Quantum-Safe Encryption for IKEv2/IPsec

Using RFC8784 and Cisco SKIP

Ajay Pandey, Product Manager, Enterprise Routing Group
Amjad Inamdar, Principal Engineer, Enterprise Routing Group

21st June 2023

Quantum-Safe Encryption : Problem and Solution

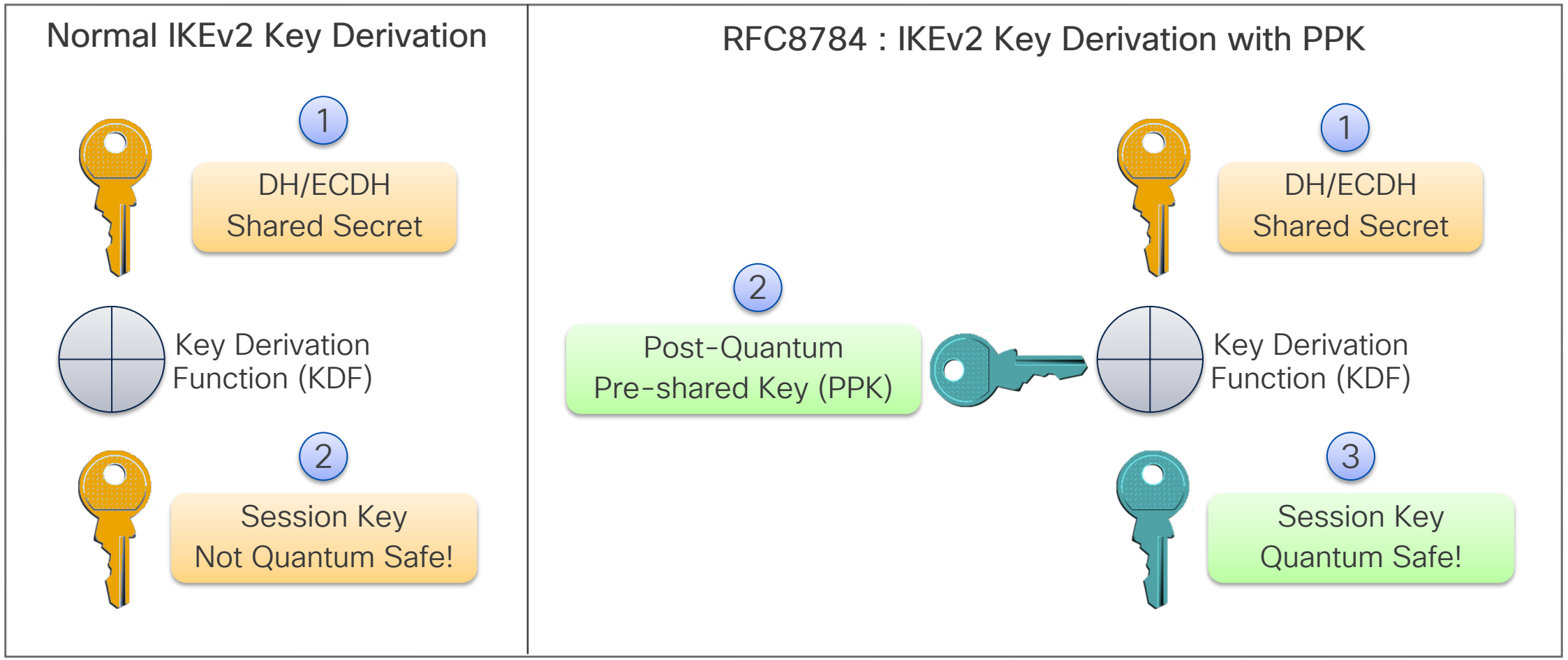
Problem Statement

- Asymmetric crypto based on mathematical problems e.g., prime factorization
- Quantum computers would break crypto algorithms e.g., https://www.technologyreview.com/2019/05/30/65724/how-a-quantum-computer-could-break-2048-bit-rsa-encryption-in-8-hours/
- Sensitive data susceptible to '*Store now, decrypt later*'

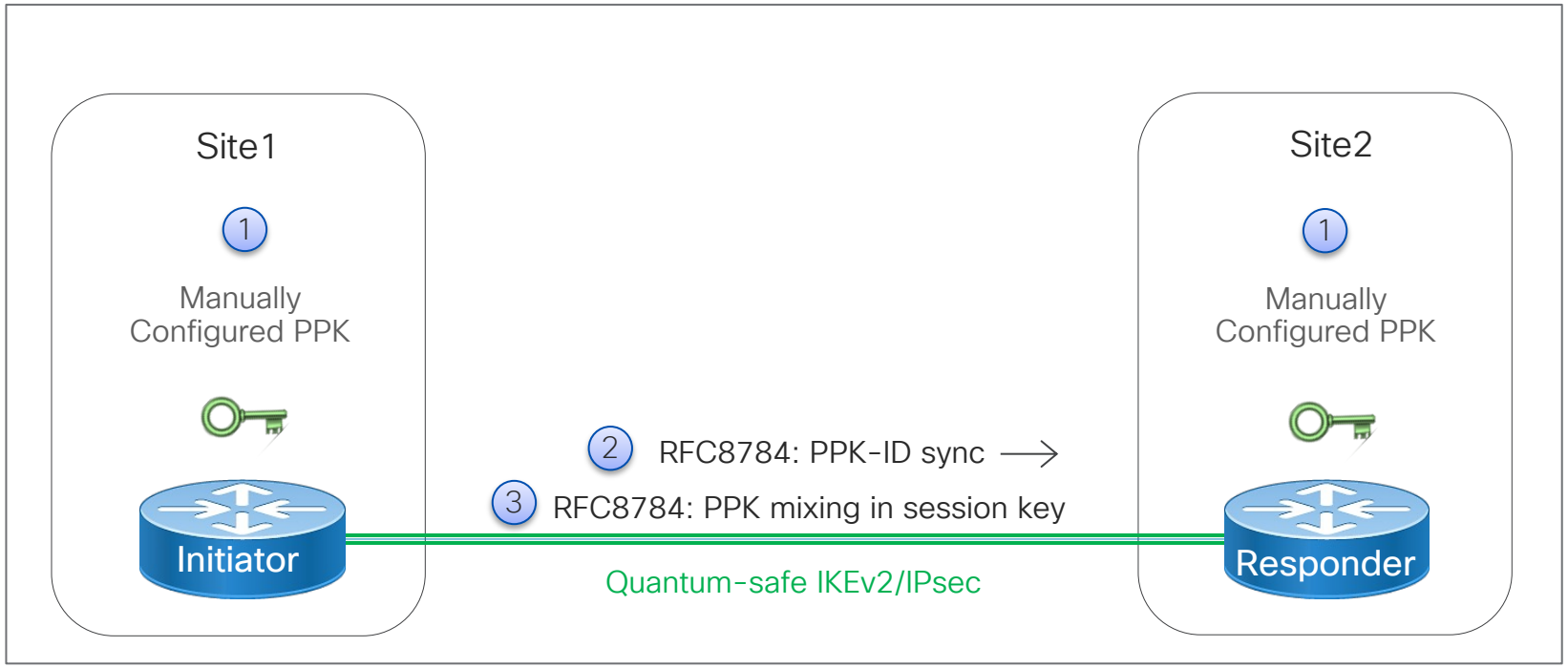
Solution

- Introducing Quantum-Safe Encryption based on RFC8784
- Post-Quantum Pre-shared key (PPK) options:
  - **Manual PPK**: PPK configured on the device
  - **Dynamic PPK**: PPK imported on the device from external key source
- Available from IOS XE 17.11: http://www.cisco.com/content/en/us/td/docs/routers/ios/config/17-x/sec-vpn/b-security-vpn/m-sec-cfg-quantum-encryption-ppk.html

IKEv2 Session Key Derivation

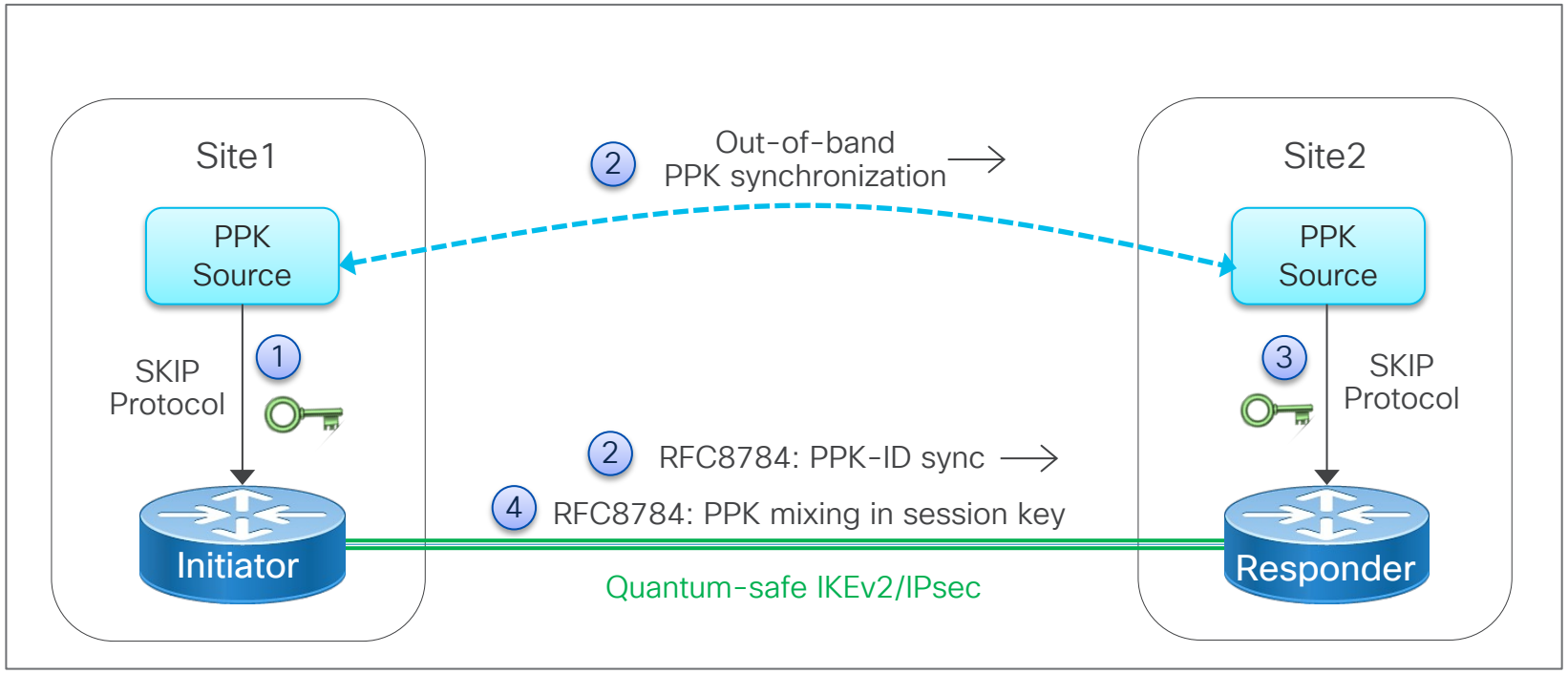


Quantum-Safe Encryption with Manual PPK



Refer : https://www.cisco.com/c/en/us/td/docs/routers/ios/config/17-x/sec-vpn/b-security-vpn/m-sec-cfg-quantum-encryption-ppk.html#manual-pre-shared-keys

Quantum-Safe Encryption with Dynamic PPK



Refer : https://www.cisco.com/c/en/us/td/docs/routers/ios/config/17-x/sec-vpn/b-security-vpn/m-sec-cfg-quantum-encryption-ppk.html#cisco-secure-key-integration-protocol-and-dynamic-ppk

Thank You !