

evolution 

BasejumpQDN

The Evolution of Quantum Safe Networks

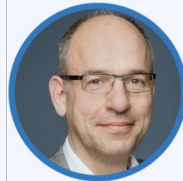
Christian Schmitz

evolutionQ helps companies get ready to be quantum-safe

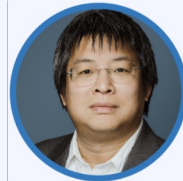
Founded and run by industry leaders



Michele Mosca
CEO



Norbert Lütkenhaus
CTO



David Jao
Chief Cryptographer

Fast Facts

- Est 2015
- 35+ team members
- AMER/APAC HQ - Waterloo, Canada
- EMEA HQ - Aachen, Germany



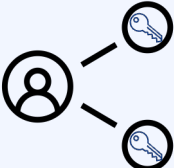
Select Partners and Industry Affiliations



The Goal is Cryptographic Resiliency

- Cryptographic Agility
 - *The ability to adapt cryptographic solutions or algorithms quickly and efficiently in response to developments to emerging threats*
 - *i.e. TLS 1.3 & IPSec*
- Defence In Depth
 - *Combining different cryptographic and security mechanisms in case of a catastrophic event*
 - *i.e. MFA, encrypting at multiple layers in the stack*
- Long Term Security
 - *Key sources not threatened by computational attacks*
 - *Harvest Now Decrypt Later (HNDL)*
 - *i.e. QKD, PSK*

New quantum-safe cryptographic technologies are available today

Post Quantum Cryptography 	Quantum Key Distribution 	Symmetric Key Infrastructure (SKI) 
<p>Scalability and flexibility of PKI. NIST Released first three in August 2024. Key Encapsulation & Digital Signatures.</p>	<p>Supported in many deployed protocols (MACSec, OTNSec, etc.). Offers Information Theoretic Security (ITS).</p>	<p>Supported in many widely deployed protocols (IPSec, MACSec, etc.). Offers Long Term Security (LTS).</p>
<p>Maturing implementations. Not Long Term Secure (LTS).</p>	<p>Specialized, expensive hardware. Operational complexity. Standards maturing.</p>	<p>Requires careful design to maintain security guarantees.</p>

Each technology has different security challenges!

Hybrid Authenticated Key Exchange (HAKE)

- Hybrid Authenticated key exchange protocols
 - Combine keying material from different sources
 - Classical PKC
 - PQC
 - PSK
 - QKD
 - I.e. $\text{SESSION KEY} = \text{KDF}(\text{Classical} || \text{PQC_KEM} || \text{PSK} || \text{QKD})$
 - Offer the greatest number of potential security guarantees
- “Authenticated” implies the use of a pre-shared key (PSK) and/or static private/public key pairs or certificates

Security Properties of the Multimodal Protocol

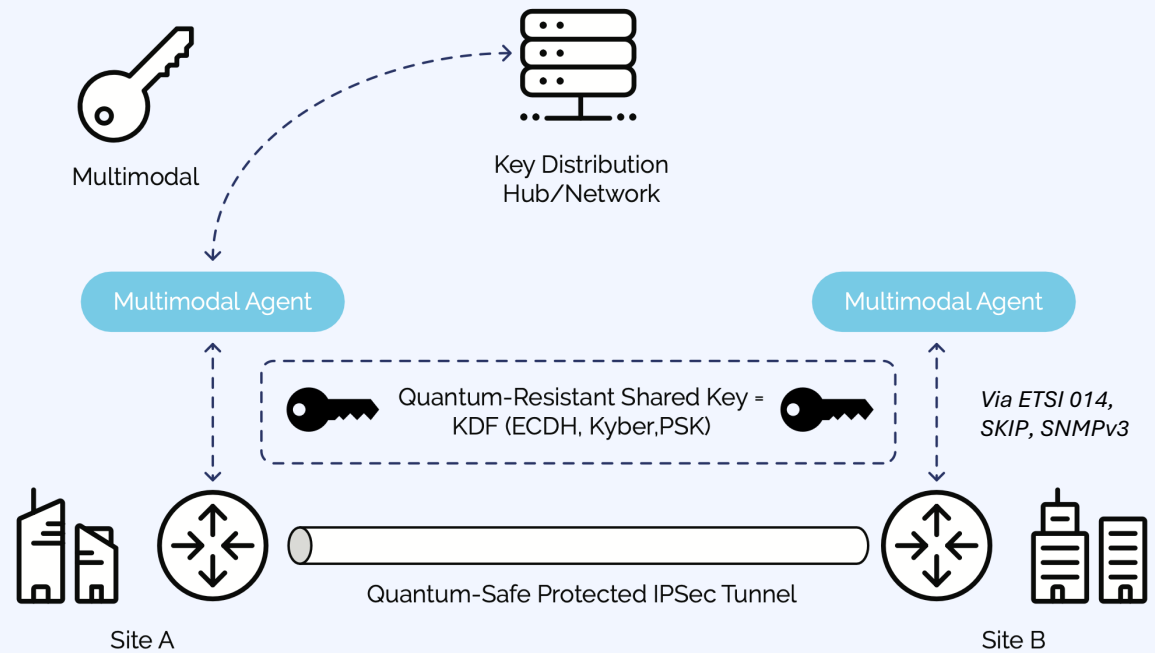
Guaranteed* security:

Long-term security (LTS) and quantum resiliency:
 Strong end-to-end keys even if all asymmetric cryptography is broken

Perfect forward secrecy (PFS):
 Past keys are secure even if
 all asymmetric crypto is broken and
 all endpoints and all KDHs have been
 breached

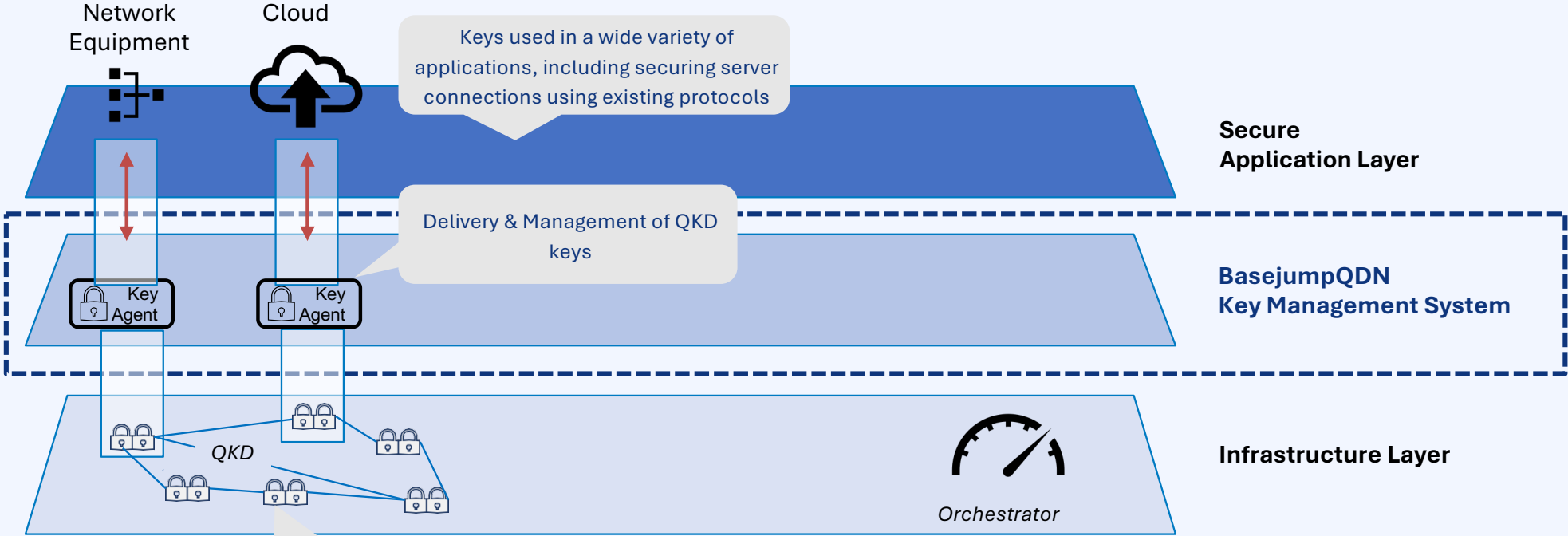
Post-compromise security (PCS)
 If a key is somehow exposed, new keys generated
 by the algorithm are not impacted by that exposure

Breaching any number of KDHs does not lead to
 endpoint identity theft



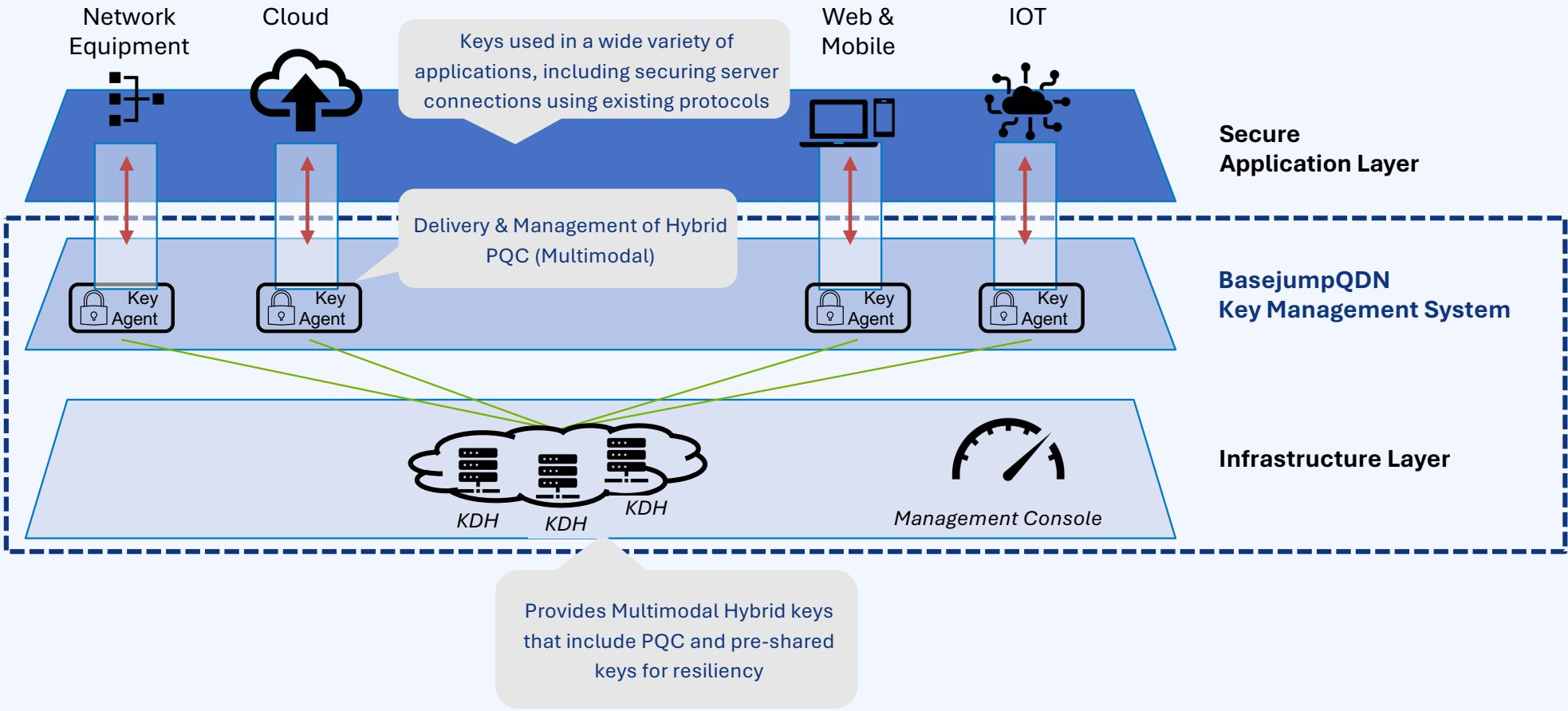
*Security Proof available: <https://www.evolutionq.com/products/multimodalkeys>

BasejumpQDN provides a single means to manage QKD key infrastructure across applications and technologies

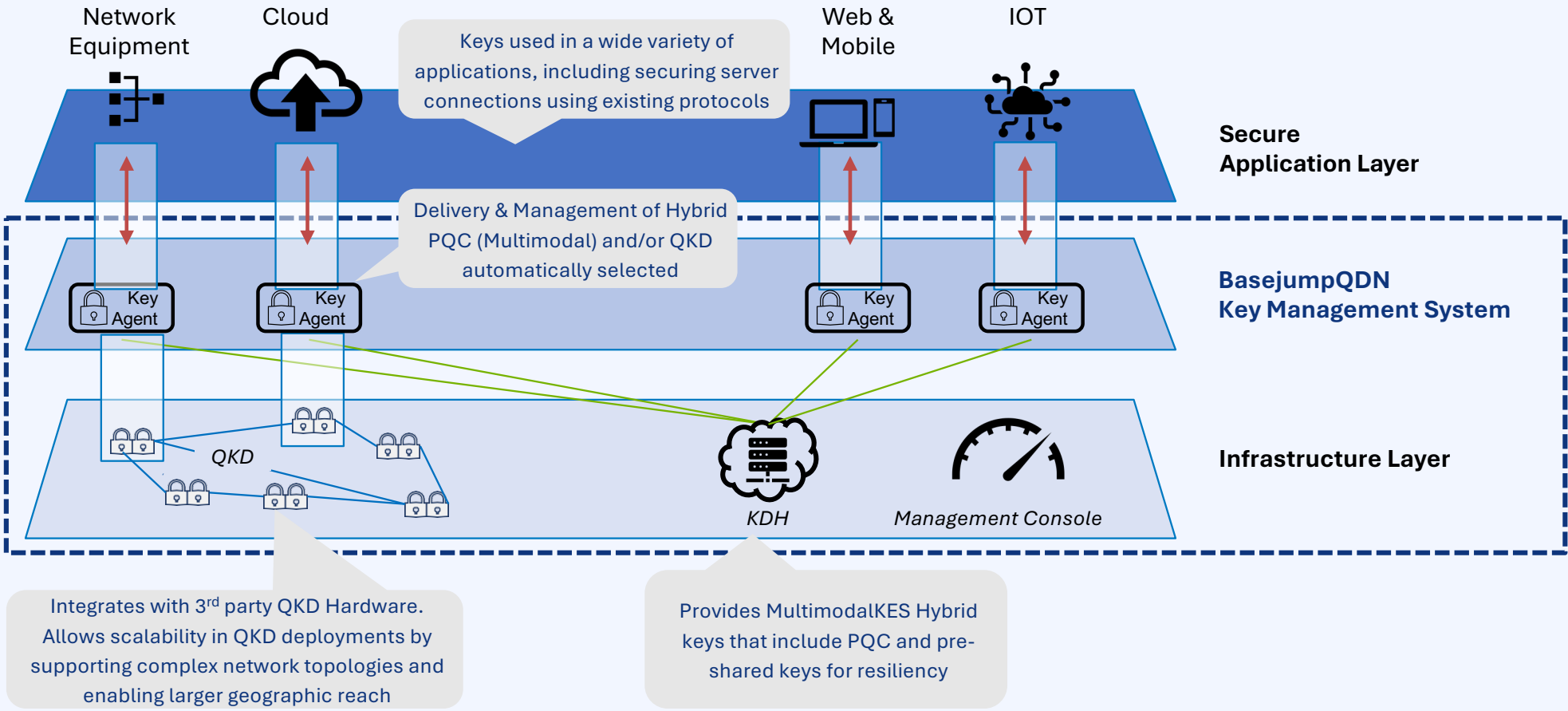


Integrates with 3rd party QKD Hardware. Allows scalability in QKD deployments by supporting complex network topologies and enabling larger geographic reach

BasejumpQDN provides a single means to manage symmetric/hybrid key infrastructure across applications and technologies

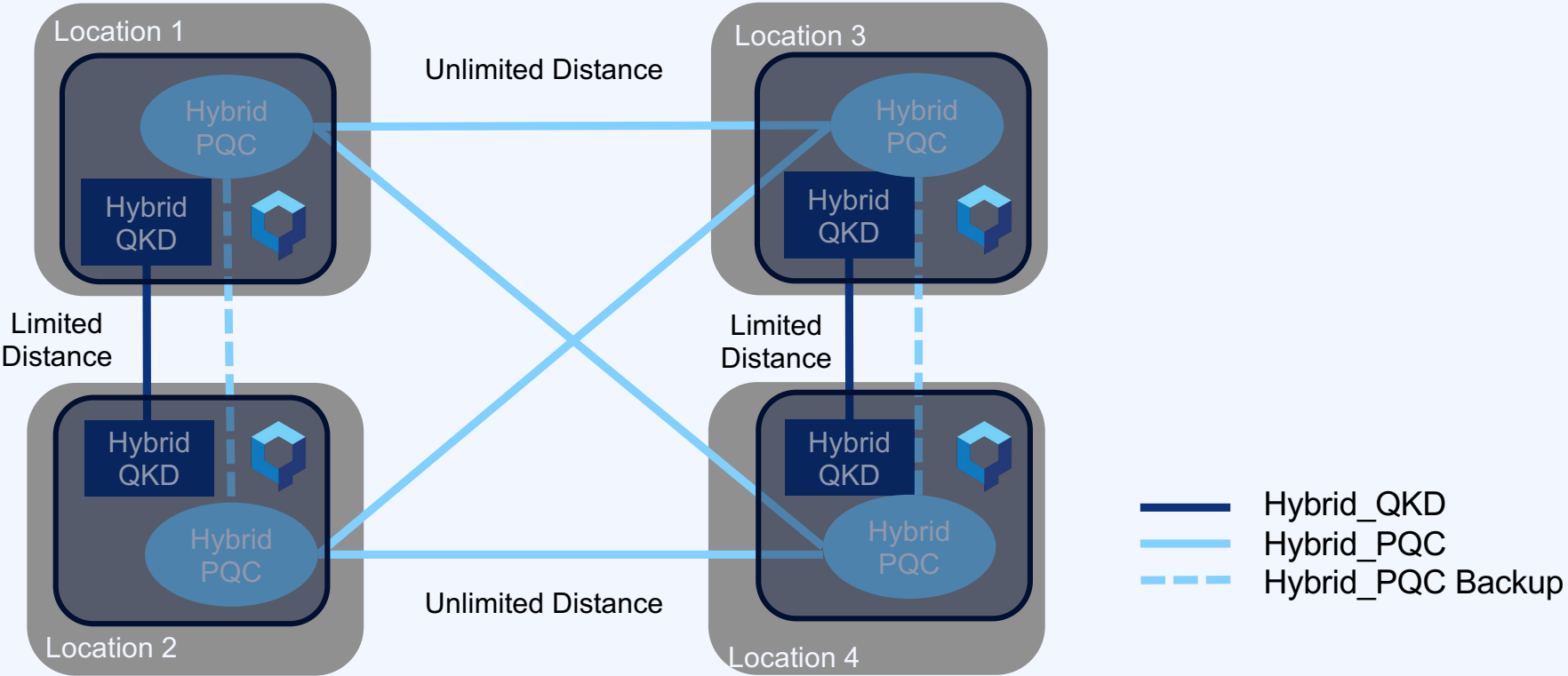


BasejumpQDN provides a single means to manage complex key infrastructure across applications and technologies



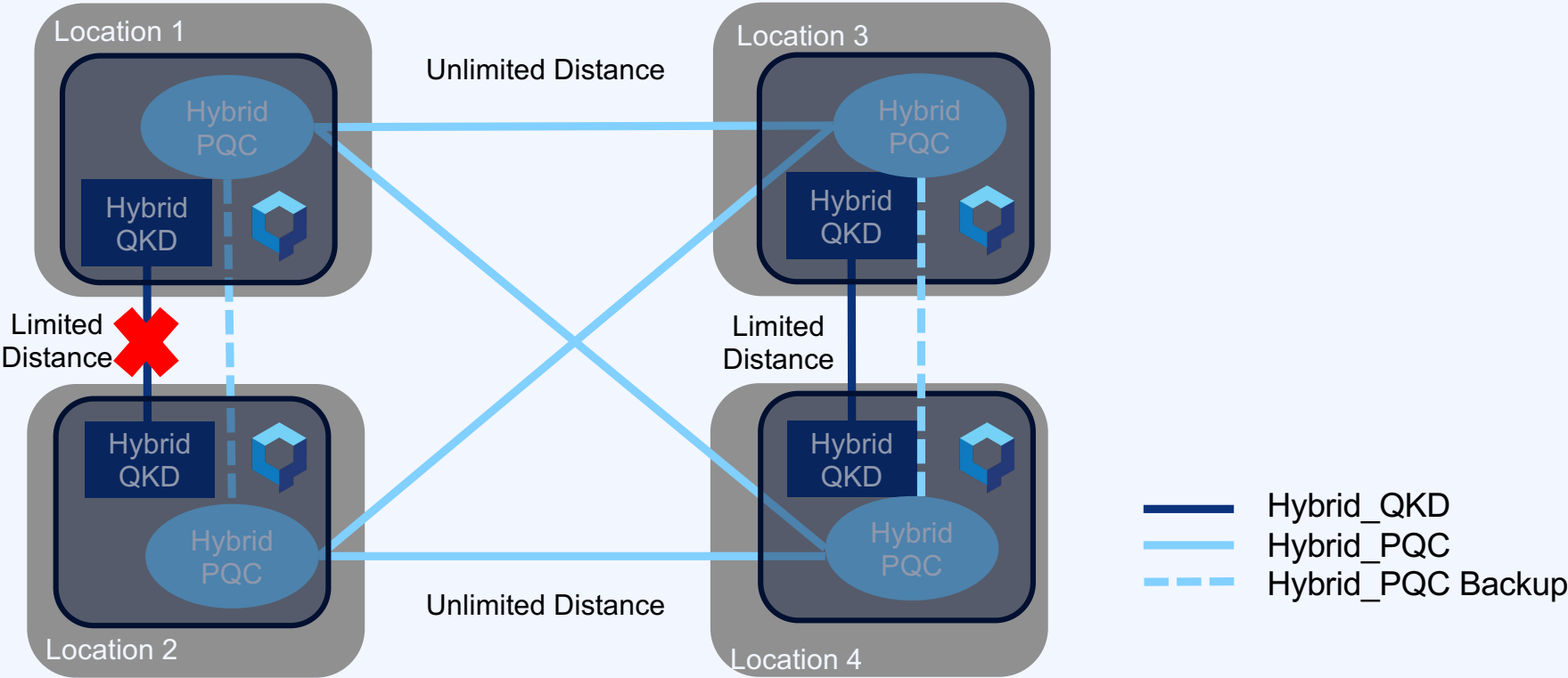
Hybrid offers Scalability

- Accommodates QKD and non-QKD links into one unified network

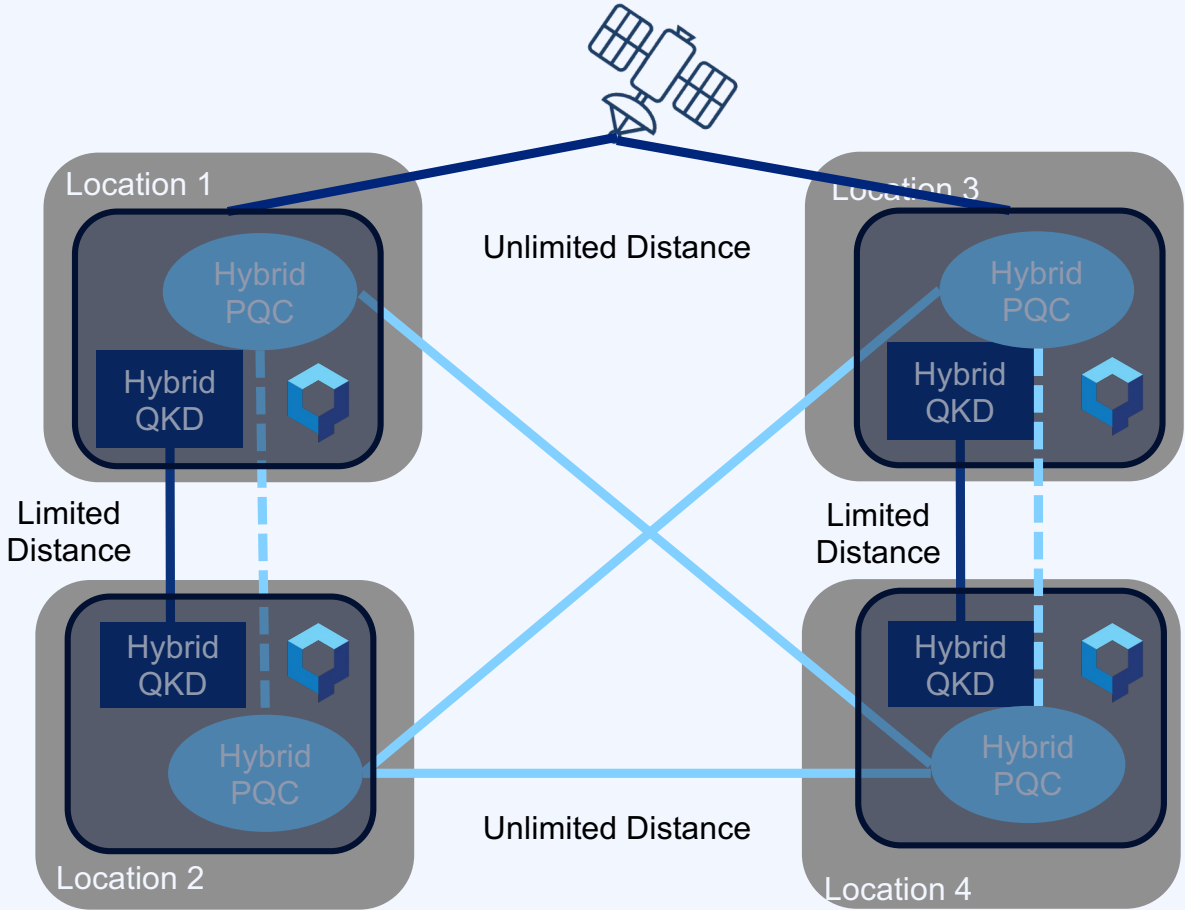


Hybrid offers Redundancy

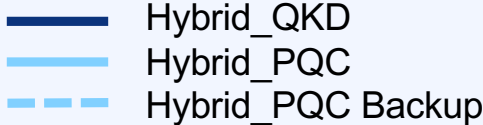
- Backup to QKD



Hybrid offers a Transition Strategy



- As QKD matures, networks can rely more heavily on it
- Satellite QKD is coming!



Security Agencies Recommendations

Hybrid Allowed/Recommended:



Bundesamt
für Sicherheit in der
Informationstechnik



While PQC algorithms are still undergoing analysis to identify potential vulnerabilities, agencies advise pairing them with classical encryption to avoid reliance on any single method.

Hybrid NOT Allowed/Recommended:



National Cyber
Security Centre
a part of GCHQ

Hybrid solutions make the implementation more complex. More security products fail due to implementation or configuration errors than failures in their underlying cryptographic algorithms.

BasejumpQDN integrates into standard protocols and infrastructure

Examples of Protocols Accepting PSKs

Layer / Function	Protocol
Physical layer	OTNSec
Link layer	MACsec (IEEE 802.1AE)
Network layer	IPsec (RFC 4301)
Transport layer	TLS 1.3 (RFC 8446, RFC 8773)
	DTLS 1.3 (RFC 9147)
	SRTP (RFC 3711)
	SSH (RFC 4253)
Application layer	CMS (RFC 5652)
Key exchange	IKEv2 (RFC 7296, RFC 8784)
	GDOI (RFC 6407)

Network OEM Integrations



QKD Device Integrations

ID Quantique
Toshiba
KETS
LuxQuanta

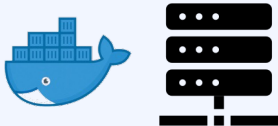
QTI
Think Quantum
Quintessence Labs
... and more!

BasejumpQDN provides flexibility for deployments

Deployed at each end point, one instance can serve multiple applications



HSM Hardware
available from evolutionQ



Software
to be deployed on a local server

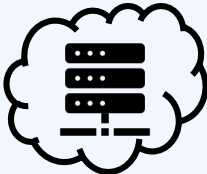


Custom SDK
for integrated or further hardened solutions

Minimum one per deployment, 2 instances recommended for redundancy



KDH
(optional for QKD-only)



"As-a-Service"
run by evolutionQ



"As-a-Service"
run by a service provider



Local Instance
run on an HSM/own infrastructure

BasejumpQDN achieves the design Goals set out

Adding Cryptographic Resiliency...

- Quantum-Safe
 - ✓ *All keys used are based on quantum-safe technologies*
- Cryptographic Agility
 - ✓ *External key agent provides separation of cryptographic implementations and end application, allowing for faster changes*
 - ✓ *E.g., changing the key agent without requiring re-certification of router OS*
- Defence In Depth
 - ✓ *Provides hybrid keys by default*
 - ✓ *Allows integration of PQC and QKD*
- Long Term Security
 - ✓ *All keys include material that is not math-based*

... in a way that can be operationalized

- Integrates to existing infrastructure
 - ✓ *Leverages RFCs to provide PSKs to infrastructure*
 - ✓ *Integrated with Nokia, Cisco, Juniper, Fortinet, etc.*
- Scalable
 - *1-to-many architecture with KDHs*
 - *No distance limitations, need for new fiber optics*
- Cost Effective
 - ✓ *Key agents can be run on servers or 'lite' HSMs*
 - ✓ *Cloud deployment model for low cost POCs/Trials*
- Adaptable over time
 - ✓ *Upgrades with QKD are seamless to the applications*



Thank you!