



# *Quantum-Safe Digital Infrastructure*

ITALTEL & Quantum Bridge Technologies (QBT)



# Symmetric-Key Distribution System (SDS)

## Cripto-ágil

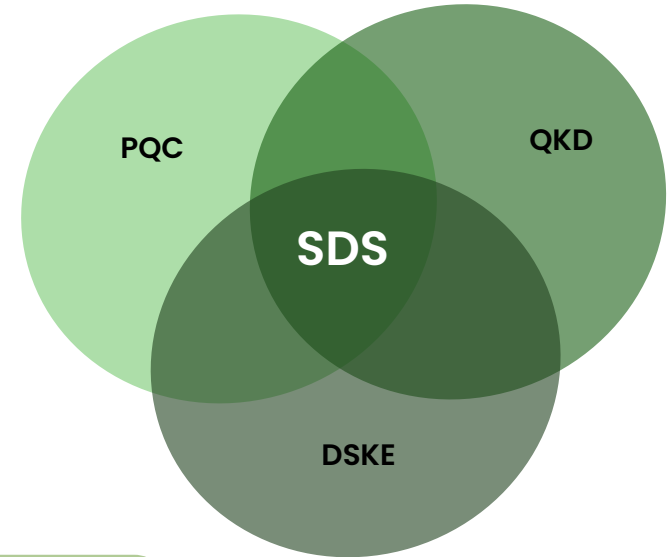
Actualiza fácilmente su pila de criptografía y combina entre PQC, DSKE y QKD sin complicaciones

## Integración fluida

Una herramienta totalmente automatizada basada en Ansible que reduce el tiempo de instalación y configuración de días a minutos

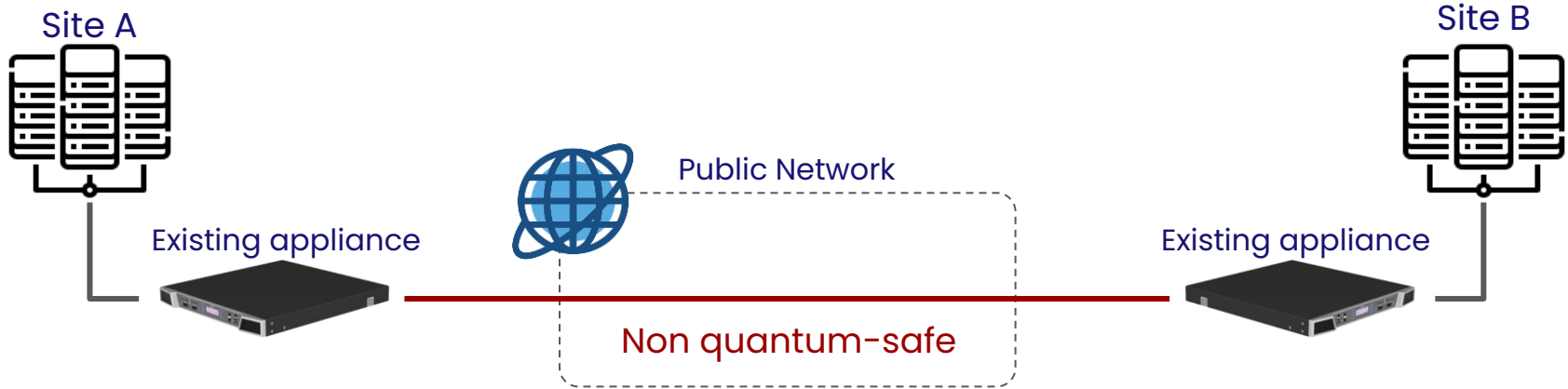
## Seguridad preparada para el futuro

Respalda por una prueba de seguridad auditable que garantiza la invulnerabilidad computacional frente a amenazas tanto clásicas como cuánticas



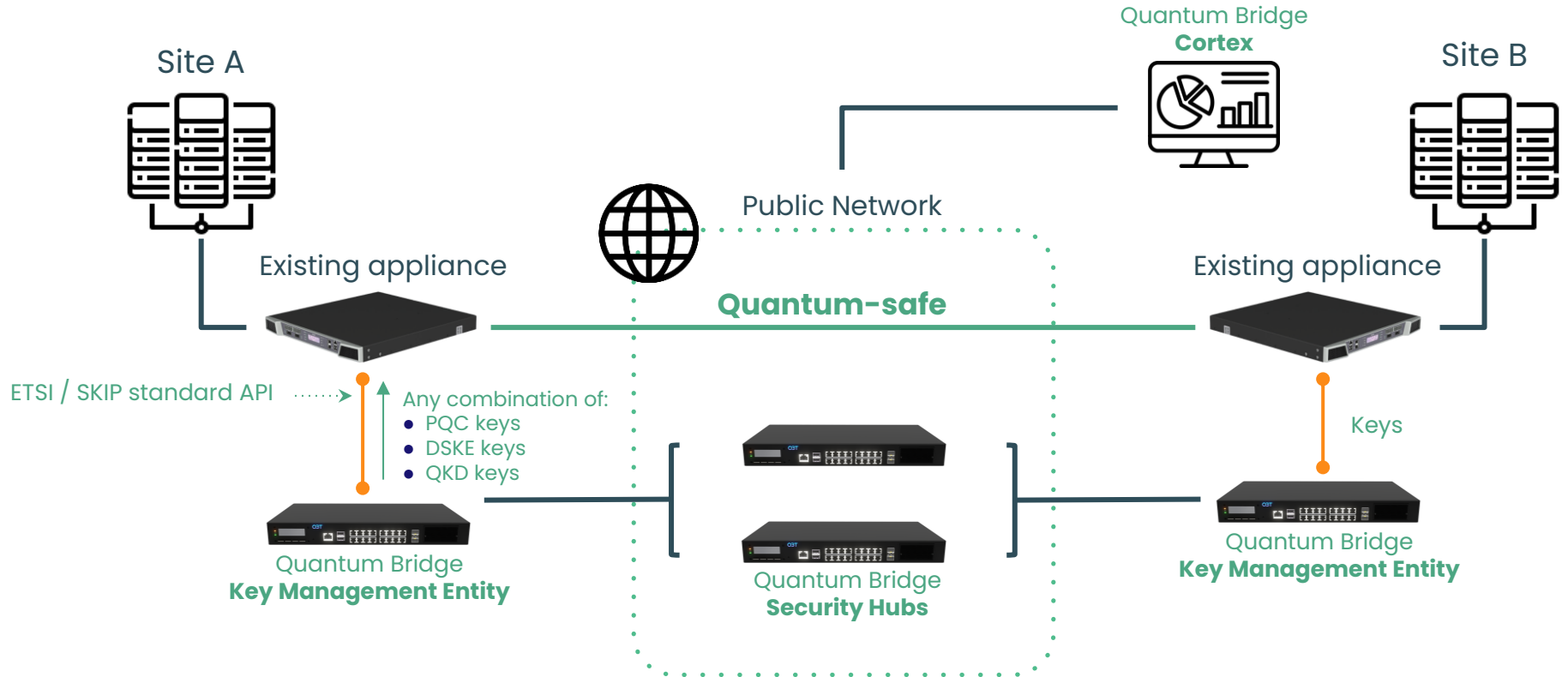
### Propuesta de valor de DSKE

- ⇒ Mayor seguridad y automatización de todo el ciclo de vida de las claves
- ⇒ Reducción de costes operativos en la gestión de claves
- ⇒ Resiliencia cuántica: mitigación de la amenaza cuántica



## Infraestructura actual:

- Redes basadas en PKI
- Expuestas a la amenaza **“capturar ahora, descifrar después”**
- Difíciles de actualizar mediante QKD y/o PQC

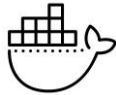


Cifra y blinda tráfico sensible entre redes críticas/estratégicas y CPDs, incluso sobre infraestructura no confiable (terceros / Internet).

## Entornos de operación



**Dispositivos móviles**  
(smartphone / tablet en terreno)



**IoT/OT en contenedores**  
( Docker / Kubernetes)



**Cloud y on-premises**  
(VMware ESXi / Hyper-V)

## Valor añadido



Disponemos de un laboratorio para PoCs / demos e integraciones con soluciones y appliances de red y ciberseguridad.

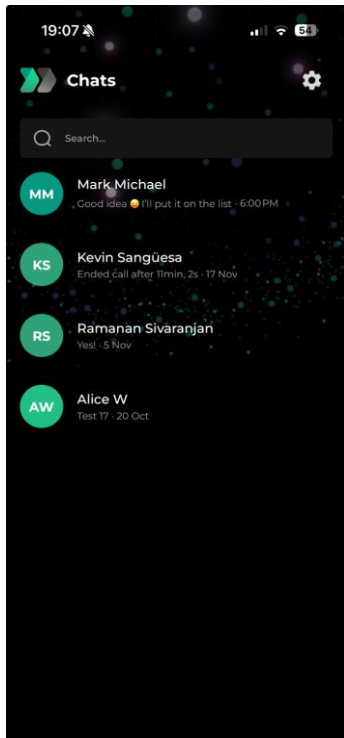
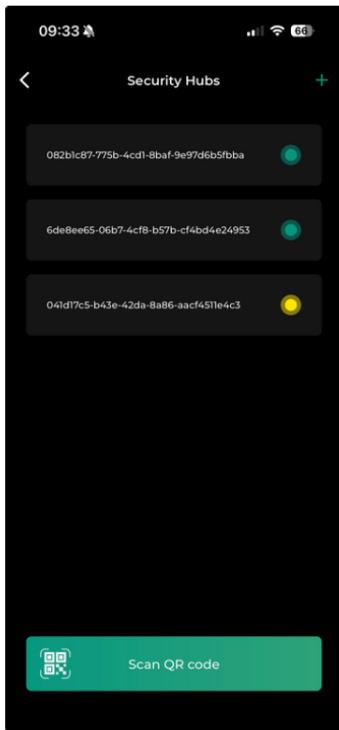


SOLUCIÓN PERSONALIZABLE SEGÚN REQUISITOS Y ENTORNOS DE CLIENTE

## Valor para diferentes entornos

- Confidencialidad y resiliencia del tráfico sensible en redes WAN/LAN y Centro de Datos.
- Operación sobre redes de transporte no confiables sin asumir "red segura".
- Interconexión segura entre sedes y enclaves distribuidos.
- **Una dominios QKD** en ubicaciones distintas (cuando aplique).





## Funcionalidades

- Chat de texto
- Compartición de archivos
- Llamadas de voz (WebRTC)
- Soporte para **iOS**
- Solución totalmente **on-premise** o **como servicio**
- Chats grupales
- Videollamadas
- Soporte para **Android**
- Gestión de usuarios a nivel empresarial con **Black Phone Manager** y Distribution Tower

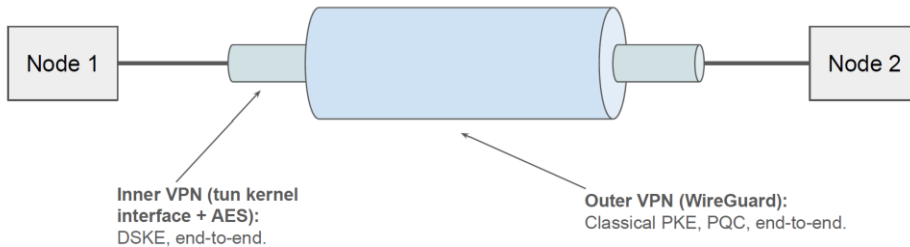
## Criptografía

- **Cifrado de extremo a extremo** mediante AES-GCM
- Claves de cifrado a partir de la combinación de **X25519, PQC y DSKE**
  - Rotación configurable
- Incorporación escalable de claves simétricas mediante **códigos QR**

La plataforma VPN que crea una red Overlay de **alta seguridad** con **doble cifrado** independiente y autogestionada que conecta sedes, nube y usuarios remotos con máximo control, escalabilidad y sin lock-in de MPLS ni de terceros.

## 1. Quantum Security by NSA CSfC-Style

Doble capa de cifrado independiente, autenticación mutua y arquitectura pensada para entornos **compliance-ready**.



## 2. Operación simple y centralizada

Los nodos se autentican primero contra un servicio central de gestión, que define identidad, reglas de red y políticas (SSO, DNS...), onboarding de peers y **conectividad site-to-site**

## 3. Menor coste y más soberanía

Funciona sobre redes públicas o privadas, **reduce dependencia de infra dedicada** y mantiene el control del cliente sobre sus claves y su postura a través del **Gateway Quantum Fabric** por site

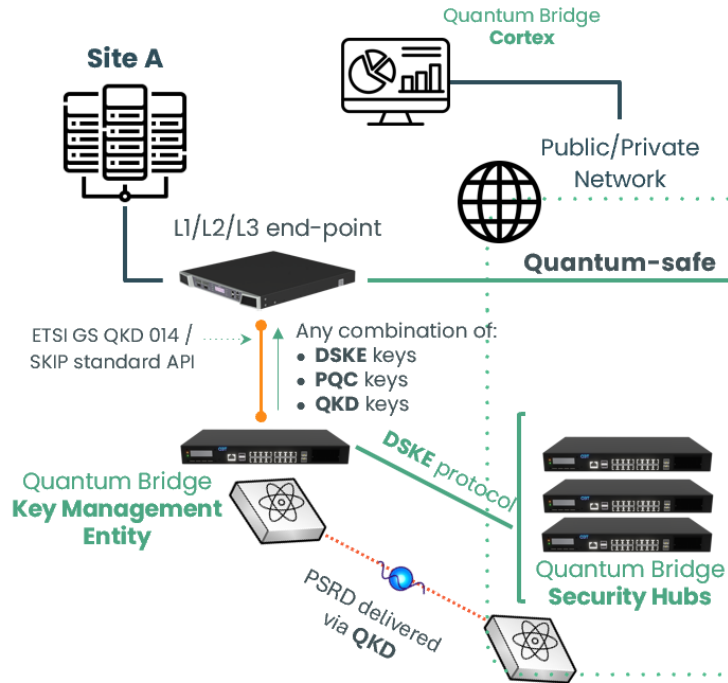
**VENTAJA:** Seguridad de red privada, con la flexibilidad económica de una red pública.



Mantiene conexiones seguras sobre Internet pública y múltiples backbones

**Ideal para:** Sector público, embajadas, defensa, infra crítica, entornos distribuidos y MSPs/Telcos que quieran ofrecer **Network-as-a-Service**.

Italtel como **distribuidor e integrador de sistemas** de la solución, proporcionando servicios de **ingeniería**



#1

**Migrar** su infraestructura hacia una postura segura frente a la computación cuántica

#2

**Diseñar y configurar** el enrutamiento seguro y la conectividad entre sedes distribuidas

#3

**Integrar** Quantum Bridge KMS con su infraestructura existente de red y seguridad

Italtel como **distribuidor e integrador de sistemas** de la solución, proporcionando servicios de **ingeniería**

#4

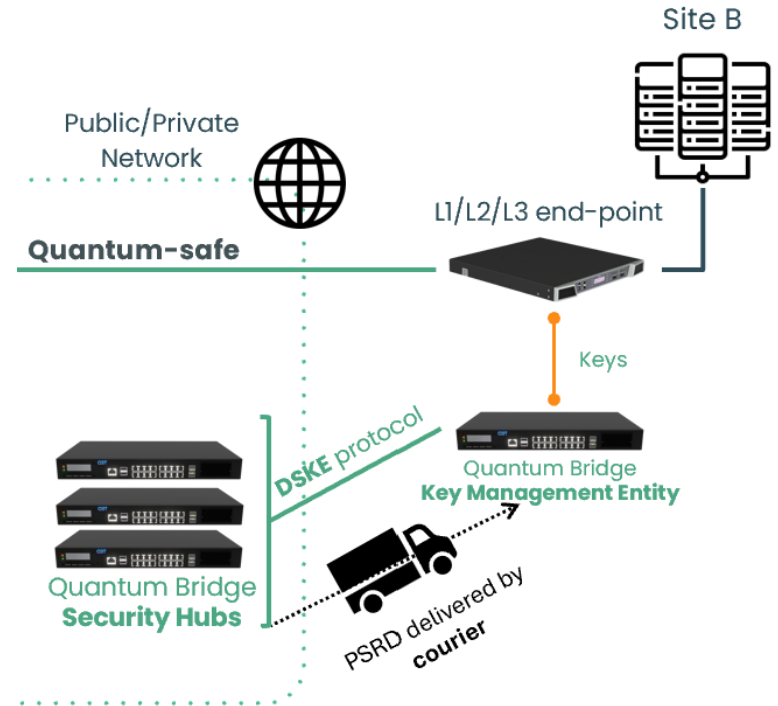
**Desplegar y automatizar** la solución completa, adaptada a la complejidad de su red

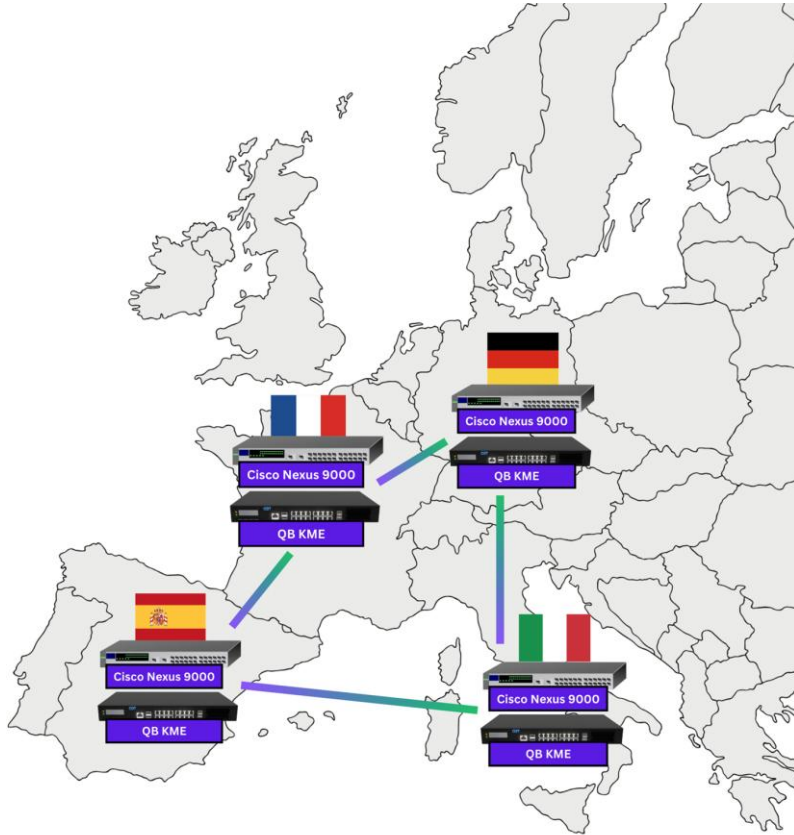
#5

**Monitorización y analítica**, con información en tiempo real e informes periódicos desde la plataforma central

#6

**Validar** casos de **uso reales** y pruebas de concepto (**PoC**) en nuestro laboratorio dedicado de **Quantum Bridge**, en diversos entornos de red

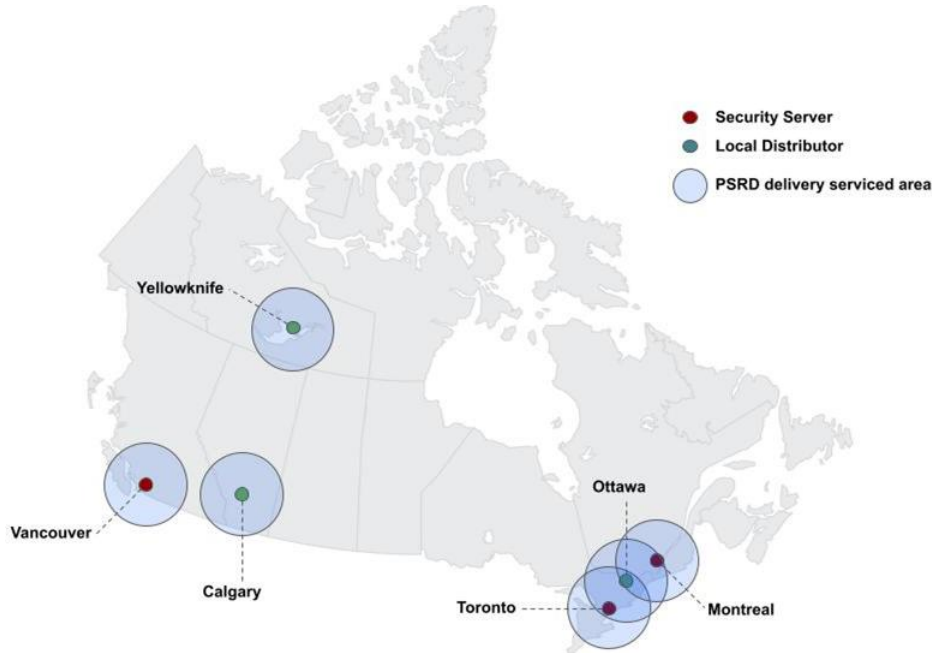




**Problema:** Seguridad a largo plazo para redes de pago en Europa

**Solución:** Quantum Bridge e Italtel desplegaron la solución para proteger una red europea transfronteriza con seguridad de nivel 2 (MACsec)





**Problema:** Seguridad a largo plazo para comunicación entre los centros

**Solución:** Proyecto piloto con Thales CN6010, dispositivos Juniper SRX y la solución Quantum Bridge Key Management System. Hubs de seguridad operados por Quantum Bridge.

Toronto startup to test its quantum-resistant key distribution solution

HOWARD SOLOMON

FEBRUARY 21, 2023



DRDC  
RDDC  
Canada



**Problema:** Seguridad a largo plazo para comunicaciones críticas (p. ej. Sistemas de transacciones de pagos)

**Solución:** Proyecto piloto con QB Key Management System solutions. Los 3 SHs están operados por el cliente.



## 4 razones para confiar en Italtel



### Tecnología sin ataduras

Elegimos siempre la mejor opción del mercado, trabajando con múltiples fabricantes.



### Soporte total, siempre

Desde la estrategia hasta la operación continua: 24x7, multicanal.



### Cercanía local, respaldo global

Centros propios en España, apoyados por una red internacional.



### Experiencia que da confianza

Más de 100 años de historia y proyectos en Telco, Administración Pública, Industria y Energía.

## Excelencia validada por normas internacionales



**Esquema Nacional de Seguridad**  
(nivel alto)



**ISO 9001**  
Gestión de la Calidad



**ISO 14001**  
Gestión del Medioambiente



**ISO 14064**  
Gases de Efecto Invernadero



**ISO 20000**  
Gestión de Servicios TI



**ISO 22301**  
Continuidad de Negocio



**ISO 27001**  
Gestión de Seguridad de la Información



**ISO 27017**  
Controles de Seguridad para Servicios Cloud



**ISO 27018**  
Protección de Información Personal en Cloud



**ISO 27701**  
Gestión de la Privacidad de la Información



**ISO 42001**  
Sistemas de Gestión de la Inteligencia Artificial



Inscrita en la Dirección General de Armamento y Material (DGAM)



**DORA**  
(Digital Operational Resilience Act)



**NIS2**  
(Network and Information Security Directive 2)