

# Digital Quantum Key Distribution (DQKD)

*Discover the future of quantum key generation, where distance is no obstacle and security is enhanced, all in a cost-effective, efficient package, compliant with ETSI-014.*







## What is Qrypt's DQKD?

**Qrypt's Quantum Random Number Generators (QRNGs)** feed Qrypt's DQKD to enable independent generation of truly random secret keys at multiple endpoints. Built on the robust BLAST protocol, DQKD defends against the Harvest Now, Decrypt Later (HNDL) attacks. DQKD also eliminates the need for centralized key distribution, minimizing bottlenecks and reducing single points of failure.

**Qrypt's QRNGs** were developed in an exclusive partnership with Los Alamos and Oak Ridge National Laboratories, have the most powerful output available at 1.575 Gbps, and are NIST ESV certified.



## The Qrypt Advantage

-  **Cost-effective alternative to traditional QKD** providing resiliency and no single point of failure
-  **No expensive hardware** for optimal scalability, performance, and global enterprise deployment
-  **Plug-and-play expansion for QKD networks** that enhances capabilities while adhering to ETSI-014
-  **Interoperability** with all existing infrastructure
-  **Solves traditional QKD limitations** including ~150km distance and 1.2 Mbps key rates
-  **Available on-premises and in the cloud** for simple setup and maximum flexibility

## Use Cases

-  Connecting QKD nodes
-  VoIP security
-  Integrate with TCP/IP protocols for enhanced security
-  Secure IoT
-  Quantum-secure IPsec VPNs
-  Secure storage
-  Integrate for secure authentication in 4G/5G networks
-  NVIDIA DPU integration

## Successful Pilot Deployment: Megaport ×

### CHALLENGE

Quantum computing poses an existential threat to modern encryption. Data captured today by cyber criminals and nation-state actors is susceptible to “Harvest Now, Decrypt Later” attacks. Enterprises must adopt quantum-secure solutions to protect data today.

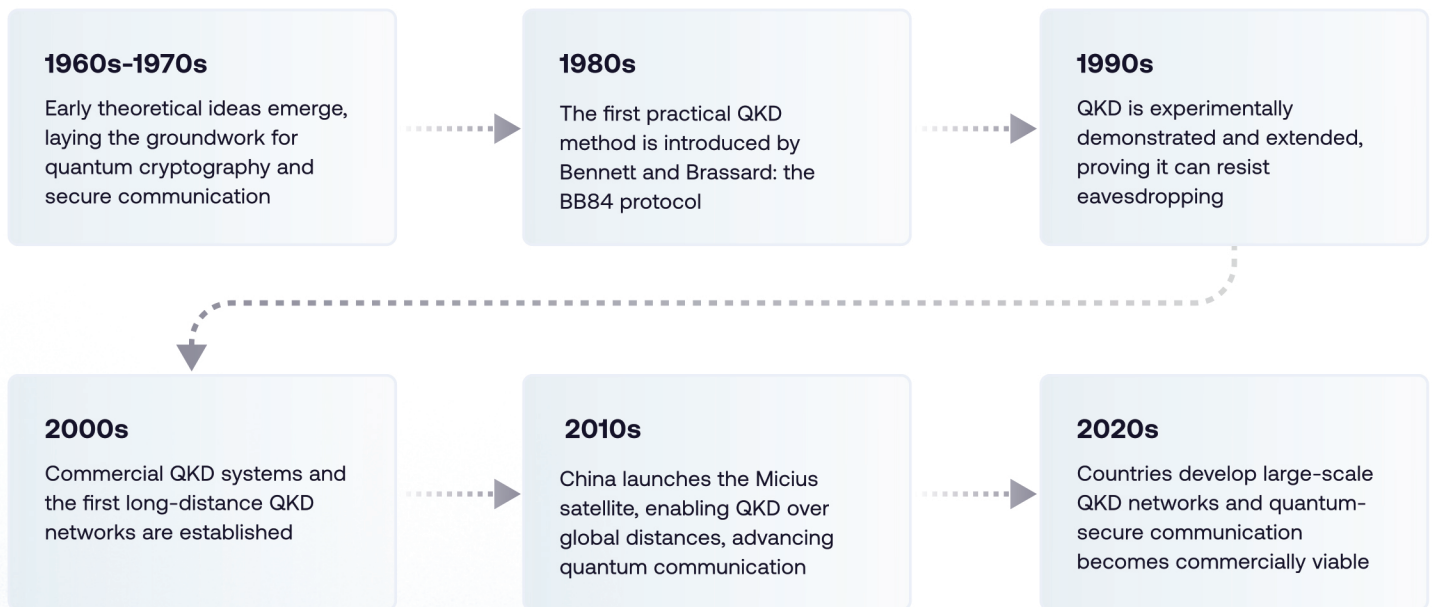
### SOLUTION

The first-ever global quantum-secure communications debuted with Qrypt’s DQKD technology over Megaport’s Network-as-a-Service, eliminating key exchange vulnerabilities during file-sharing across three global locations: (1) AWS in San Francisco, (2) Azure US East in Virginia, and (3) Google Cloud in Tokyo.

### SUCCESS

- **Seamless, scalable deployment** via SDN into existing infrastructure, without any expensive hardware overhaul
- **Future-proof data protection** using quantum entropy and zero-trust encryption to safeguard critical data from evolving cyber and quantum threats

## The History of Traditional QKD



The European Quantum Communication Infrastructure (EuroQCI) was launched in 2020 to create a secure, pan-European quantum communication network using QKD to safeguard data transmission and enhance cybersecurity across EU member states, supercharging commercial demand



## Qrypt's DQKD Complements Traditional QKD

**1**

### Redundancy

Enhances resiliency by providing backup key distribution, ensuring continuous secure communication.

**2**

### Range

Expands secure key distribution beyond the physical limitations of traditional QKD.

**3**

### Responsive

Supports both software and hardware deployments, integrating seamlessly into diverse infrastructures.



## Getting Started with Qrypt's DQKD



### Simple Deployment with Docker Container or a Dedicated Server System

Qrypt's DQKD offers both a software- and hardware-based deployment. Implementing software-based DQKD is as straightforward as a Docker container. Hardware-based DQKD can be easily deployed by integrating servers hosting DQKD into any ETSI-014 compliant network, regardless of scale or technical spread.

#### Software Deployment

Deploy Qrypt's DQKD in your network as a Docker container, designed for hassle-free integration. This approach ensures compatibility with a wide range of systems and simplifies the transition to enhanced quantum security.

#### Hardware Deployment

For enhanced security, DQKD can be deployed on dedicated hardware. The DQKD instances will reside within the same security boundary as the application requesting keys from DQKD, and can be accessed using the ETSI-014 API.



### Accessing Documentation

For detailed guidance on setup and deployment, access our documentation here: [docs.qrypt.com](https://docs.qrypt.com). This resource provides the necessary information to integrate Qrypt's DQKD into your network seamlessly.

Implementing Qrypt's DQKD is a straightforward step towards securing your communications against quantum and classical threats, ensuring your cryptographic infrastructure remains robust and future-proof.

## How Qrypt's DQKD Works: A Technical Overview

Qrypt's DQKD streamlines quantum-secure key management through a sophisticated, software- or hardware-based Key Management Entity (KME) deployable either as a virtual machine (VM), as a container, or on a dedicated hardware system. The following is a step-by-step breakdown of the key generation and exchange process:

- 1 Initiation:**  
 Server Application Entities (SAEs) at different sites initiate the key request process by contacting their respective DQKD KMEs within the security boundary.
- 2 Key Generation:**  
 Each KME generates encryption keys upon request, utilizing the Qrypt SDK. This process is facilitated by REST APIs that are compatible with the ETSI GS QKD 014 specifications.
- 3 Metadata Exchange:**  
 KMEs securely exchange metadata over an encrypted channel, robust enough to maintain security for at least one hour, enabling the recreation of identical keys at multiple sites.
- 4 Key Recreation:**  
 Upon receipt of the metadata, the receiving KME uses the Qrypt SDK to recreate the corresponding key, ensuring that both sites have synchronized encryption keys.
- 5 Key Storage:**  
 The generated keys are stored in-memory, with options to use secure key storage solutions such as SoftHSM or physical HSM, interfaced through PKCS#11 standards.
- 6 Key Retrieval:**  
 SAEs retrieve the keys from their KMEs within the same security boundary, enabling encrypted communications with the assurance of quantum security, as the symmetric key is never transmitted.

This process facilitates secure key exchange across any geographical distance and aligns with Quantum Key Distribution (QKD) principles, offering a quantum-resistant security layer that can integrate with or enhance existing QKD infrastructures.

