Building Quantum-safe Networks

Enhancing Security with Symmetric Key Distribution, QKD, and PQC

Melchior Aelmans

Global Service Provider Architecture / Quantum Lead

Juniper Networks

Driven by Experience™

Forward-Looking Statements

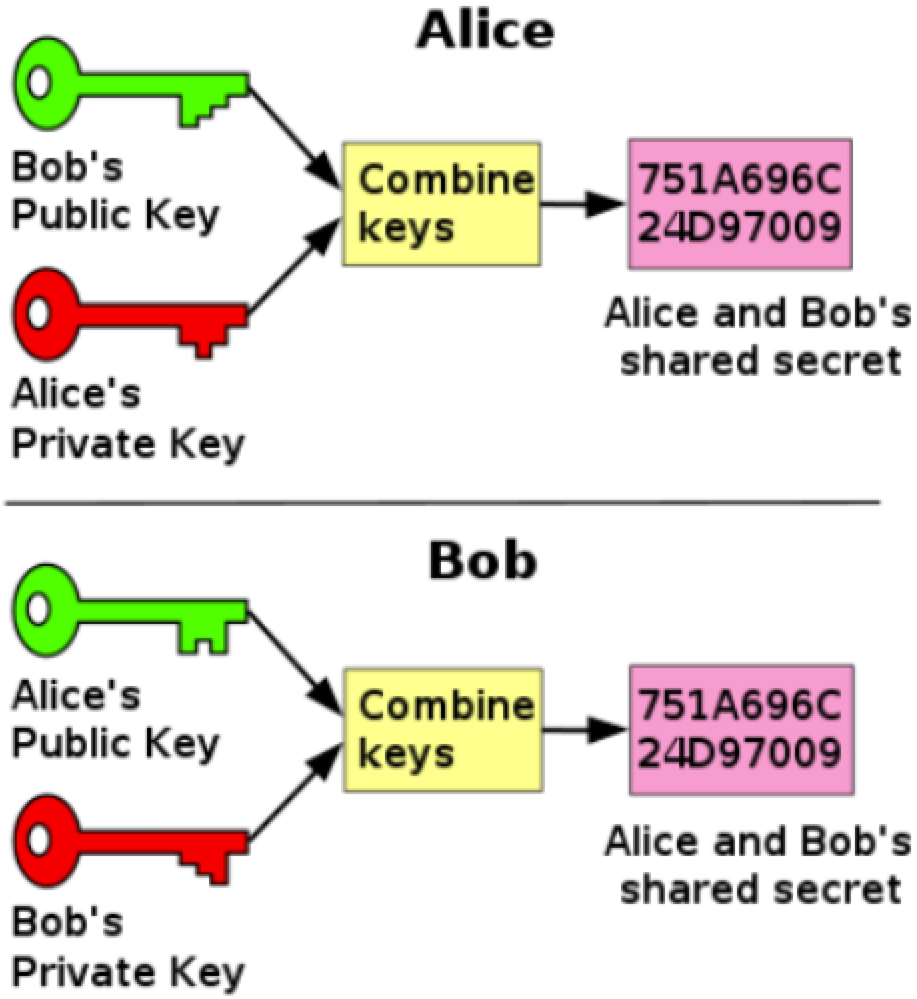
This presentation contains forward-looking statements within the meaning of Section 27A of the Securities Act of 1933, as amended, and Section 21E of the Securities Exchange Act of 1934, as amended, which statements involve substantial risks and uncertainties. Except for historical information contained herein, all statements could be deemed forward-looking statements, including, without limitation, Juniper Networks' views concerning our business, economic and market outlook; our expectations with respect to market trends; our product development; the strength of certain use-cases and customer segments; the introduction of future products; the strength of our solution portfolio; the timing of recovery from COVID-19 on customer demand and resolution of supply challenges; and overall future prospects.

Actual results or events could differ materially from those anticipated in those forward-looking statements as a result of several factors, including: general economic and political conditions globally or regionally; the duration of the effects of the COVID-19 pandemic; business and economic conditions in the networking industry; changes in the financial stability of and overall technology spending by our customers; the network capacity requirements of our customers and, in particular, cloud and communication service providers; the timing of orders and their fulfillment; manufacturing and supply chain constraints, changes or disruptions in our business operations caused by, among other things, armed conflicts, cyberwarfare, political tensions, natural disasters and climate change; availability of product components; delays in scheduled product availability; adoption of regulations or standards affecting Juniper Networks' products, services or the networking industry; the impact of inflationary pressures; executive orders, tariffs, governmental sanctions, changes in laws or regulations and accounting rules, or interpretations thereof; and other factors listed in Juniper Networks' most recent reports on Form 10-Q and 10-K filed with the Securities and Exchange Commission. These forward-looking statements are not guarantees of future performance and speak only as of the date of this presentation. Juniper Networks undertakes no obligation to update the information in this presentation in the event facts or circumstances subsequently change.

Agenda

- How does the legislative landscape look
- Overview of the evolving legislative landscape
- Key Global Regions and Legislative Developments
- Impact on Encryption Practices
- Navigating the Complexity
- What are the options?

Public Key Cryptography



Problem 1:

- Public key cryptography has a *definitive mathematical link* between the public and (secret) private key.
- Classic computers would take millions/trillions of years to attempt to use the public key to find the associated private key.
- **Shor's Algorithm** can however be used by quantum computers can be used to derive the private key from its public key.

Problem 2:

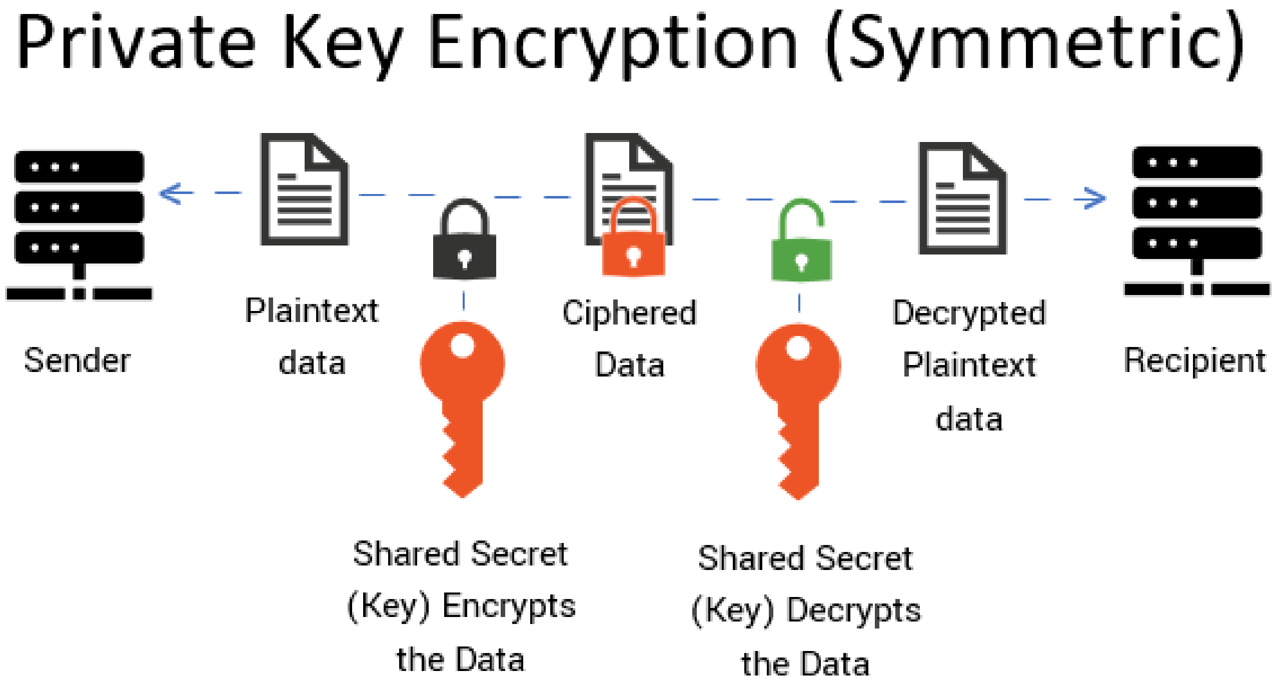
- While powerful enough quantum computers are not available now, the concern/opportunity is in attackers stealing and storing encrypted data to decrypt with the quantum computers of tomorrow.

Conclusion:

- Public Key cryptography as it exists today is not, and cannot, be 'quantum secure'.

By Davidgothberg - Own work, Public Domain, https://commons.wikimedia.org/w/index.php?curid=1028579

SYMMETRIC KEY CRYPTOGRAPHY



- Keys cannot be intercepted.
- No public/private pairs.
- No mathematics in the key creation so cannot be reverse engineered – long random numbers which are unbreakable are the 'essence' of secure symmetric key.
- Quantum Random Number Generator (QRNG) used to derive keys with high entropy.
- Symmetric keys are therefore 'quantum safe'.

However…..

- Symmetric keys are not easily scalable.
- Symmetric keys may be difficult to securely distribute over current communications structure.

Quantum safe – legislation and guidance

- Guidance and legislation appearing around the globe – examples:

- Quantum Computing Cybersecurity Preparedness Act passed in late 2023
- Requires (by law) investigation and creation of plans “on the migration of information technology to post-quantum cryptography”

- Guidance from NCSC focuses on NIST efforts to standardize PQC
- Legislation likely at end of NIST process (2023-2024)

- ENISA whitepapers for progress and current mitigation recommendations available now
- No EU-wide legislation
- Local governments start to demand the use of symmetric key distribution and quantum resistant algorithms

How does the legislative landscape look

Countries with General right to use encryption

Finland

In Finland, everyone has the right to protect their communications and identification information how the wish, using any technical possibilities available, unless otherwise provided by law.

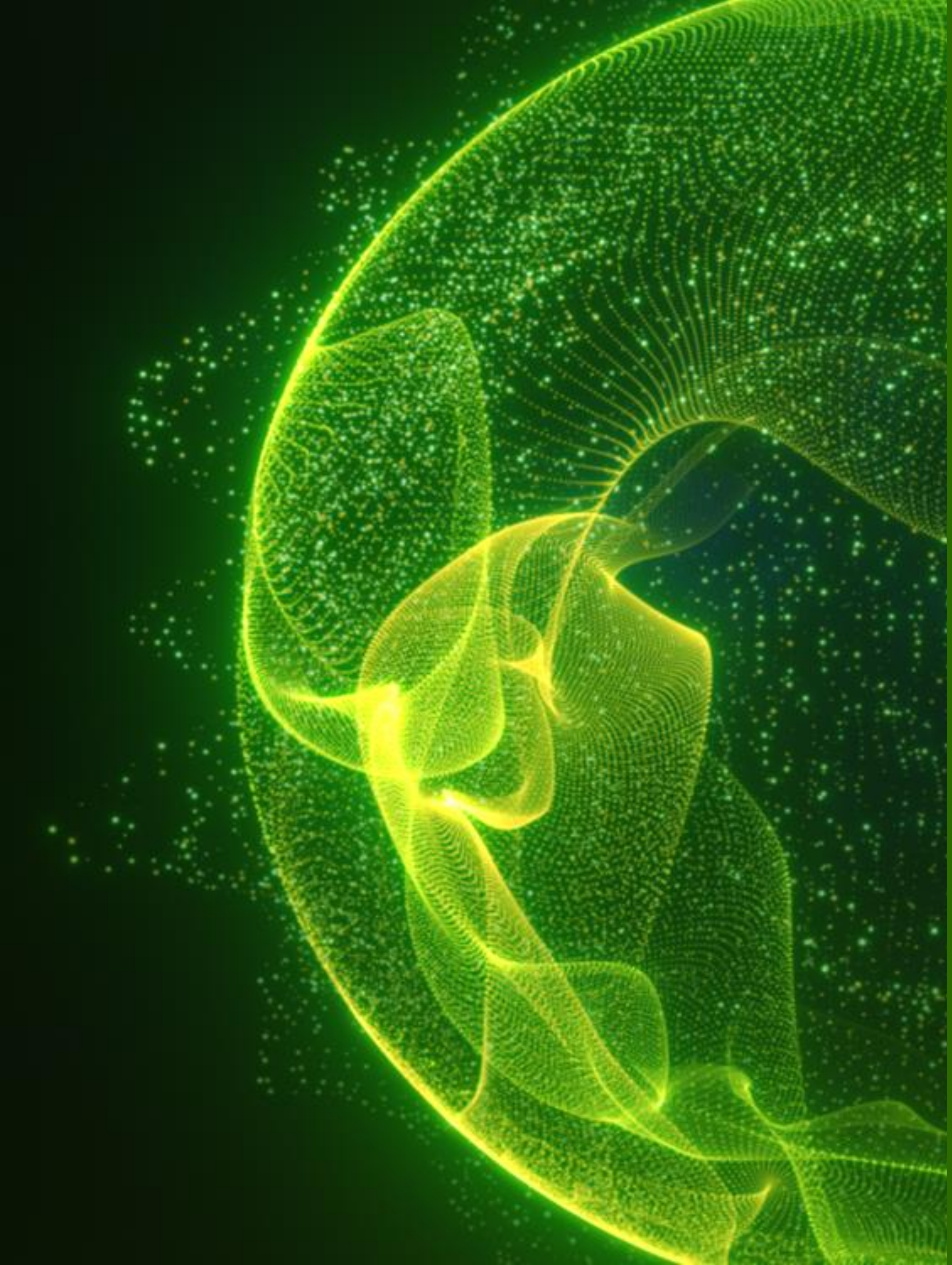
Source: https://www.gp-digital.org/world-map-of-encryption/

Countries with laws and policies that force providers to assist authorities

Finland

The law requires anyone to hand over passwords and decryption keys if it is necessary to conduct a search of data contained in a device during the course of a criminal investigation.

Source: https://www.gp-digital.org/world-map-of-encryption/



Overview of the evolving legislative landscape

Overview of the Evolving Encryption Legislative Landscape in the EU (1/2)

- **General Data Protection Regulation (GDPR):**
  - Implemented in 2018, GDPR set a high standard for data protection and privacy in the EU.
  - Requires encryption for sensitive data as a security measure.
  - Imposes strict penalties for non-compliance (up to 4% of annual revenue).
- **E-Privacy Regulation (Upcoming):**
  - Will complement GDPR, focusing on confidentiality in electronic communications.
  - Encryption of communications data is a key feature.
  - Challenges remain in balancing privacy rights with government surveillance needs.

Overview of the Evolving Encryption Legislative Landscape in the EU (2/2)

- **NIS2 Directive (Network and Information Security Directive):**
  - Adopted on 16 January 2023 and Member States have until 17 October 2024 to transpose its measures into national law.
  - Expands the scope of sectors required to meet cybersecurity standards, including encryption.
  - Focuses on improving incident response, risk management, and the security of critical infrastructure.
  - Requires organizations to implement robust encryption measures to protect against cyber threats.
- **Digital Markets Act (DMA) & Digital Services Act (DSA):**
  - Both aim to regulate large digital platforms, pushing for transparency in encryption protocols.
  - Focus on protecting users from cyber threats while respecting privacy.
- **Law Enforcement and Encryption:**
  - Ongoing debate over “backdoors” in encryption for law enforcement.
  - EU governments are divided on allowing access to encrypted communications for crime prevention.

A Secure a Post-Quantum Cryptography Future

- Though a quantum computer powerful enough to break current forms of cryptography does not yet exist, the Biden-Harris Administration is preparing for and mitigating the risks to government and critical infrastructure systems posed by a potential future quantum computer. - White House
- By December 31, 2023, agencies maintaining NSS shall implement symmetric-key protections (e.g., High Assurance Internet Protocol Encryptor (HAIPE) exclusion keys or VPN symmetric key solutions) to provide additional protection for quantum-vulnerable key exchanges, where appropriate. - National Security Memorandum Biden Administration

BSI: Use of Quantum-Safe Mechanisms

- It is advisable to use quantum-safe mechanisms in the very near future, especially for systems that process data with longer-term protection requirements. These methods should only be used in combination with a classical key derivation method.

Source: https://www.bsi.bund.de/SharedDocs/Downloads/EN/BSI/Publications/TechGuidelines/TG02102/BSI-TR-02102-1.pdf?__blob=publicationFile&v=7

NCSC: Preparing for Quantum-Safe Cryptography

- The NCSC expects that major commercial products and services will transition to QSC once NIST standards are available and protocols (IPSec, TLS, etc.) are updated to support QSC.
- For organisations needing long-term cryptographic protection, the NCSC can advise on the deployment of suitable mitigations.
- The NCSC recognises the serious threat that quantum computers pose to long-term cryptographic security. QSC using standards-compliant products is the recommended mitigation for the quantum threat, once such products become available.
- Organisations that manage their own cryptographic infrastructure should note the work of ETSI and NIST on planning QSC transition when making long-term investment decisions.

Source: https://www.ncsc.gov.uk/whitepaper/preparing-for-quantum-safe-cryptography

Impact on Encryption Practices

IETF Cryptographic Dependencies

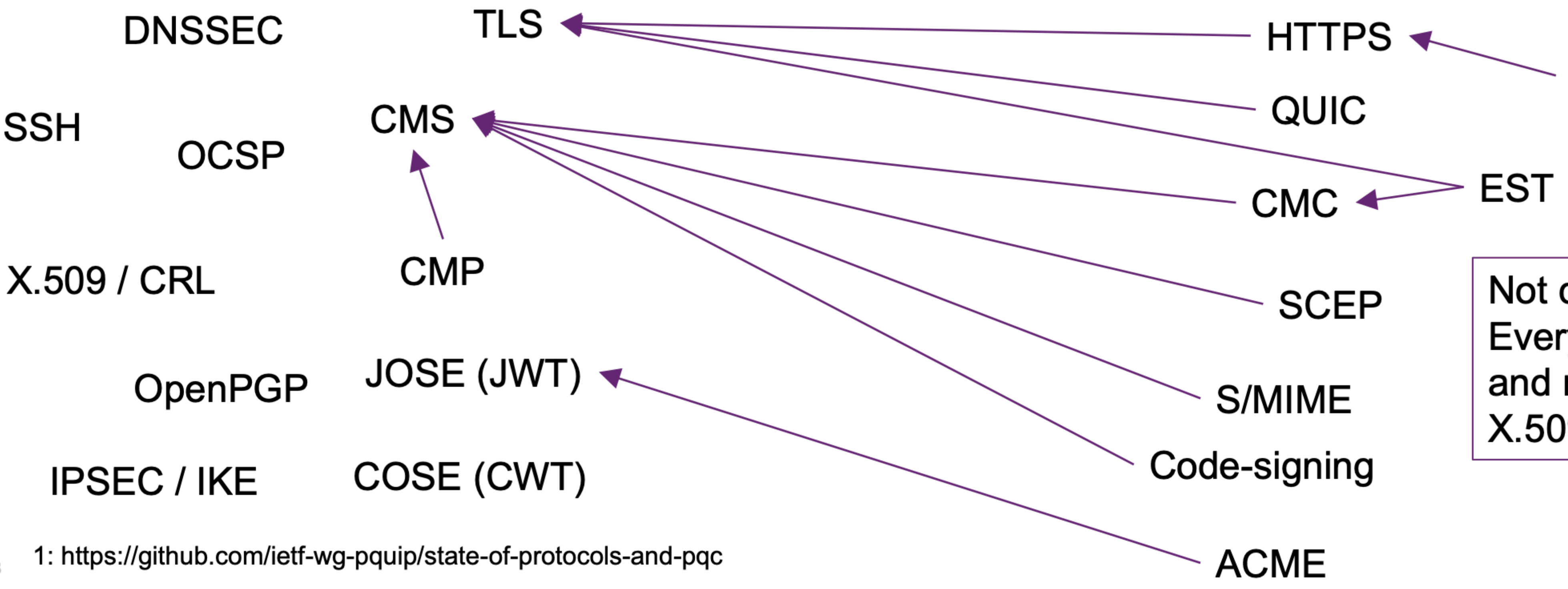
Good news: not everything needs to be touched.

Defines its own crypto

(ie needs updating)

Gets its crypto by embedding another protocol

(ie does not need updating)



Not drawn:
Everything on the right, and most on the left, use X.509 certificates.

1: https://github.com/ietf-wg-pquip/state-of-protocols-and-pqc

So, what is the right way forward?

- Migrating to PQC today - might expose new risks
- Do nothing – data might be decrypted in the future when CRQC is available
- Hybrid approach – best of both but multiple options

Mixing Preshared Keys in the Internet Key Exchange Protocol Version 2 (IKEv2) for Post-quantum Security RFC8784

The possibility of quantum computers poses a serious challenge to cryptographic algorithms deployed widely today.

The Internet Key Exchange Protocol Version 2 (IKEv2) is one example of a cryptosystem that could be broken; someone storing VPN communications today could decrypt them at a later time when a quantum computer is available.

It is anticipated that IKEv2 will be extended to support quantum-secure key exchange algorithms; however, that is not likely to happen in the near term.

To address this problem before then, this document describes an extension of IKEv2 to allow it to be resistant to a quantum computer by using preshared keys.

Internet Engineering Task Force (IETF)
Request for Comments: 8784
Category: Standards Track
Published: June 2020
ISSN: 2070-1721

S. Fluhrer
Cisco Systems
P. Kampanakis
Cisco Systems
D. McGrew
Cisco Systems
V. Smyslov
ELVIS-PLUS

Mixing Preshared Keys in the Internet Key Exchange Protocol Version 2 (IKEv2) for Post-quantum Security

Abstract

The possibility of quantum computers poses a serious challenge to cryptographic algorithms deployed widely today. The Internet Key Exchange Protocol Version 2 (IKEv2) is one example of a cryptosystem that could be broken; someone storing VPN communications today could decrypt them at a later time when a quantum computer is available. It is anticipated that IKEv2 will be extended to support quantum-secure key exchange algorithms; however, that is not likely to happen in the near term. To address this problem before then, this document describes an extension of IKEv2 to allow it to be resistant to a quantum computer by using preshared keys.

And what about MACsec?

- MACsec (Media Access Control Security) can be considered quantum-safe due to its use of AES-256 encryption, which is robust against both classical and quantum attacks.
- AES-256 employs a 256-bit key size, providing an immense key space that is infeasible to break with current or foreseeable computing capabilities, including quantum computers.
- AES-256 remains resistant to these attacks due to its symmetric key nature.
- “Only” thing needed is a quantum-safe Key Exchange/Distribution method.

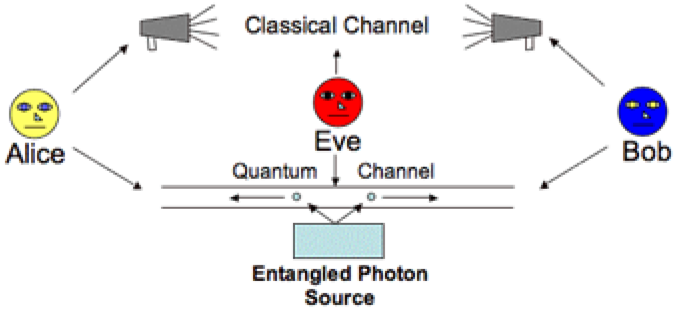
What are the options?

Secure Key Exchange Options

Post-Quantum Cryptographic Algorithms

- Standardization of new 'quantum resistant' crypto algorithms in the works
- May be vulnerable against "classical computer" attack
- Selection process finalized

Quantum Key Distribution (QKD)

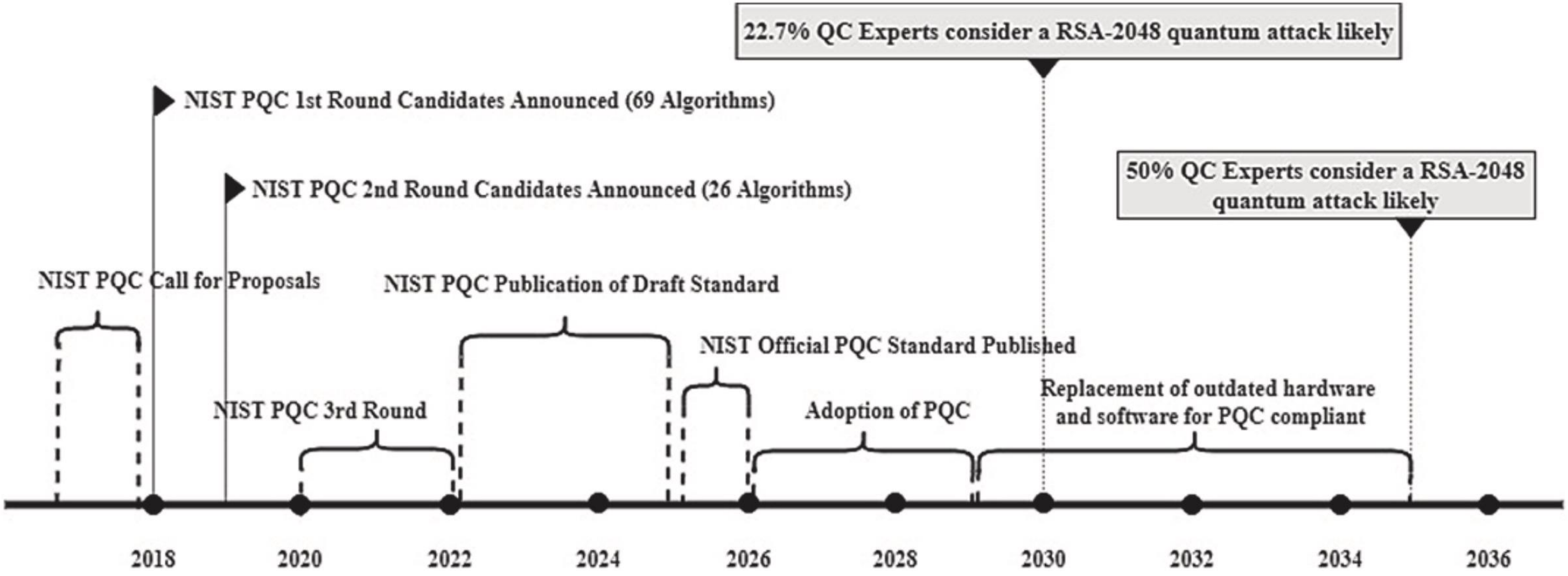


- Hardware based
- Uses photon properties to generate secure keys
- Limited range (for now)
- Point-to-Point (for now)

Symmetric Key Establishment

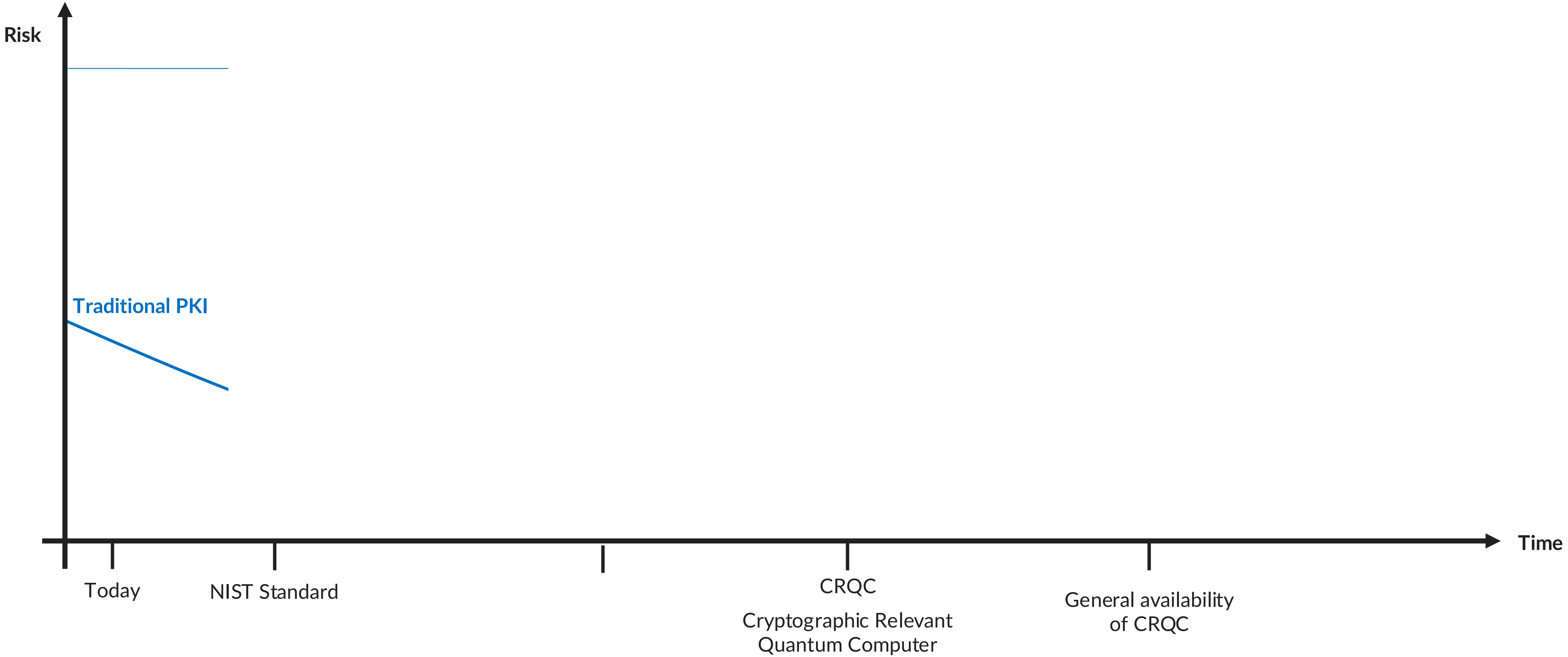
- Add an additional secret to symmetric key material based on long random number
- Otherwise uses normal IKE/IPsec standards
- Key distribution mechanism not standardized (yet)

NIST PQC Timeline



Source: https://www.sciencedirect.com/science/article/pii/S2590005622000777

The Issue with introducing pQC

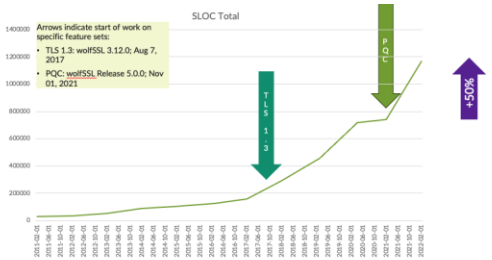


Post-Quantum Cryptography and the Grain of Salt

Resistance against digital computer attacks?

Belgian researchers have cracked a final-round candidate that the U.S. National Institute of Standards and Technology (NIST) was evaluating for its Post-Quantum Cryptography (PQC) standard.
Research experts broke the SIKE algorithm in about 62 minutes according to their article, An Efficient Key Recovery Attack On SIDH.

Implementation Complexity



- Source Code to implement new Algorithms is substantial (+50% increase over existing code)
- Even well tested code can have ~1 defect / 2000 Lines of Code
- Implementation complexity can add vulnerability can also uncover existing vulnerabilities

Large Key Size

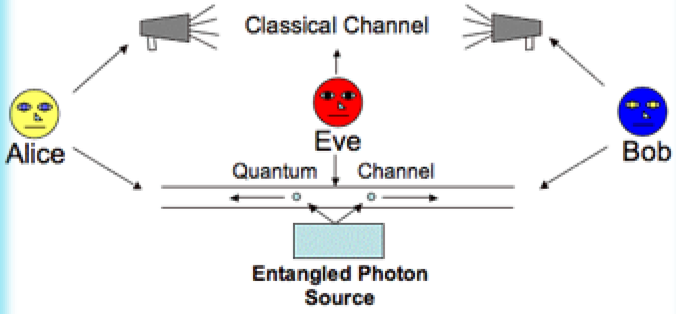
- Leveraging a PQC Algorithm significantly increases the key sizes and the ciphertext/ signature sizes compared to traditional Signatures.
- How much more memory, compute power, latency is needed?

QUANTUM CRYPTOGRAPHY – Multiple Options

Post-Quantum Cryptographic Algorithms

- Standardization of new ‘quantum resistant’ crypto algorithms in the works
- May be vulnerable against “classical computer” attack
- Selection process finalized

Quantum Key Distribution (QKD)



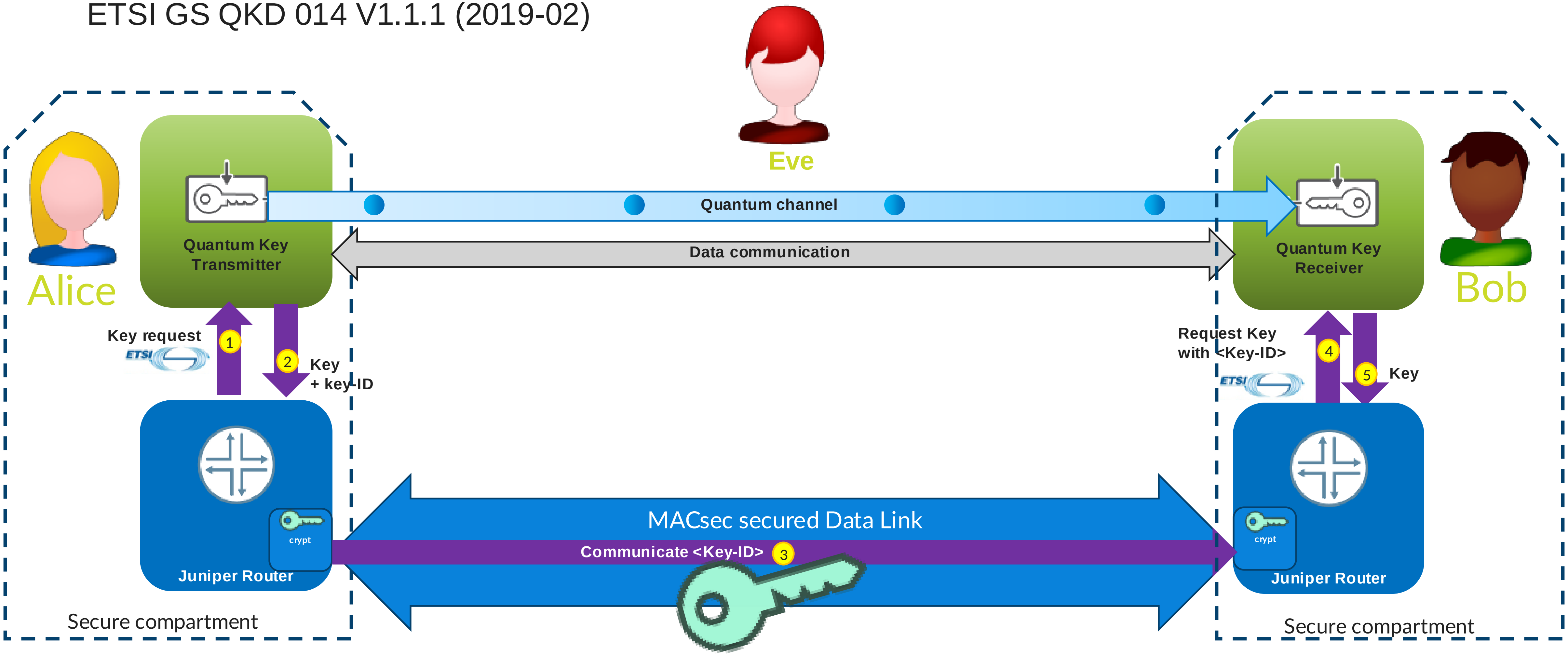
- Hardware based
- Uses photon properties to generate secure keys
- Limited range (for now)
- Point-to-Point (for now)

Symmetric Key Establishment

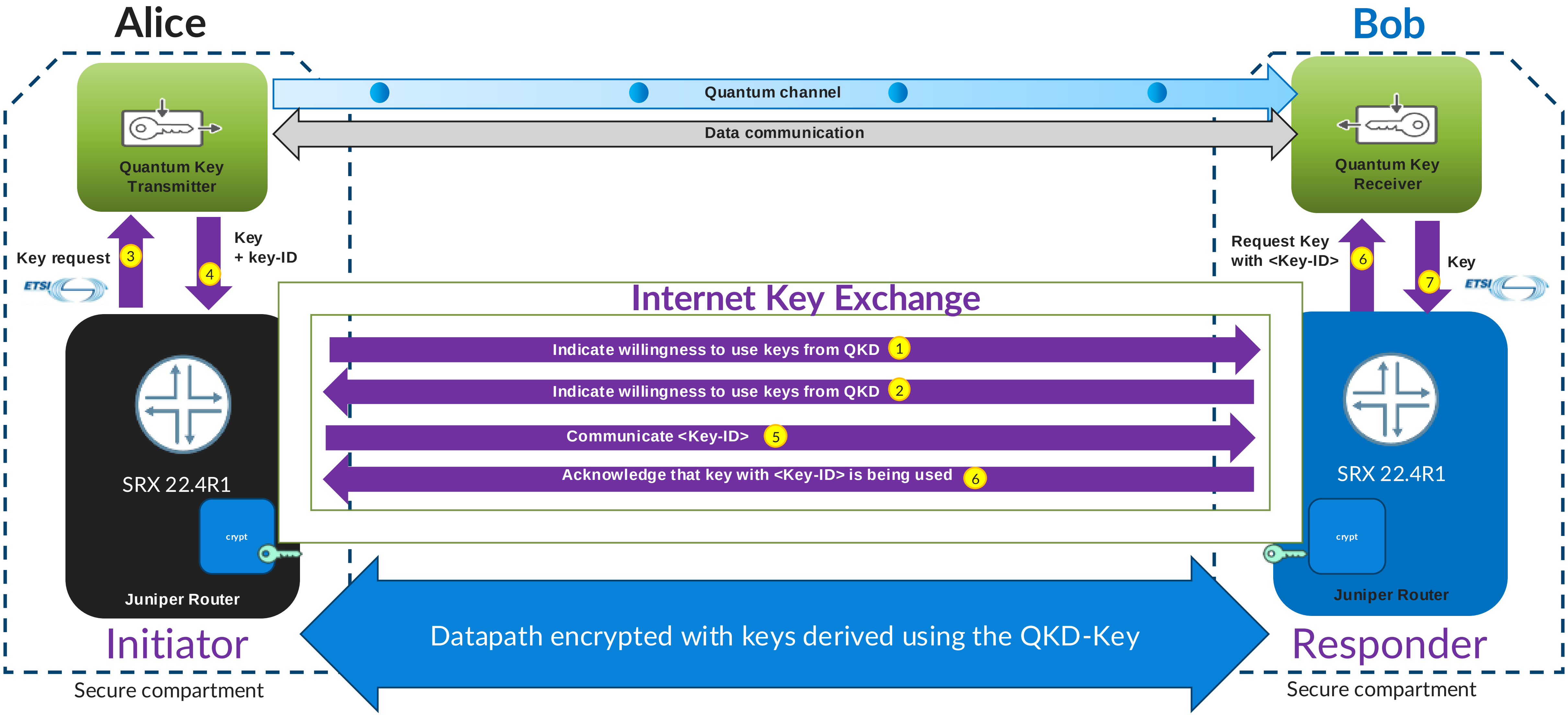
- Add an additional secret to symmetric key material based on long random number
- Otherwise uses normal IKE/IPSec standards
- Key distribution mechanism not standardized (yet)

QKD in MACsec with ETSI-QKD

Quantum Key Distribution (QKD); Protocol and data format of REST-based key delivery API
ETSI GS QKD 014 V1.1.1 (2019-02)



QKD in IPsec (IKEv2 negotiation), RFC8784



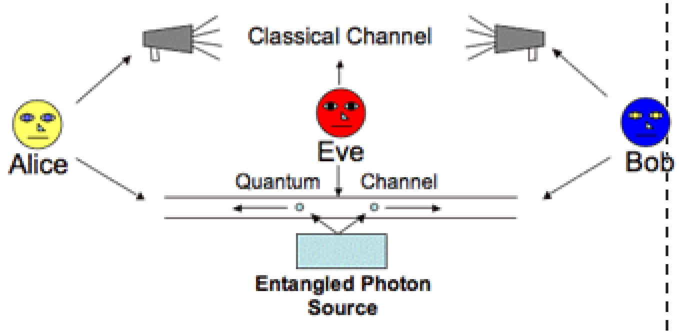
SRX1500|SRX4200|SRX4600|SRX5400|SRX5600|vSRX3.0 [IETF RFC 8784]

Quantum Cryptography – Multiple Options

Post-Quantum Cryptographic Algorithms

- Standardization of new ‘quantum resistant’ crypto algorithms in the works
- May be vulnerable against “classical computer” attack
- Selection process finalized

Quantum Key Distribution (QKD)

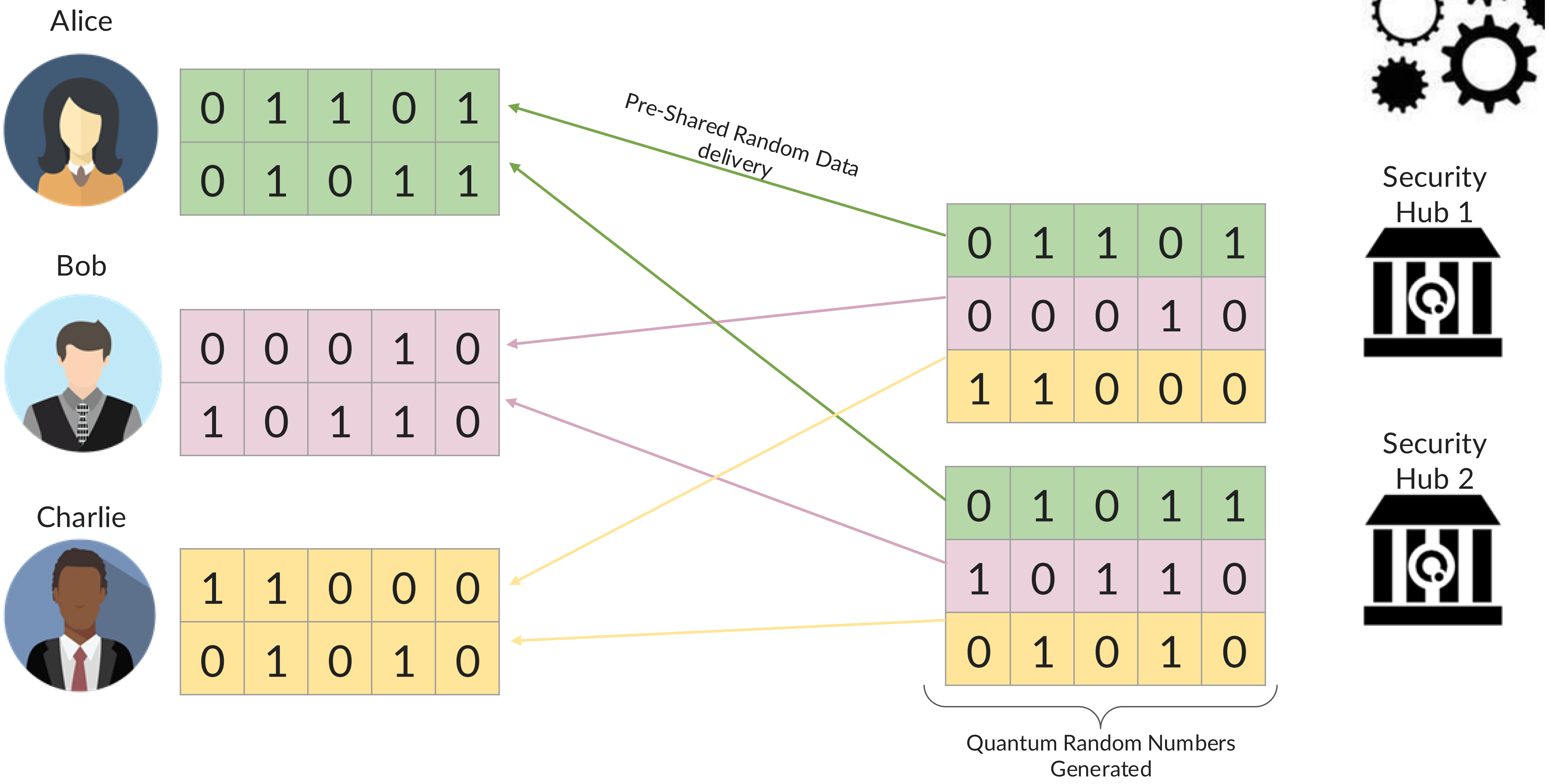


- Hardware based
- Uses photon properties to generate secure keys
- Limited range (for now)
- Point-to-Point (for now)

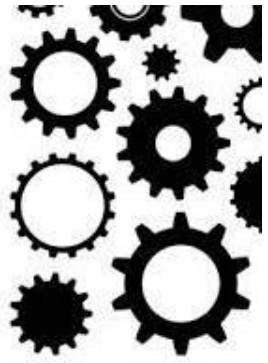
Symmetric Key Establishment

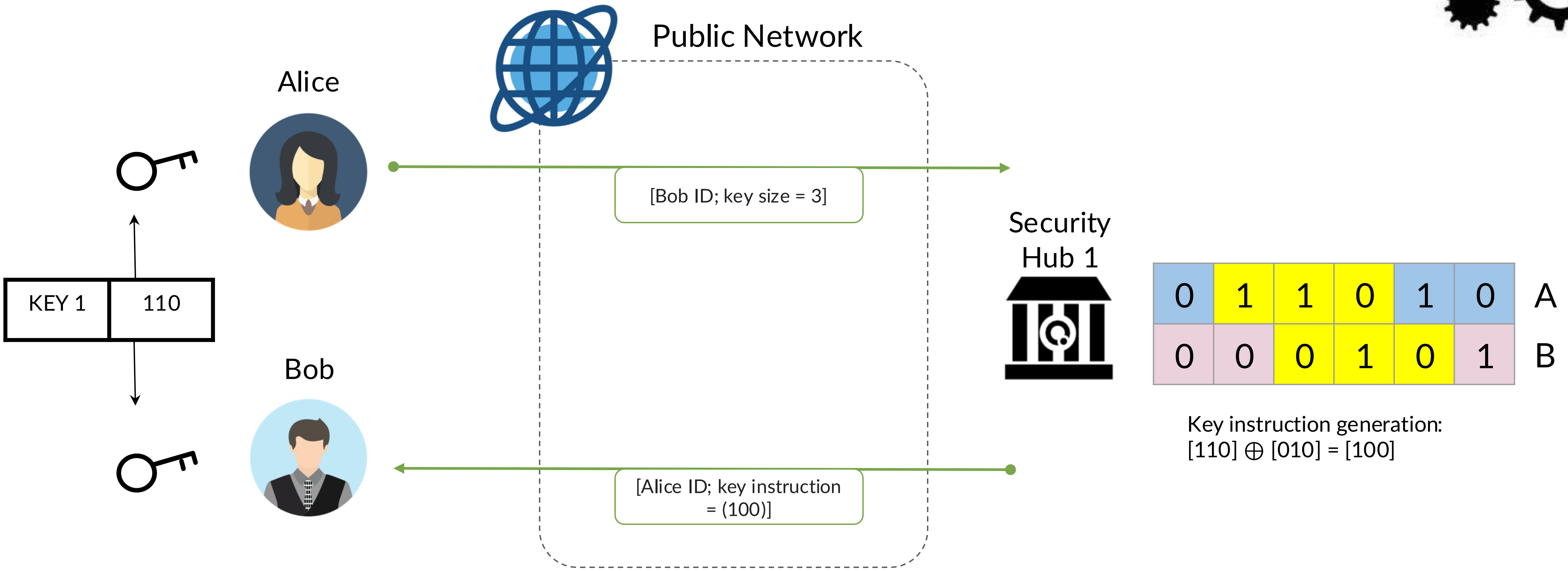
- Add an additional secret to symmetric key material based on long random number
- Otherwise uses normal IKE/IPSec standards
- Key distribution mechanism not standardized (yet)

DSKE Setup Phase

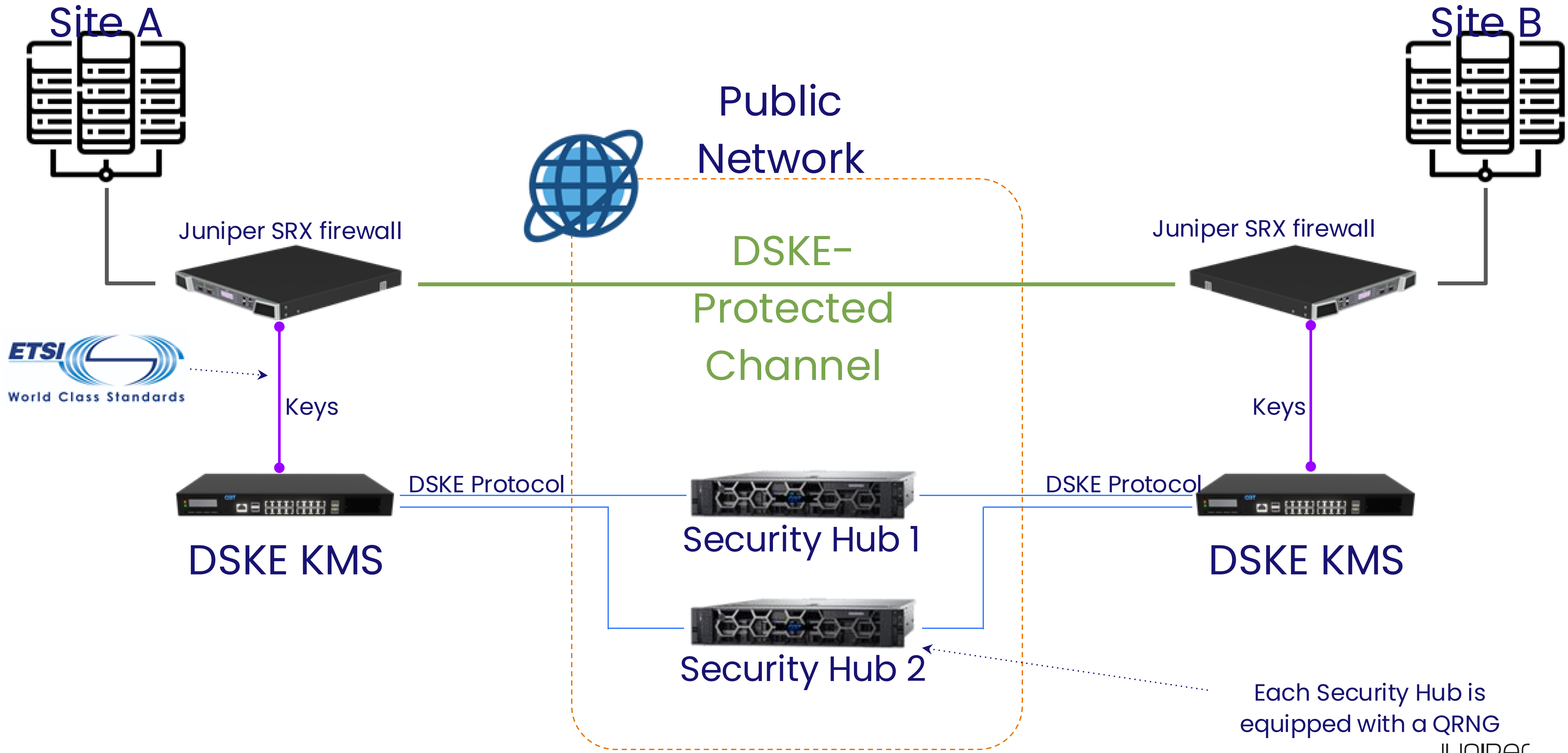


DSKE – Key Creation

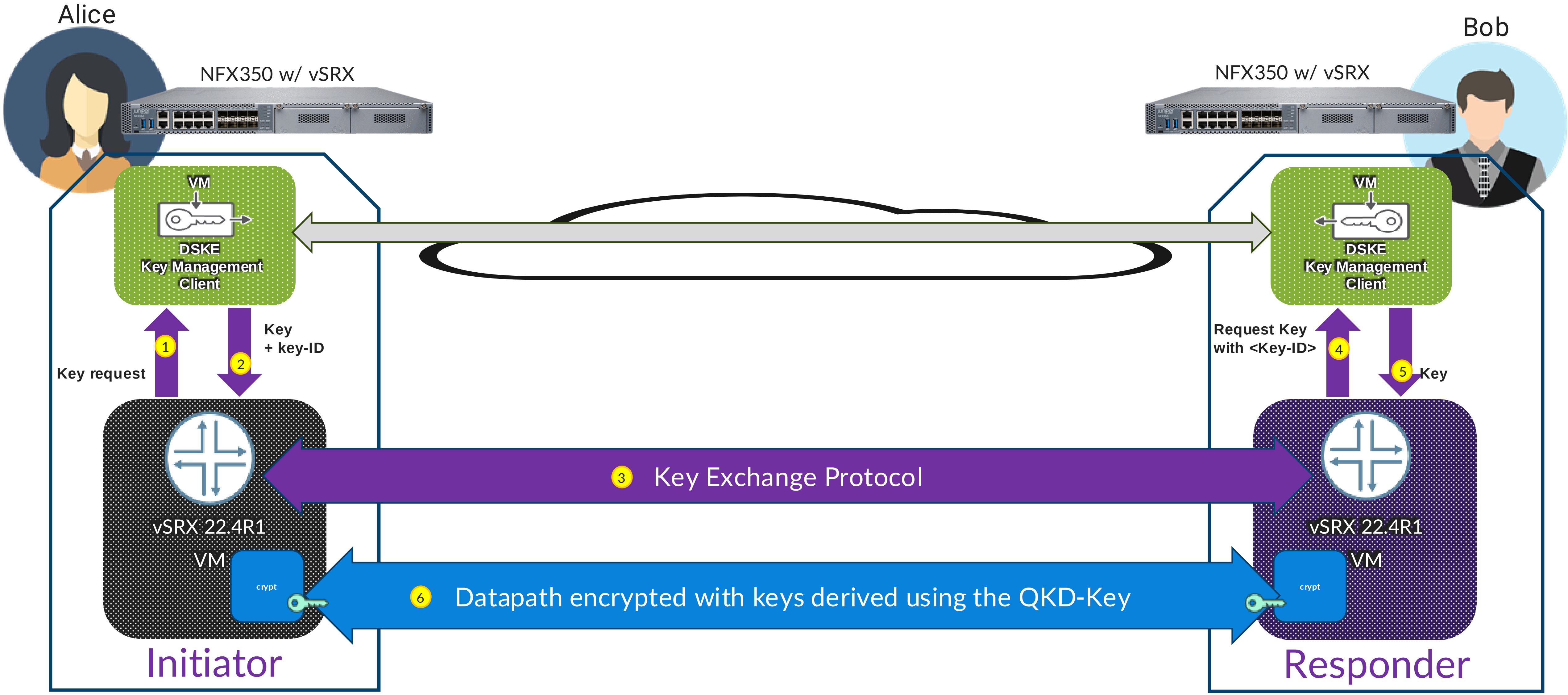




Quantum Bridge - Distributed Symmetric Key Exchange



Symmetric Key Distribution
Secure virtualized environment using Juniper NFX



Conclusion

- Encryption Legislation might sound boring, but it could have quite some impact for operators.
- There are options available already today to protect sensitive data against attacks in the future.
- Start building knowledge on the subject. The CRQC might be there sooner ten we know today.
- Think about the value of your data in 5-10-20 years and take appropriate measurements.
- Ask your vendors how they can help you prepare again future attacks.
- Read, follow, co-author IETF drafts and RFC (sounds boring as well but great way to learn and influence).

Thank you

JUNIPER NETWORKS