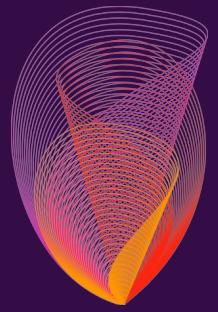


lyntia

NETWORK TO BUSINESS

# Quantum Key Distribution @ ESNOG-33

Luxquanta, Juniper & lyntia

**Índice**

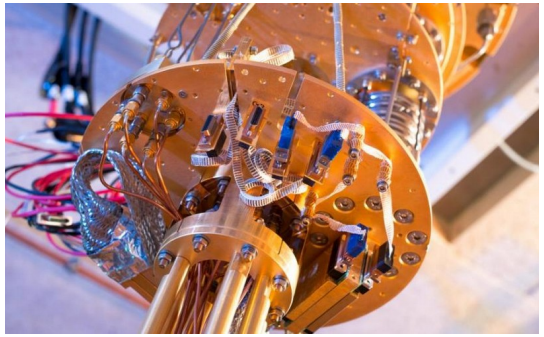


## Índice



# La amenaza de la computación cuántica

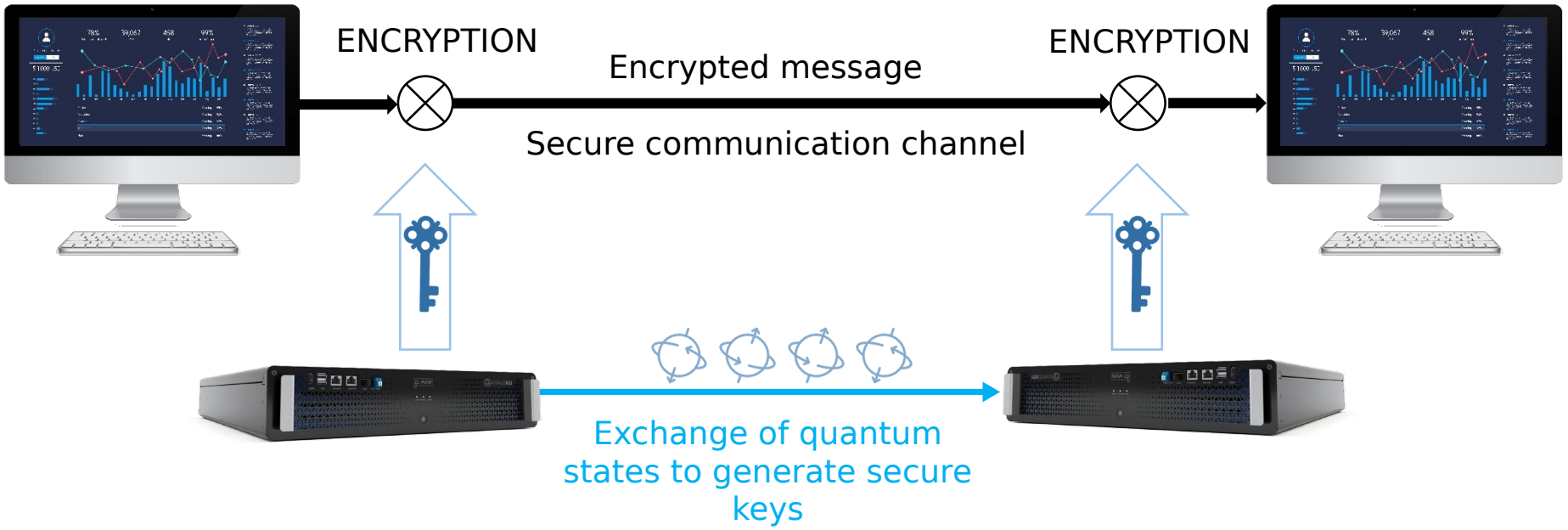
- Las computadoras cuánticas serán capaces de descifrar la criptografía actual.
- Algoritmos quedarán obsoletos:
  - RSA (firmas digitales)
  - ECDH (acuerdo de claves)
  - DSA (acuerdo de claves)
- La estrategia de “Harvest Now – Decrypt later” es una amenaza para nuestros datos hoy.



# Quantum Key Distribution

La distribución de claves cuánticas (QKD) aprovecha las propiedades de la mecánica cuántica para distribuir claves entre ubicaciones remotas que pueden utilizarse para el cifrado. La QKD puede proporcionar protección de datos a largo plazo y con garantía de futuro, incluso contra ordenadores cuánticos.

# Quantum Key Distribution




- QKD crea una clave criptográfica mediante el intercambio de estados cuánticos entre dos ubicaciones a través de un canal cuántico.
- Este canal protege el intercambio de claves mediante el principio de la mecánica cuántica, lo que imposibilita la escucha.
- Las claves se utilizan para cifrar los datos, lo que garantiza su confidencialidad a través de canales clásicos no seguros.

| NOVA LQ® IN ACTION

# Field-proven technology trusted by public and private stakeholders across Europe and beyond

**10+**
COUNTRIES
Deployed from EU to NA

**3**
VERTICALS
Telcos
Data Centers
Governments

TRUSTED
Proven in real-world, production-grade environments

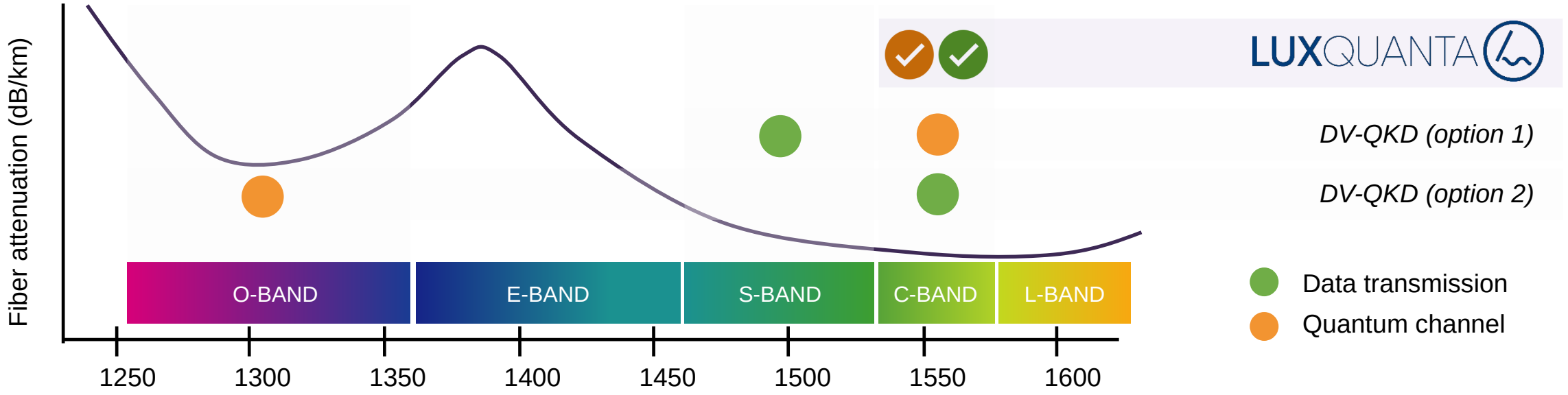
INTEROPERABLE
Integrated with top industry vendors

European Commission
ENDORSED BY EUROPE
Selected supplier for Europe's secure quantum network EuroQCI

# CV-QKD coexiste con los datos en banda C

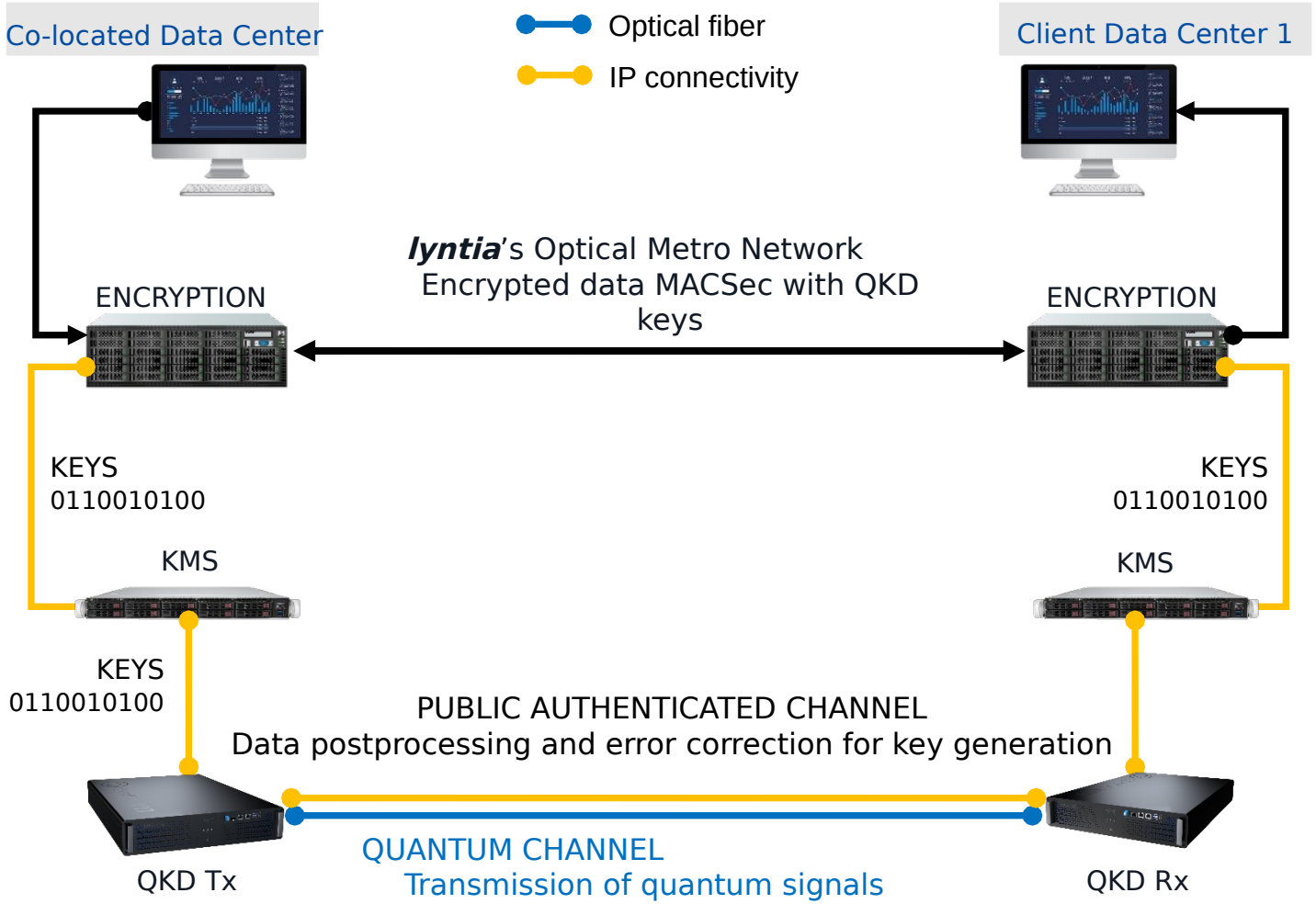
**Fiber attenuation and spectral coexistence of the quantum channel**

*LuxQuanta vs. other DV-QKD approaches*



# Diagrama de conectividad

## Descripción General de la Arquitectura




***Juniper Networks**' utiliza las claves generadas por el sistema QKD para proteger la red óptica metropolitana de Lyntia.*

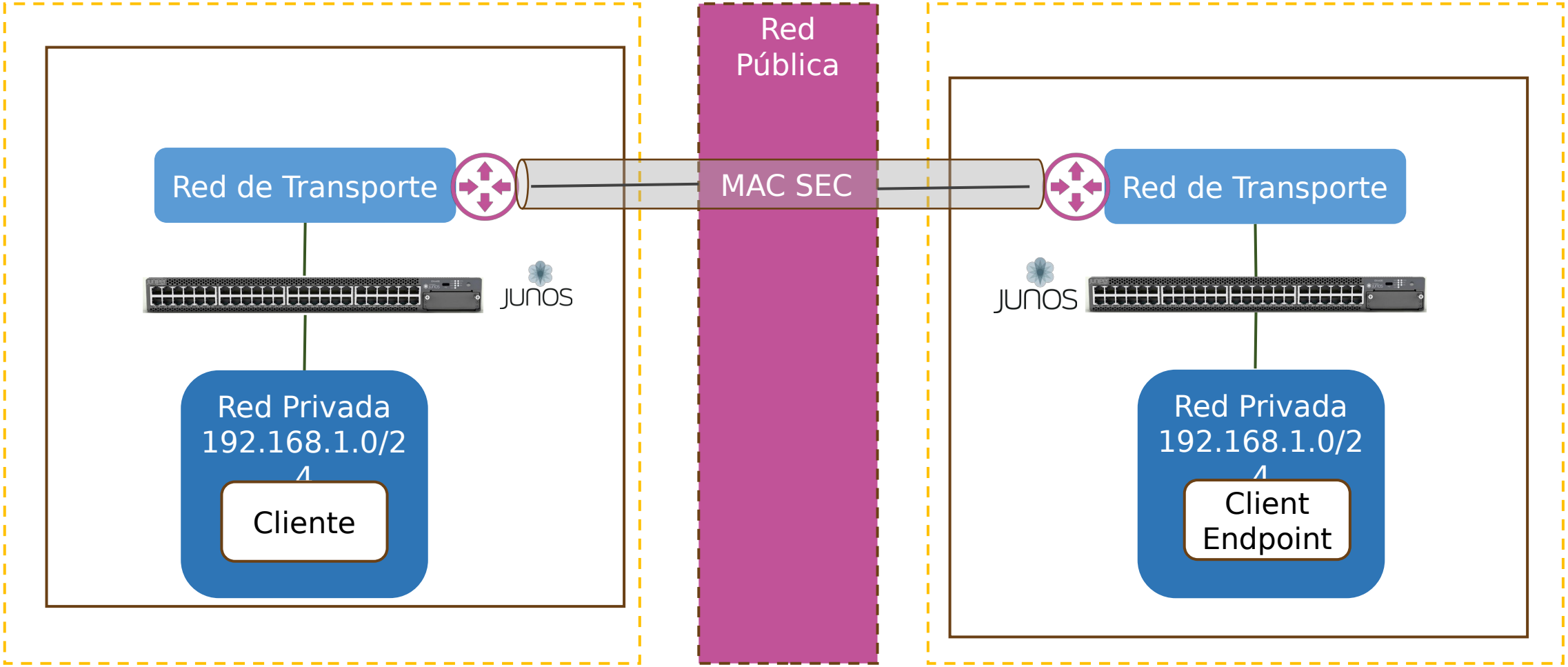
***Merqury Cybersecurity** KMS (Key Management System) es un sistema intermediario que administra, almacena y distribuye claves QKD a los dispositivos que las consumen. Permite:*

***LuxQuanta NOVA LQ** CV-QKD crea una clave criptográfica mediante el intercambio de estados cuánticos entre dos ubicaciones a través de un canal cuántico.*

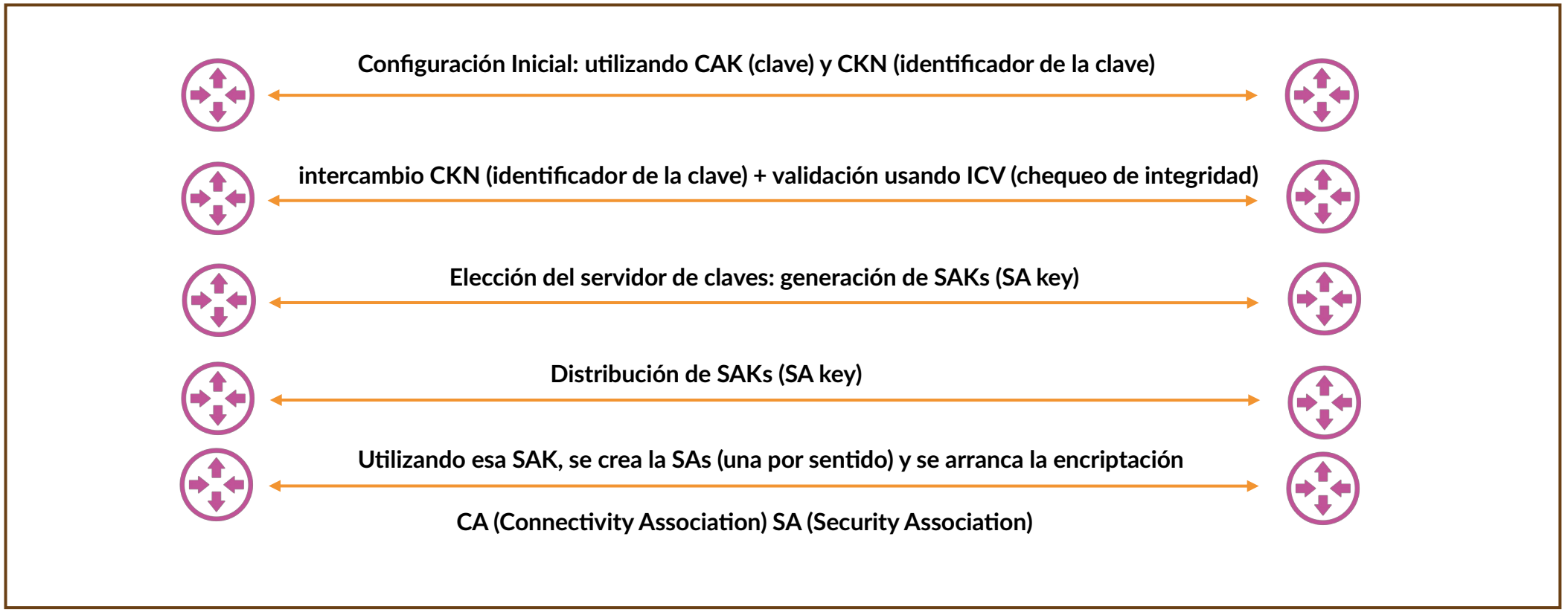
## Índice



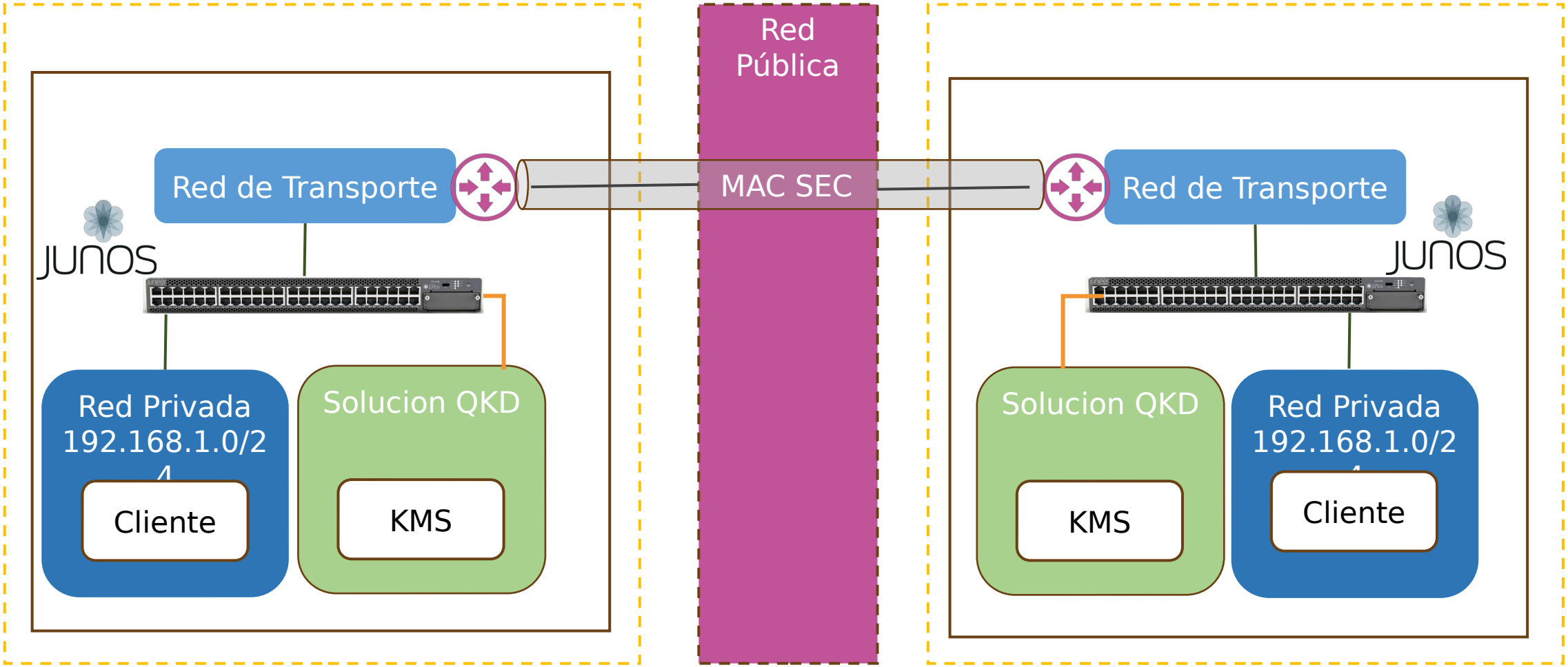
# Uso tradicional de MACSEC.



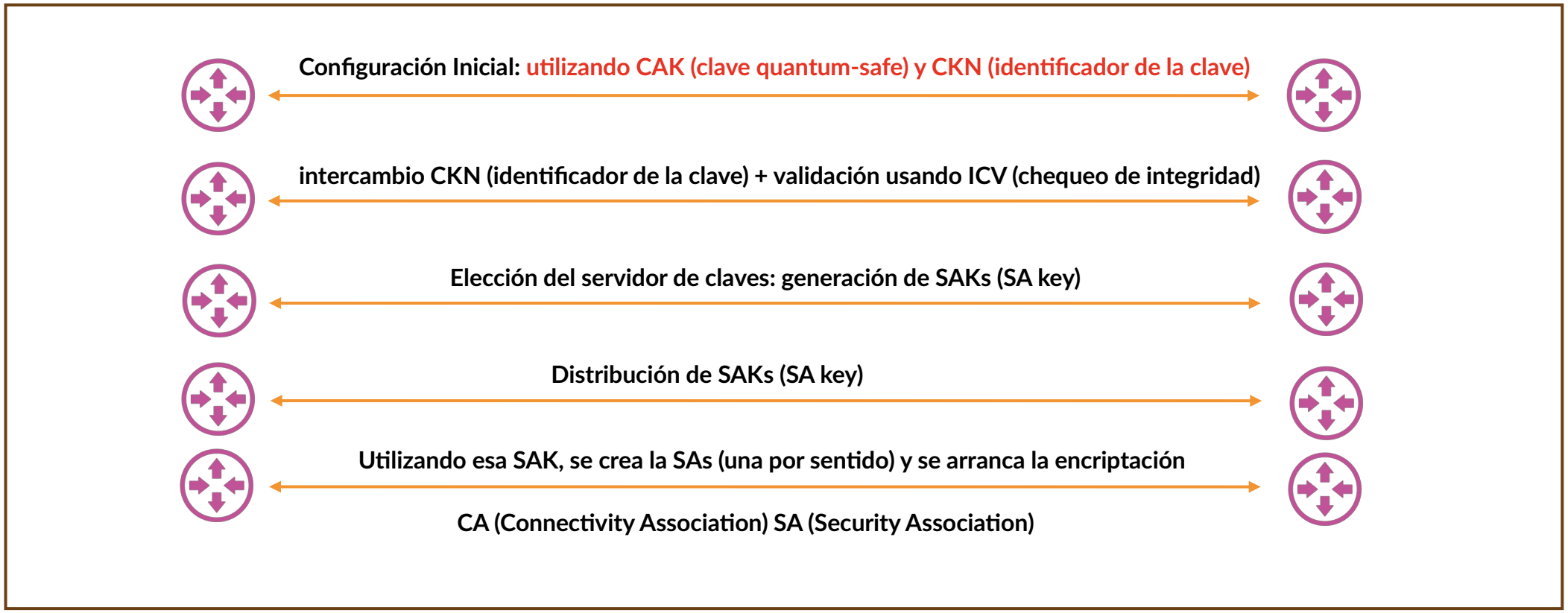
# MACSEC flujo de establecimiento.



# Claves Quantum-safe con MACSEC.



# MACSEC usando claves Quantum-safe.

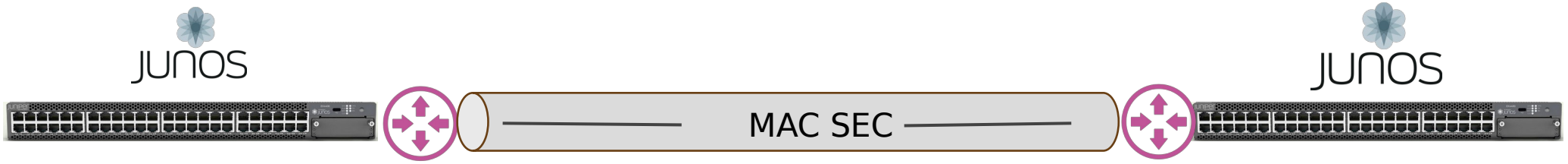


# MACSEC Quantum-safe (config en JunOS).

onfiguración MAC + macro con python script.

```
set security macsec connectivity-association {c_a} cipher-suite gcm-aes-xpn-256
set security macsec connectivity-association {c_a} security-mode static-cak
set security macsec connectivity-association {c_a} pre-shared-key ckn <ckn_example>
set security macsec connectivity-association {c_a} pre-shared-key cak <cak_example>

set security macsec interfaces {interface} apply-macro qkd kme-ca false
set security macsec interfaces {interface} apply-macro qkd kme-host {kme-qkd-server}
set security macsec interfaces {interface} apply-macro qkd kme-port 443
set security macsec interfaces {interface} connectivity-association {c_a}
set security macsec interfaces {interface} apply-macro qkd kme-key-id-check true
```



# MACSEC Quantum-safe: consumo de claves I .

**Paso 1**: Inicio del consumo de claves quantum-safe:

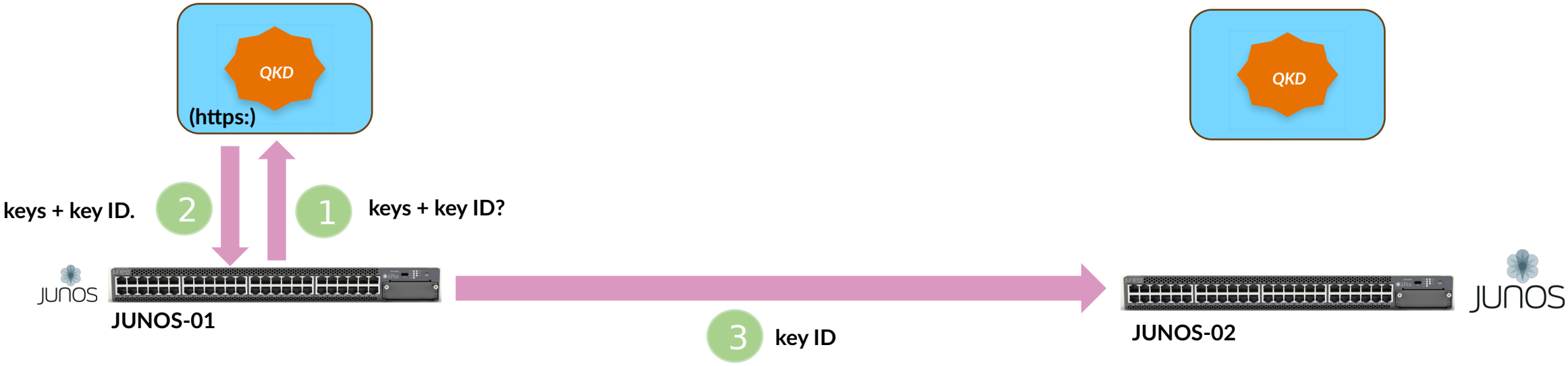
JUNOS-01 solicita vía API (HTTPS) una clave (key) y el identificador de la clave (key_id).

**Paso 2**: QKD/KMS responde con una clave quantum-safe + un identificador.

# MACSEC Quantum-safe: consumo de claves II .

**Paso 3**: JUNOS-01 Envía del Key ID al peer JUNOS-02.

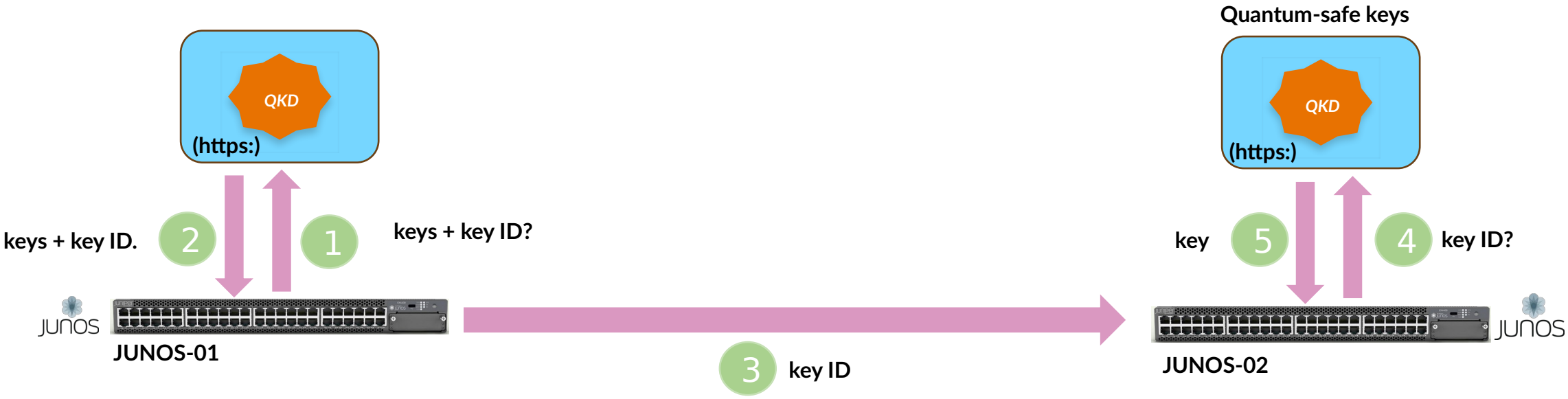
**JUNOS-01** envía el identificador (key_id) de la clave a utilizar a **JUNOS-02**.



# MACSEC Quantum-safe: consumo de claves III

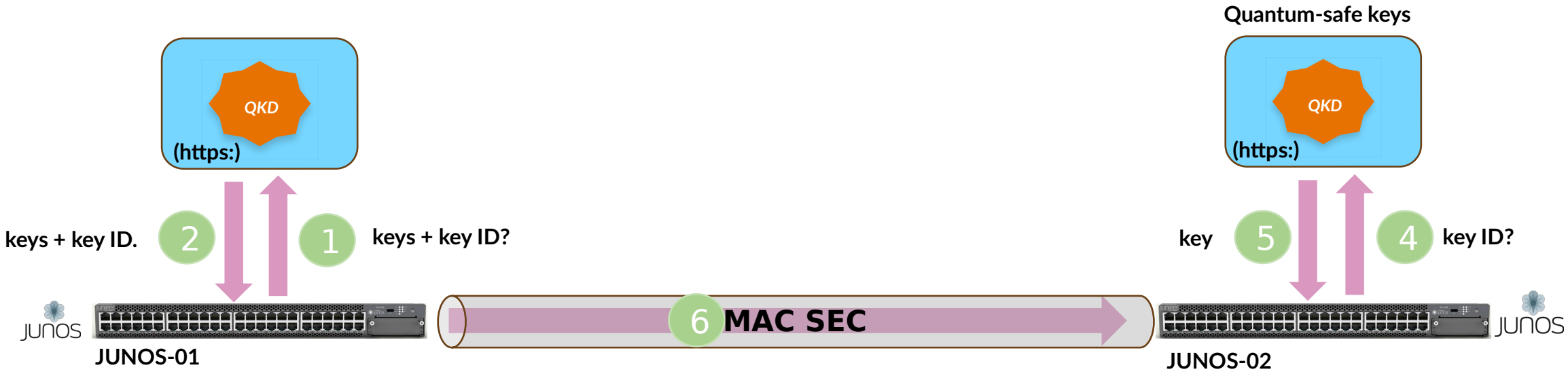
**Paso 4**: JUNOS-02 consulta con el QKD/KMS las clave quantum-safe usando el identificador.

**Paso 5:** QKD/KMS respondes a JUNOS-02 con la clave asociada a dicho indentificador



# MACSEC Quantum-safe: consumo de claves IV

**Paso 6:** ambos peer utilizan la clave para autenticar y encriptar



## Índice



LUXQUANTA

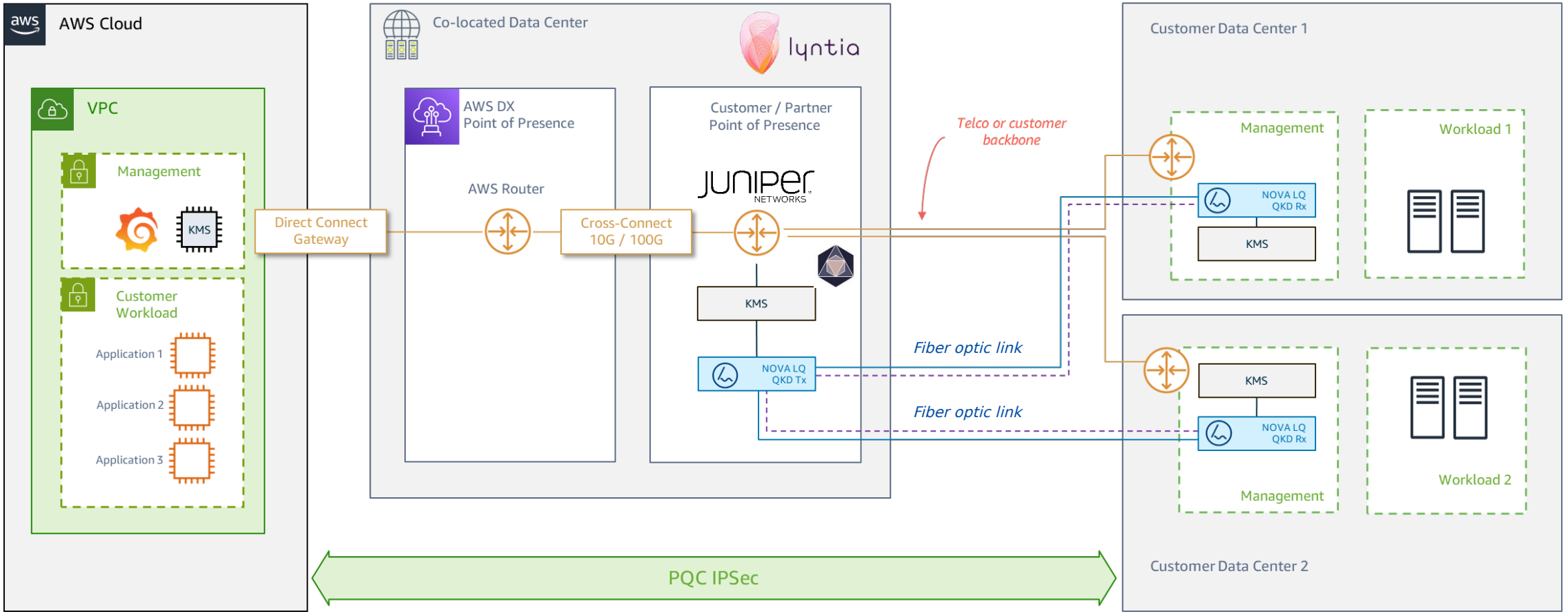
merqury cybersecurity

JUNIPER NETWORKS

lyntia
NETWORK TO BUSINESS

# Private quantum-secure connection

## Descripción General de la Arquitectura



# Respaldo publico a la tecnología

En términos de encriptación, la unión europea apuesta por la criptografía quántica con el objetivo de construir un ecosistema tecnológico propio que sustente la soberanía digital y la protección de infraestructuras criticas.

## SITUACIÓN GEOPOLITICA

**1.Presión sobre los estándares de cifrado**: Algunos gobiernos están promoviendo leyes que exigen puertas traseras en sistemas de cifrado, lo que genera tensiones entre privacidad y seguridad nacional.

**2.Desconfianza en proveedores extranjeros**: Las tensiones han llevado a restricciones sobre el uso de tecnologías extranjeras, lo que afecta la interoperabilidad y la confianza en los sistemas de cifrado globales

**3.Nuevas regulaciones y soberanía digital**: Países están legislando para que los datos se almacenen y cifren localmente, lo que impacta la arquitectura de servicios en la nube y la gestión de claves de cifrado.

**Dos enfoques para un mismo problema**: encriptar los datos sensibles y mantener una soberanía digital

**Union Europea, China, Japón y Canadá apuesta por la criptografía Quántica**

Estados Unidos y Reino Unido se centran en la transición hacia la criptografía post-quántica (PQC)

## SOLUCIÓN UE

El **EuroQCI (Infraestructura Europea de Comunicación Cuántica)** es una ambiciosa iniciativa de la Unión Europea cuyo objetivo es construir una red de comunicaciones cuánticas ultra segura que abarque todo el territorio de la UE

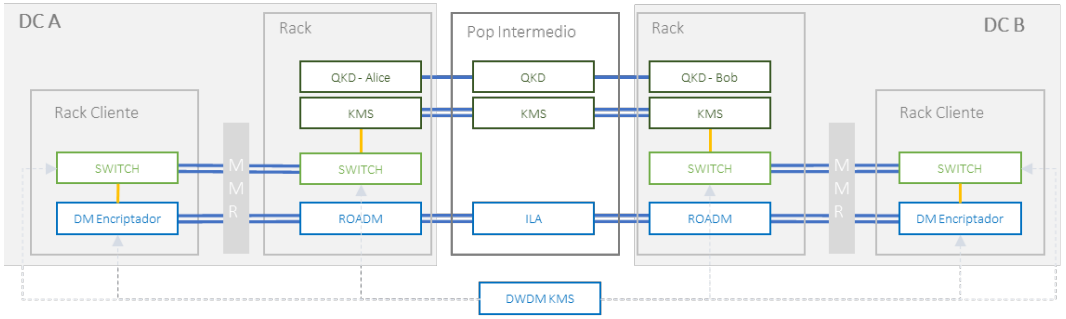
- **Proteger infraestructuras críticas** como hospitales, redes eléctricas, centros de datos y organismos gubernamentales.
- **Reforzar la soberanía digital europea**, reduciendo la dependencia de tecnologías extranjeras.
- **Impulsar la industria cuántica europea**, involucrando a empresas, pymes y centros de investigación.
- **Contribuir a la Estrategia de Ciberseguridad de la UE y al objetivo de la Década Digital de estar a la vanguardia de las capacidades cuánticas para 2030**

https://digital-strategy.ec.europa.eu/en/policies/european-quantum-communication-infrastructure-euroqci

# Nuevos servicios y arquitecturas

La criptografía quántica es una realidad con múltiples casos de uso y donde el mayor reto para el corto plazo es conseguir construir soluciones multitenancy que permitan el acceso a la tecnología para cualquier tamaño de empresa o necesidad.

## Arquitectura QKD multi-tenant




- Una cadena de QKD para generar claves entre dos Data Centers
- El proveedor neutro de conectividad y encriptación aloja los equipos QKD en los racks de su propiedad
- Se implementa una solución Hub/Spoke con MACsec dentro de los Data Centers para extender las claves generadas por el enlace QKD los racks del cliente final.

## Servicios QKD

**QKD Encription L1 DCI**

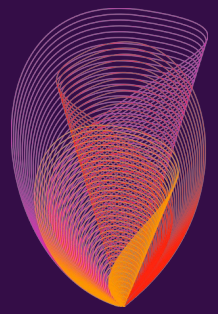
- La mejor solución para capacidades de 10/100/400G por la baja latencia y mínima reducción del ancho de banda útil.
- Se utilizan encriptadores DWDM y el cliente dispone de un portal web donde administrar la seguridad de sus servicios.

**QKD Encription L2 DCI**

- Una buena opción para capacidad inferiores a 10G Ethernet por la menor inversión.
- Se utilizan switches de nivel 2 para la encriptación, de menor tamaño y consumo para facilitar su instalación en el rack de cliente.

**Quantum keys-as-a-service DCI**

- Servicio de claves generadas por entropía quántica entre dos data centers.
- Se habilita una capa de nivel2/3 para securizar las comunicaciones entre los servidores KMS y los encriptadores del cliente final.



lyntia

NETWORK TO BUSINESS