IDQ

Redefining Security

▸ Clarion KX Platform

Quantum Key Exchange (Q-KX) platform for end-to-end Post Quantum Security

Mapping and maintaining robust cybersecurity practices on current infrastructure, while simultaneously addressing the looming quantum computer threat across enterprise-wide networks, is challenging. This is due to the complexity of cryptographic methods and the variety of vendor solutions that rely on them to securely transmit highly confidential or sensitive information.

ID Quantique, with its Clarion KX platform, addresses this challenge by giving CIOs and CISOs full control over the key exchange plane while supporting a diverse portfolio of encryption vendor solutions for the data plane to meet the ever-growing demands of secure data exchange.

Clarion KX is a comprehensive cybersecurity solution that effortlessly ensures data in transit is always resistant to both current cryptographic attacks and the looming quantum computer threat, assuring long-term confidentiality against 'harvest now, decrypt later' cyber-attacks.

Purpose-built for large-scale quantum-safe key distribution, Clarion KX delivers the highest end-to-end security with a blend in solution for Corporate, Government and Telecom Operator Network infrastructure.

KEY INDUSTRIES

Telecom & Data Center Service Providers	Banking & Finance	Government & Defence
Critical Infrastructure	Healthcare Organizations	IP-rich Enterprises

KEY USE CASES

Quantum-Safe infrastructure migration	Crypto-agility with the best of physics and math cryptography	Easy multi-vendor encryption/solution integration
Scalable, resilient key distribution infrastructure	Migrate to PQC today, deploy QKD tomorrow	Seamless integration of any QKD technology

CLARION KX ESSENTIAL FUNCTIONALITIES

1 Managed crypto agile Quantum Safe migration in complex communication infrastructure

2 Symmetric Quantum keys from the QKD and/or QRNG sources

3 QKD/PQC together or separately depending on use case and network capabilities

4 Open interfaces for high interoperability with existing and future infrastructure

5 Low latency, redundant and high availability key distribution
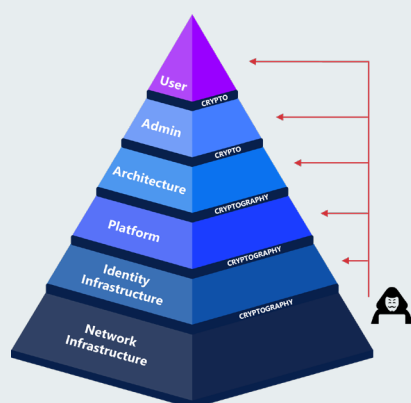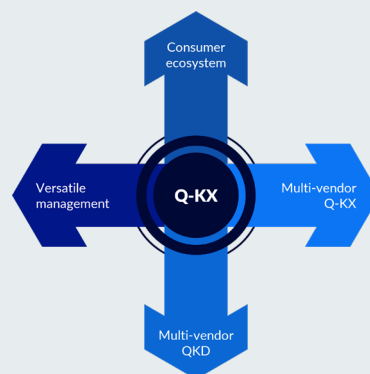
THE NEED FOR QUANTUM SECURITY AT THE CORE

The quantum threat breaks key exchange at the foundation of your network. Attackers accessing your physical network will be able to extract any secret and confidential information transiting through the IT infrastructure, therefore impacting all stacks from the ground up. This drastically shifts the paradigm of managing IT security: the foundation of your network infrastructure must now be the cornerstone of your cyber security strategy.

ONE UNIFIED PLATFORM TO MANAGE HYBRID CRYPTOGRAPHY ON NETWORK WIDE KEY EXCHANGE

Already field-proven in nationwide deployments, Clarion KX platform intelligently leverages both agile algorithm-based cryptography and quantum physics-based security to ensure unified, highly secure, out of band key exchange anywhere on the network. It also leverages a NIST-approved source Quantum Random Number Generation (QRNG) everywhere, to provide unbreakable keys.
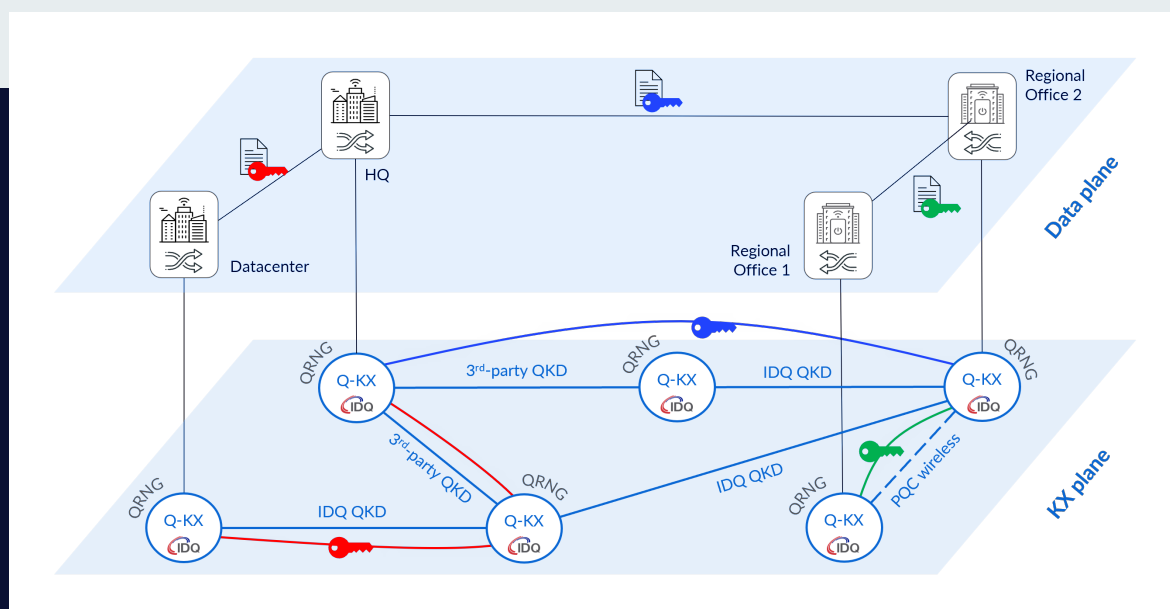
CLARION KX ECOSYSTEM

The XG/R QKD Systems

Solteris Network Appliance

KEY MANAGEMENT AND MONITORING

Clarion KX platform offers you unprecedented control over the Key Exchange plane. Ensuring full control of your crypto policy management as well as a resilient approach that fully encompasses crypto agility at its core. Its extensive Central Management service suite integrates Software Defined Network (SDN) capabilities, integration into Enterprise services via QNET API as well as IDQ's Quantum Management System (QMS) Web UI to facilitate all small to large QKD deployments.
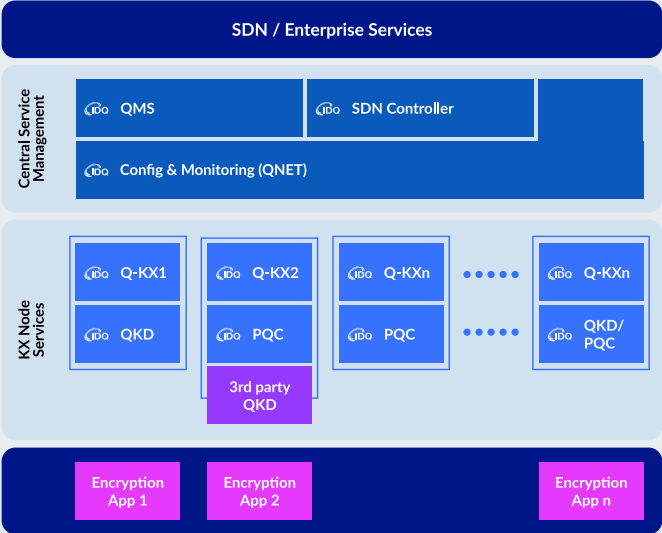
SDN / Enterprise Services		

Central Service Management

QMS	SDN Controller	
Config & Monitoring (QNET)		

KX Node Services

Q-KX1	Q-KX2	Q-KXn	••••	Q-KXn
QKD	PQC	PQC	••••	QKD/PQC
	3rd party QKD			

Encryption App 1	Encryption App 2	Encryption App n

Layer 3 Network	FORTINET · CISCO · THALES · XNsystems
Layer 2.5 MPLS	HITACHI Inspire the Next
Layer 2 Data Link	THALES · JUNIPER NETWORKS · IDQ
Layer 1 Physical	ADVA · ciena · NOKIA · PacketLight · WOORINET · ribbon

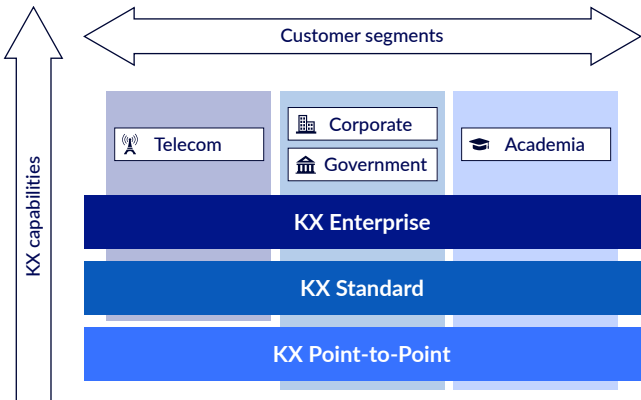*Integration with other suppliers available upon request*

INTEROPERABILITY WITH THIRD-PARTY SECURITY SYSTEMS

Clarion KX supplies symmetric keys over industry standard interfaces to encryptors on any OSI layer whether that being optical, MACSec, IPSec based VPN or Application layer. IDQ has a partnership with a leading solution provider to ensure forward long-term support. As an open platform, it can also easily be leveraged by any application to facilitate application to application direct encryptions and QKD systems (when applicable).

ADAPTIVE CLARION KX PLATFORM OFFERING

Clarion KX Platform addresses multiple customer segments, operational requirements, network sizes and business use cases. It covers Quantum Keys as a Service where trust, Service Level Agreement and delegation are crucial; Corporate and Government sectors where ownership, resilience and control is critical, as well as Academia and education where learning and experimenting with technology is key to adoption. For each of the aforementioned segments, Clarion KX provides the flexibility to start small now and scale up as needed.

Customer segments

KX capabilities

Telecom	Corporate	Academia
	Government	

KX Enterprise

KX Standard

KX Point-to-Point

FEATURES, INTEGRATION AND DEPLOYMENT

Clarion KX node services	XG/R QKD Systems	Solteris Network Appliance
Description	IDQ QKD systems and Clarion KX software all-in-one. Included in all IDQ's XG Series of QKD systems.	Standalone KMS appliance with embedded IDQ QRNG running Clarion KX software suite.
Applications	Small and large network infrastructures focusing on simplicity of integration and management of the QKD technology.	Quantum-safe networks requiring increased redundancy, multi-QKD vendor support, or if a separate hardware for Q-KMS is required.
Key features		
Connect any encryptors (ETSI GS QKD 014, SKIP, SNMP)	Yes	Yes
Secure key relaying	Yes	Yes
NIST-certified QRNG	Yes	Yes
FIPS 140-3 ready Q-KX Crypto Module	Yes	Yes
Redundant key routing and key buffering	Yes	Yes
Automatic in-node Q-KMS redundancy	Yes[1]	Yes[1]
Q-KX and QKD in one appliance[2]	Yes	
Integration with any QKD vendor	Yes[3]	Yes
Hybrid key exchange (PQC/QKD)	Yes	Yes
Edge connects and fiberless link (PQC)	Yes	Yes
Out of Band key delivery	By design	Compatible[4]
Datacenter access	Yes[5]	Yes

[1] Need to at least two appliances in the node
[2] Small rack footprint
[3] In relay nodes
[4] Via network segregation between Q-KX plane and data plane
[5] For large amounts of entropy or key consumers, use Solteris

Clarion KX central services	
Description	Management and monitoring of all Clarion KX node services
Features	**Central Server**
Q-KX management channel	Hub and spokeconnection to nodes, out of band compatible
Central server scalability	Cluster Deployment compatible
Q-KX Network orchestration	ETSI GS QKD 018 (*ready) or API based (WebAPI) Web UI
Q-KX Network configuration	ETSI GS QKD 015 (*ready) API based (WebAPI) Web UI
Management Access & control	User/Role based compatible with Enterprise solutions
Central server supported OS	Linux Ubuntu (on request: Alma, RedHat)
Client configuration app supported OS	Linux Ubuntu, Windows 10 and 11

IDQ

WORLD HEADQUARTERS

ID QUANTIQUE SA
Rue Eugène-Marziano 25
1227 Acacias/Geneva
Switzerland

www.idquantique.com | info@idquantique.com

SALES AND SUPPORT OFFICES

USA	**Austria**	**Singapore**	**South Korea**
Boston, MA	Vienna	Singapore	SungNam-si