IETF RFC 8174, *Ambiguity of Uppercase vs Lowercase in RFC 2119 Key Words*, by B Leiba, May 2017, Copyright © 2017 IETF Trust and the persons identified as the document authors. All rights reserved.

[3] MEF 10.4, *Subscriber Ethernet Service Attributes,* Mplify, December 2018

Appendix A Acknowledgements (Informative)

The following contributors participated in the development of this document and have requested to be included in this list.

- Sander **BARENS**
- Sergio **COZZOLINO**
- Tim **CROY**
- Isabella **MELLI**
- Abilash **MENON**
- Alex **PATERSON**
- Ettore **PULIERI**
- Stefan **REICHMUTH**
- Sharon **ROZOV**
- Antonella **SANGUINETI**