Post-Quantum Cryptography (PQC) Without Compromising Performance

World Leading Network Solutions by Arqit and Intel

Divya Pendyala
Cloud Software Architect at Intel

Dr. Michael Murphy
Deputy Chief Technology Officer at Arqit

Phil Burn
Solution Architect at Arqit

Date: Apr 30, 2024
Time: 9AM PDT / 12PM EDT

intel network builders partner

Post-Quantum Cryptography (PQC) Without Compromising Performance: World Leading Network Solutions by Arqit and Intel

Dr Michael Murphy, Deputy Chief Technology Officer

April 30th 2024

Data is at risk *today*

1 Store now, decrypt later

A serious and current threat to the long-term secrecy of information

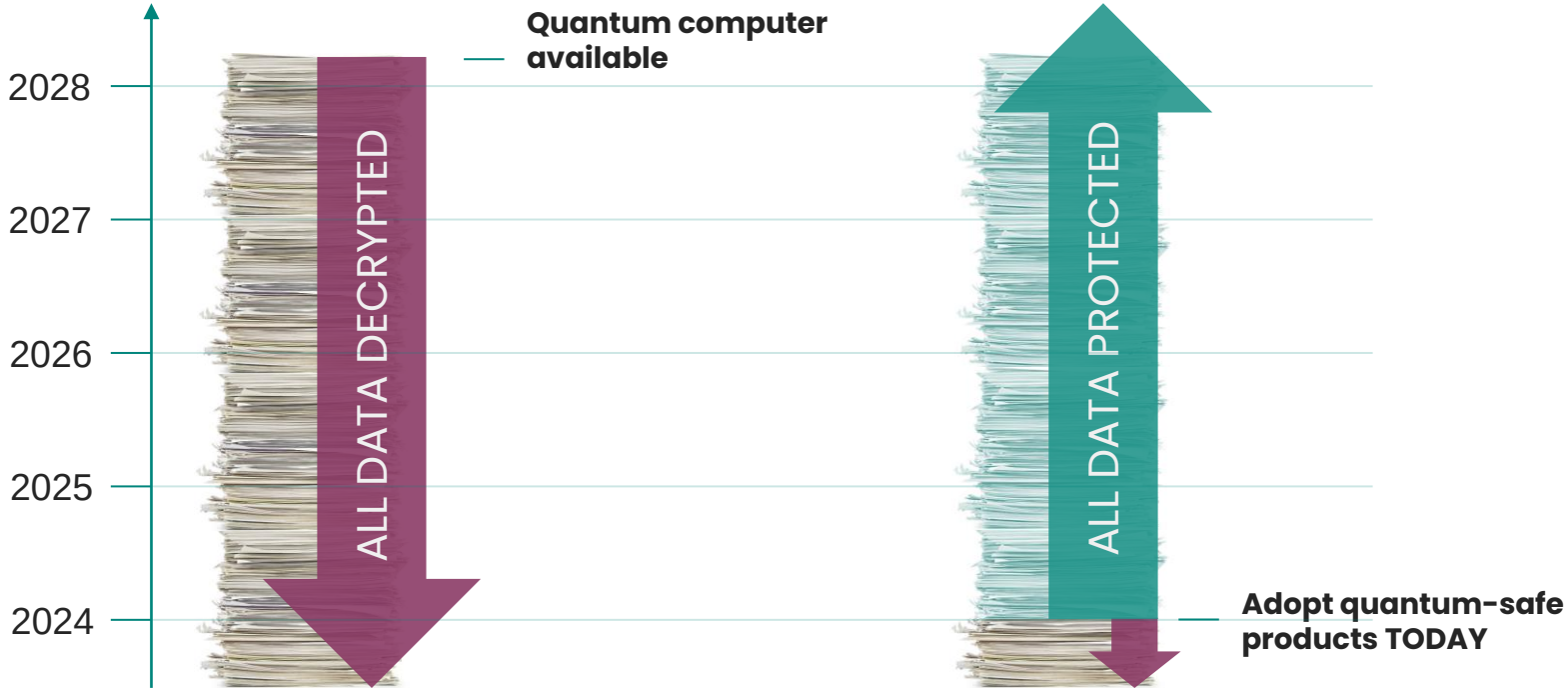
2 Scaling issues

Achieving high performance without compromising security

3 Standardisation

New standards are slow to adopt and hard to verify in the short term

Store now, decrypt later

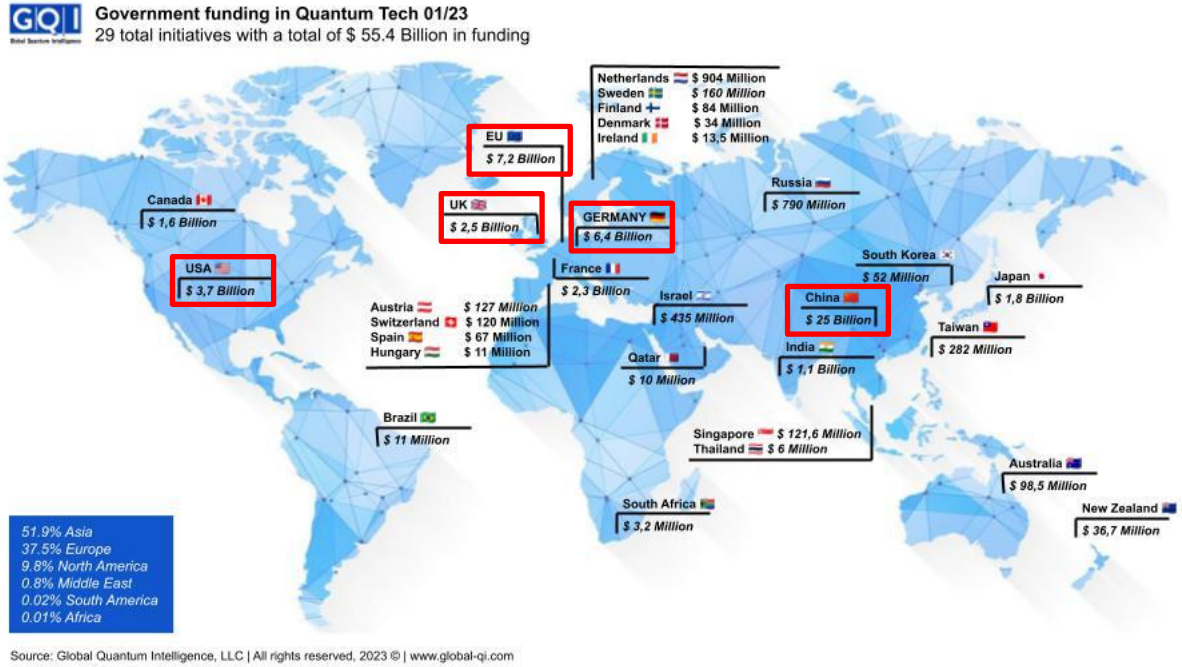


Stronger, simpler encryption

ARQIT

How far are we from a quantum computer?

Best estimates predict between 5–15 years



China: $25.0b

EU: $7.2b

Germany: $6.4b

USA: $3.7b

UK: $2.5b

Stronger, simpler encryption

ARQIT

Recent advancements in quantum computing

Microsoft, Quantinuum claim breakthrough in quantum computing

By **Stephen Nellis**

April 3, 2024 10:11 PM GMT+1 · Updated 5 days ago

A view shows a Microsoft logo at Microsoft offices in Issy-les-Moulineaux near Paris, France, March 25, 2024. REUTERS/Gonzalo Fue
Photo *Purchase Licensing Rights*

April 3 (Reuters) - Microsoft (MSFT.O) and Quantinuum on Wednesday said they have achieved a step in making quantum computers a commercial reality by making them more reliable.

Landmark IBM error correction paper published on the cover of Nature

IBM has created a quantum error-correcting code about 10 times more efficient than prior methods — a milestone in quantum computing research.

27 March, 2024

Stronger, simpler encryption

ARQIT

The threat is recognized today…

December 2023, U.S. National Security Agency Cybersecurity Year in Review

December 2022, U.S. Congress, Quantum Computing Cybersecurity Preparedness Act

White House National Security Memorandum 10 May 4, 2022

> *"Within three to seven years, quantum computers will be able to crack the algorithms behind the encryption keys that protect our data and the internet's infrastructure."*

Richard Watson
EY Global Cybersecurity Consulting Leader
Quantum computing: 5 steps to take now. Nov 21st 2022

January 2024, IBM
(https://www.ibm.com/quantum)

How prepared is your organisation to tackle the threat posed by quantum computers?

1 We are not prepared at all.

2 We are slightly prepared.

3 We are mostly prepared.

4 We are fully quantum resilient.

Stronger, simpler encryption

ARQIT

Arqit SKA™–Platform is a quantum-safe security product

Dynamic PPKs/PSKs

Compatible with pre-shared key mechanisms and can be mixed with PKI

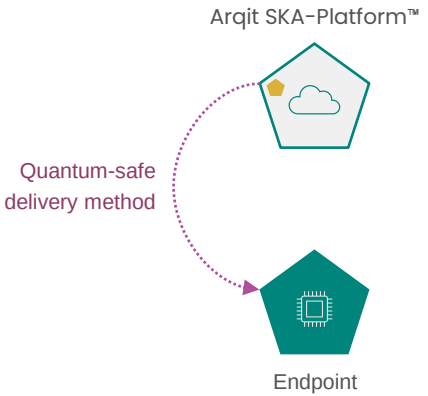
Scalable & flexible

Global cloud-based service which is easy to scale and lightweight at the endpoint

Standards-based

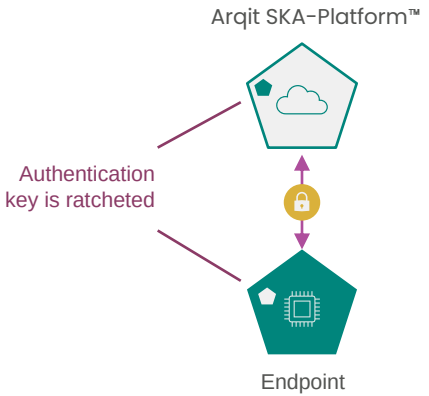
Uses existing strong, standardised cryptography tested over decades

Provisioning, authentication, and key agreement



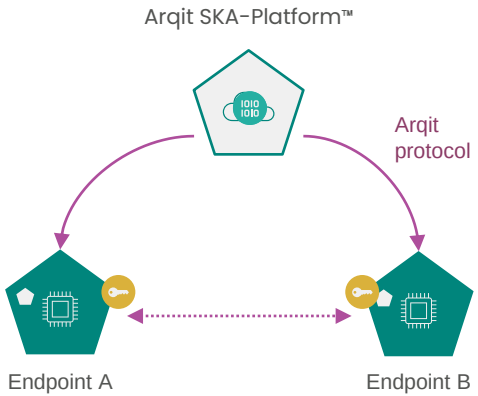
1

Every endpoint is securely provisioned once with a “bootstrap” key



2

Endpoints strongly, mutually authenticate with perfect forward secrecy



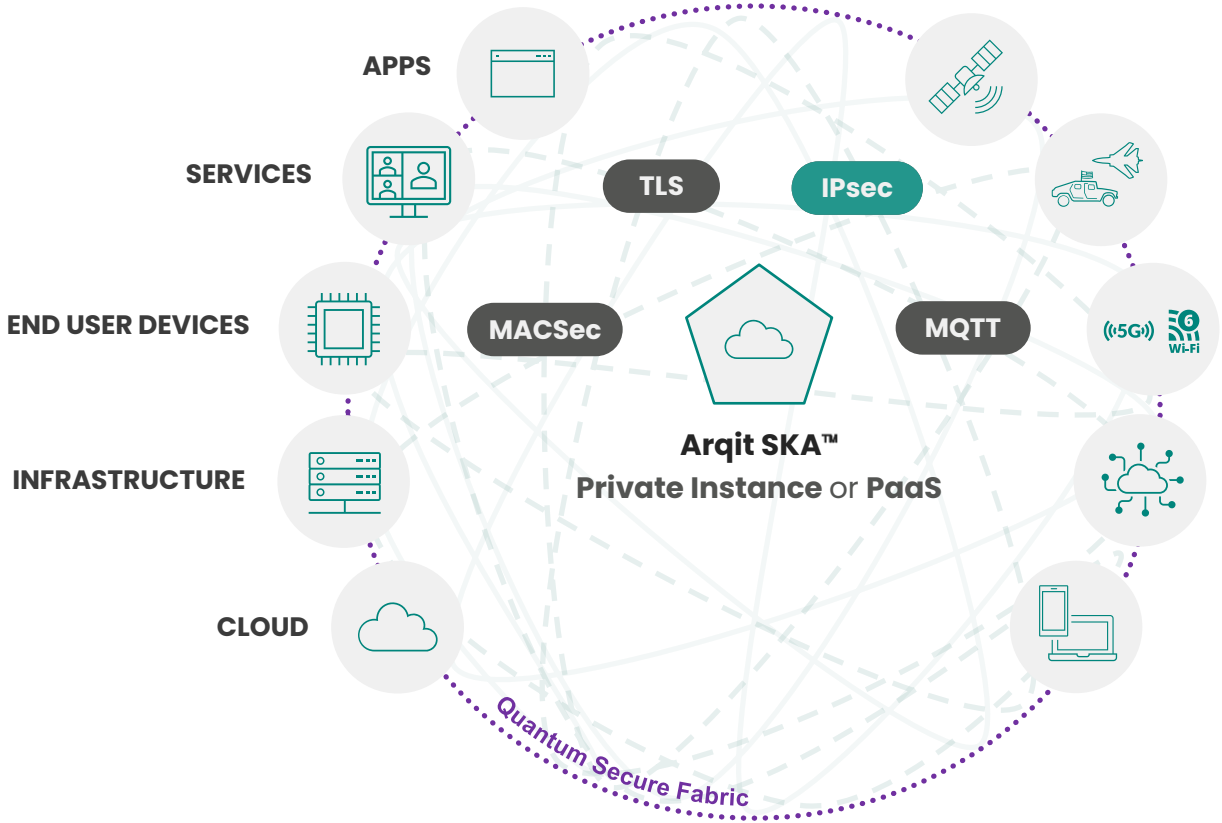
3

Groups of endpoints agree quantum-safe symmetric keys using material provided by Arqit SKA™

Stronger, simpler encryption

ARQIT

Keys can quantum-secure any channel



Post-Quantum Cryptography (PQC) Without Compromising Performance

World Leading Network Solutions by Arqit and Intel

Divya Pendyala
Cloud Software Architect
Network & Edge Solutions Group at Intel Corporation

Edge NetSec Evolution Drives Demand for Compute

- AI enabled network security
- Comprehensive integration of NetSec workloads
- Vendor consolidations, multi-vendor solutions integrations and interoperability

Secure work force connectivity

Secure edge device connectivity

Secure application connectivity

Increase in end points, variation, and attack surface

- Increase in traffic
- Intelligent and AI enabled network security

- More purposeful compute
  - Processors
  - Accelerators

Disclaimer: No product or component can be absolutely secure.

Introducing the Intel® NetSec Accelerator Reference Design ....an autonomous server on a PCIe add-in card

- Server on a card: orchestration and mgmt. independent of the host
- NIC (Intel® Ethernet Controller E810) + Intel SOC
  - Flexible compute augmentation for Host Platform
  - Workload migration from host to free up processor cores
- Scalable Intel Architecture for common network functions
- Maintain architectural consistency with Intel Architecture
- Low software lift (if any) to on-board

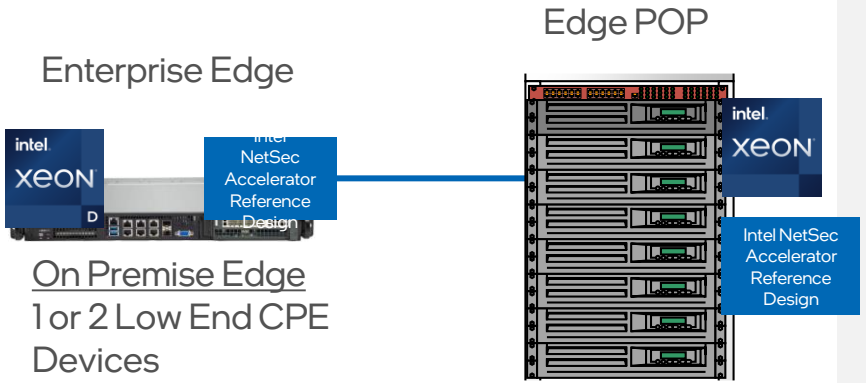
Intel NetSec Accelerator Reference Design Ver 1 (Intel Atom®: 8C, 16C)

Intel NetSec Accelerator Reference Design Ver 2 (Intel® Xeon® D: 4C, 8C, 10C)

Deployment Models	Use Cases and Workloads
Network Accelerator Aka Partial Application Offload	**Network and Security Appliances** IPsec, SSL, IDS/IPS, NGFW
Full Application Offload Aka Distributed Appliance	**SASE and Network Edge Connectivity** SD-WAN, Head End and Far Edge

Intel® NetSec Accelerator Reference Design Product Positioning

1. Acceleration of networking and security workloads
2. Customers looking for Intel coherency
   - Same NIC/SOC as used on appliances
   - Ease of consumption; low software reprofiling, if any
3. Anchors on driving scale and TCO
   - Workload acceleration → platform scaling
   - Deployment of fully packaged apps/appliances in 3rd party hosts
     - Edge: enable scalable cluster nodes
     - 'Appliance on a card' that works autonomously in a host



On which platform is your cryptographic application (TLS, IPsec VPN, etc.) hosted, at the edge ?

a. x86 by Intel

b. x86 by others

c. ARM

d. Other

Post-Quantum Cryptography (PQC) Without Compromising Performance: World Leading Network Solutions by Arqit and Intel

Phil Burn, Solution Architect

April 30th 2024

Arqit & Intel PQC Solution

A world leading out-the-box solution that provides high throughput and quantum safe data communications

1 Quantum safe

Creates quantum-secure data links and supports a quantum-secure deployment that caters to a wide range of use cases

2 High performance

Provides all the functional benefits Intel hardware without compromising performance

3 Simple installation

Out-the-box deployment enables a high performance PQC solution that can be implemented across your network today

There is a solution available for VPN

Protection against store now, decrypt later with minimal effort

Leading open-source libraries have added PQC methods for hardening VPN tunnels…

… which are enabled by Arqit's NetworkSecure™ and the Intel® Netsec Accelerator Reference Design

NetworkSecure™

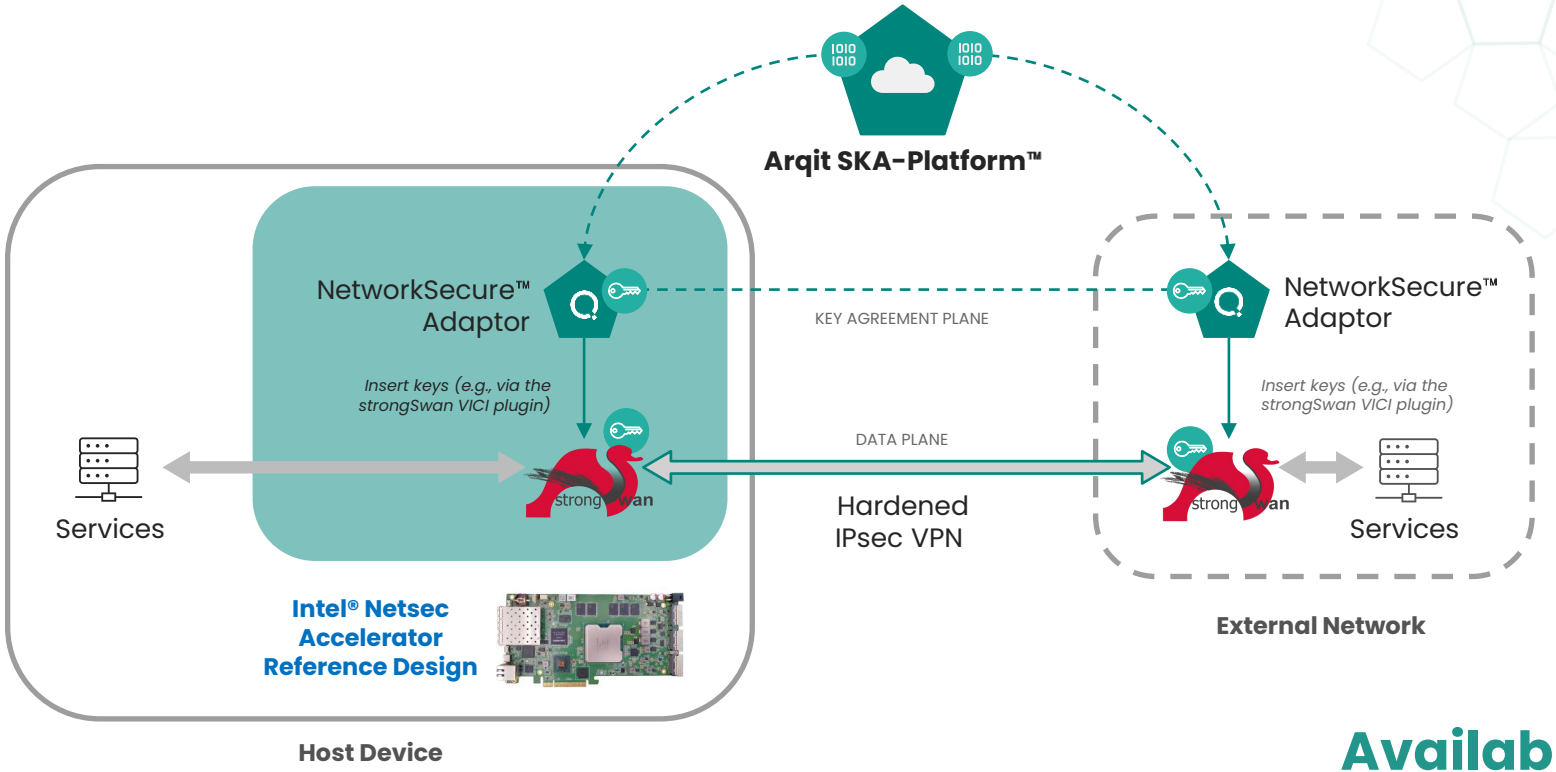
Intel® Netsec Accelerator Reference Design

Stronger, simpler encryption

ARQIT

Quantum-secure “server on a NIC”

PQC IPsec via Arqit NetworkSecure™ and the Intel® Netsec Accelerator Reference Design



Available today.

Stronger, simpler encryption

ARQIT

World leading high performance with PQC

Integration with VPP-SSwan to provide out-the-box solution

Technology Guide

intel

FD.io VPP-SSwan and Linux-CP - Integrate StrongSwan with World's First Open Sourced 1.89 Tb IPsec Solution

Authors

Roy Fan Zhang

Georgii Tkachuk

Pablo De Lara Guarch

Tomasz Kantecki

Kai Ji

John DiGiglio

1 Introduction

FD.io Vector Packet Processing (VPP) IPsec is an important component in VPP to enable secure, reliable, and fast networking applications. VPP IPsec provides a set of easy-to-use CLI and VAPI commands for users to configure Security Policy Database (SPD), Security Associations (SA), and associated cryptographic algorithms and keys.

With VPP IPsec running on a single 3rd Gen Intel® Xeon® Scalable processor core, one can achieve 31 Gbps throughput for a single Security Association for tunnel IPsec with AES-GCM-128 cryptography algorithm (IPSec IPv4 Routing, 2023[1]), over six times of what can be achieved with Linux Kernel based IPsec. For a 4th Gen Intel® Xeon® processor, the system performance can even achieve up to 1.89 Terabit No Drop Rate (NDR) IPsec tunnel throughput with 40 CPU cores in a single processor package, equivalent to almost 50 Gbps per CPU core[2]. With such a high throughput advantage, switching from kernel IPsec to Fd.io VPP IPsec appears as an obvious solution. However, it also brings new problems to be solved. IPsec relies on secured methods to setup SAs between two endpoints. The protocol to handle the SA setup is Internet Key Exchange (IKE). Fd.io VPP IPsec contains a mature, performant, and widely used IPsec implementation, but it is an incomplete IKEv2 implementation that is not production ready.

ARQIT

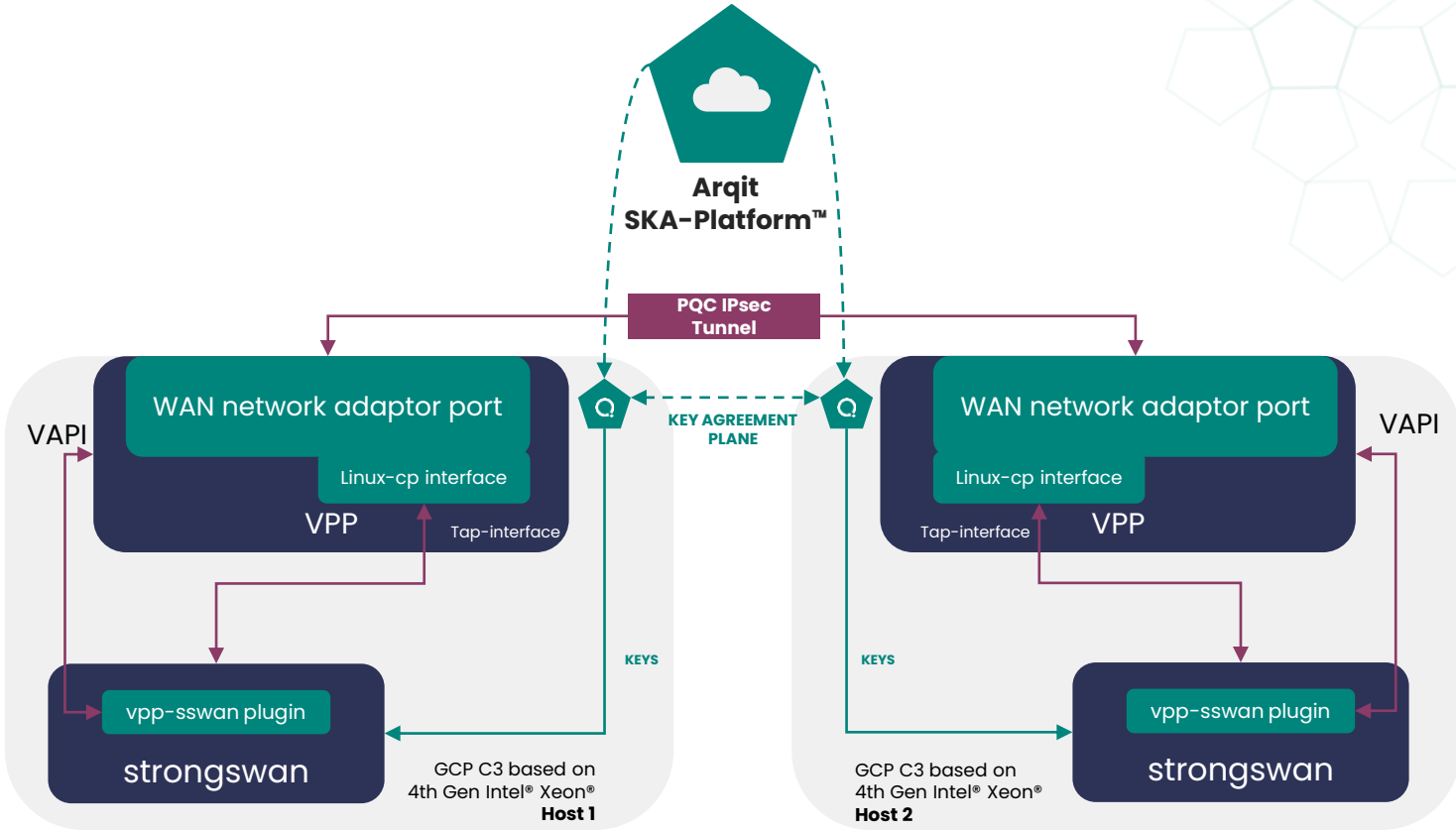
Now quantum-secure!

Stronger, simpler encryption

ARQIT

PQC Vector Packet Processing (VPP)

Proven quantum safe IPsec without compromising performance



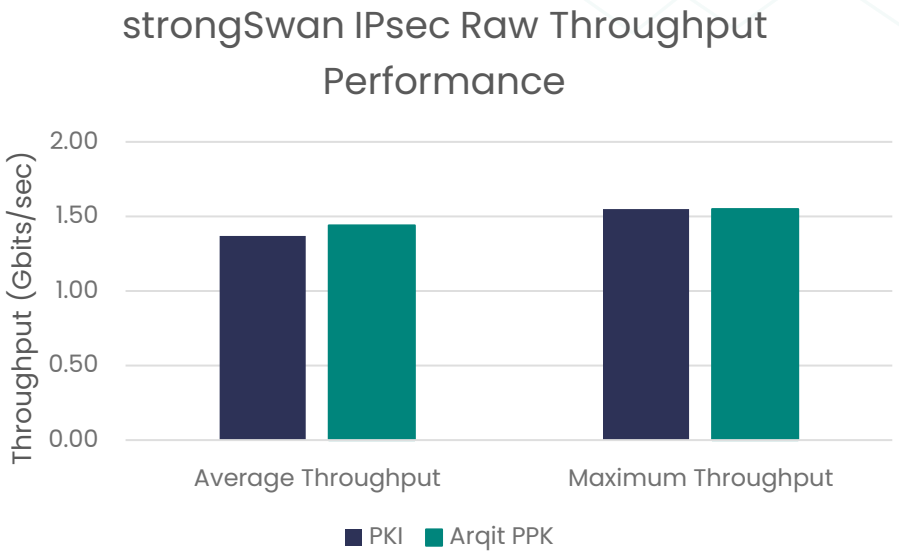
Stronger, simpler encryption

ARQIT

How does Arqit compare to standard PKI?

Comparative performance testing using Intel public cloud instances

Component	Description
Server Platform	GCP C3 with Intel® Xeon® Scalable processors
CPU	Intel® Xeon® Platinum 8481C processor @ 2.70GHz
Memory	32GB SSD
Storage	100GB SSD
NIC	Google, Inc. Compute Engine Virtual Ethernet [gVNIC] based on Intel® IPU

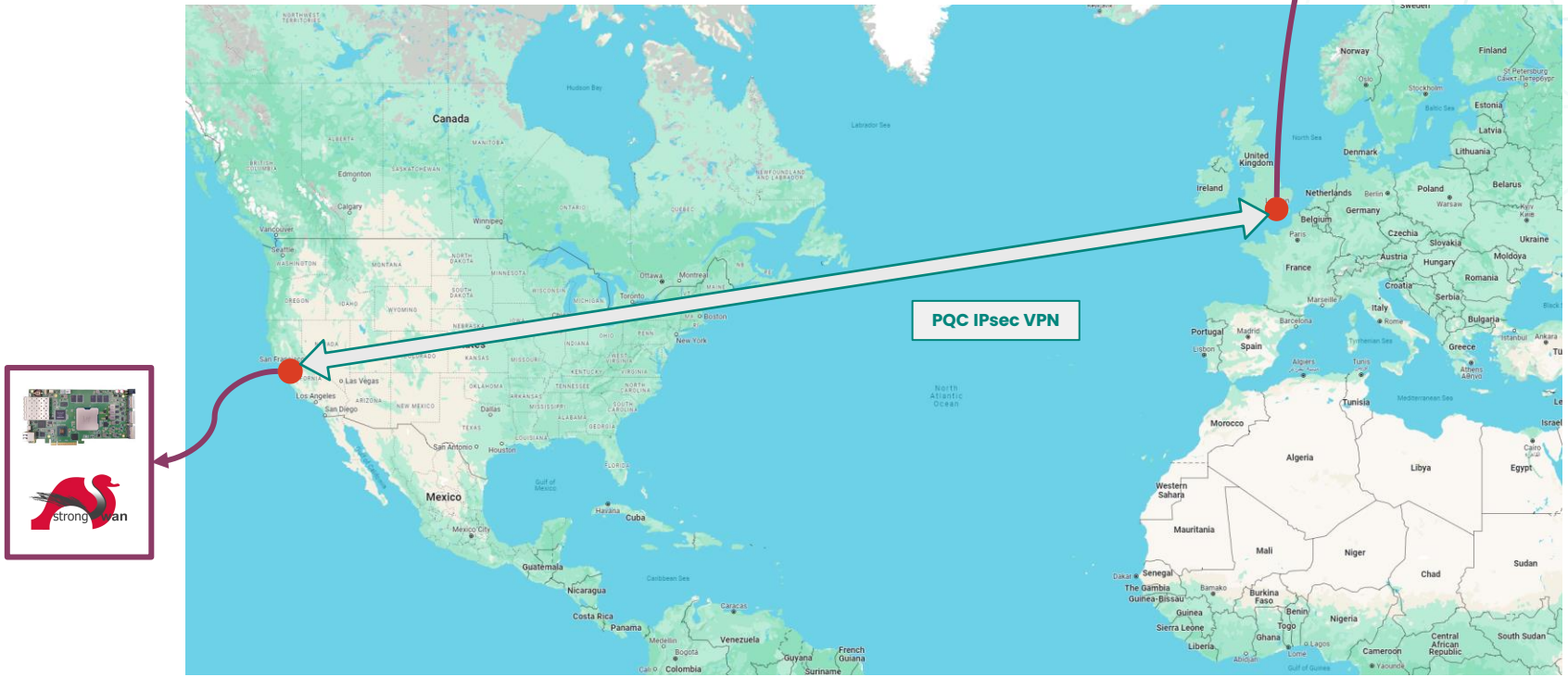


Stronger, simpler encryption

ARQIT

Live Demonstration

PQC IPsec to send data across the pond



Stronger, simpler encryption

ARQIT

Live Demonstration

Stronger, simpler encryption

ARQIT

PQC solutions for the netsec accelerator

Arqit and Intel present a much wider range of PQC solutions…

Commercial Solutions

FORTINET®

JUNIPER® NETWORKS

Open Source Solutions

strongSwan

OPENVPN™

WIREGUARD®
FAST, MODERN, SECURE VPN TUNNEL

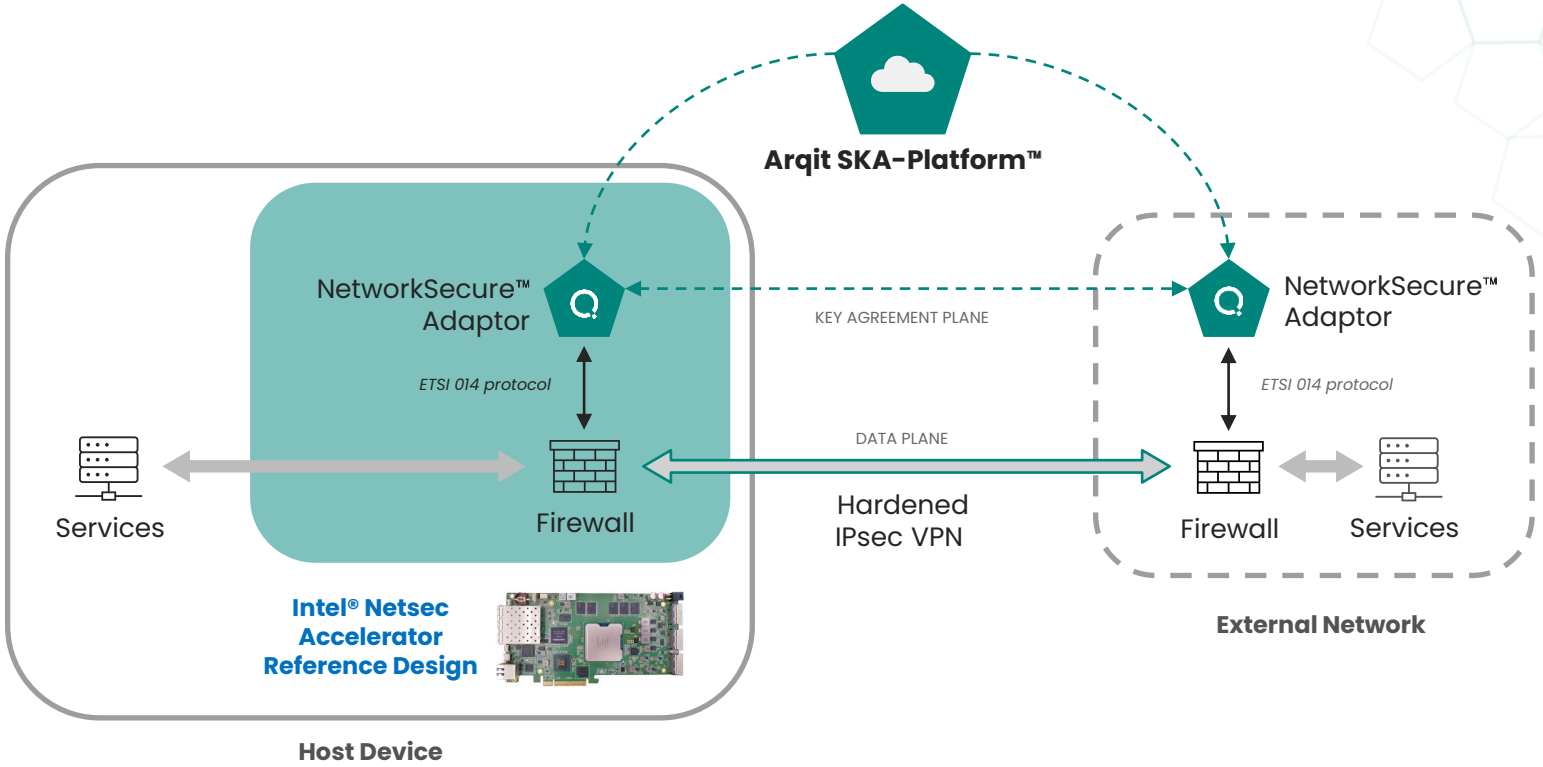
And many more!

Stronger, simpler encryption

ARQIT

PQC solutions for next-gen firewalls

High performance and quantum secure NGFWs from edge to cloud

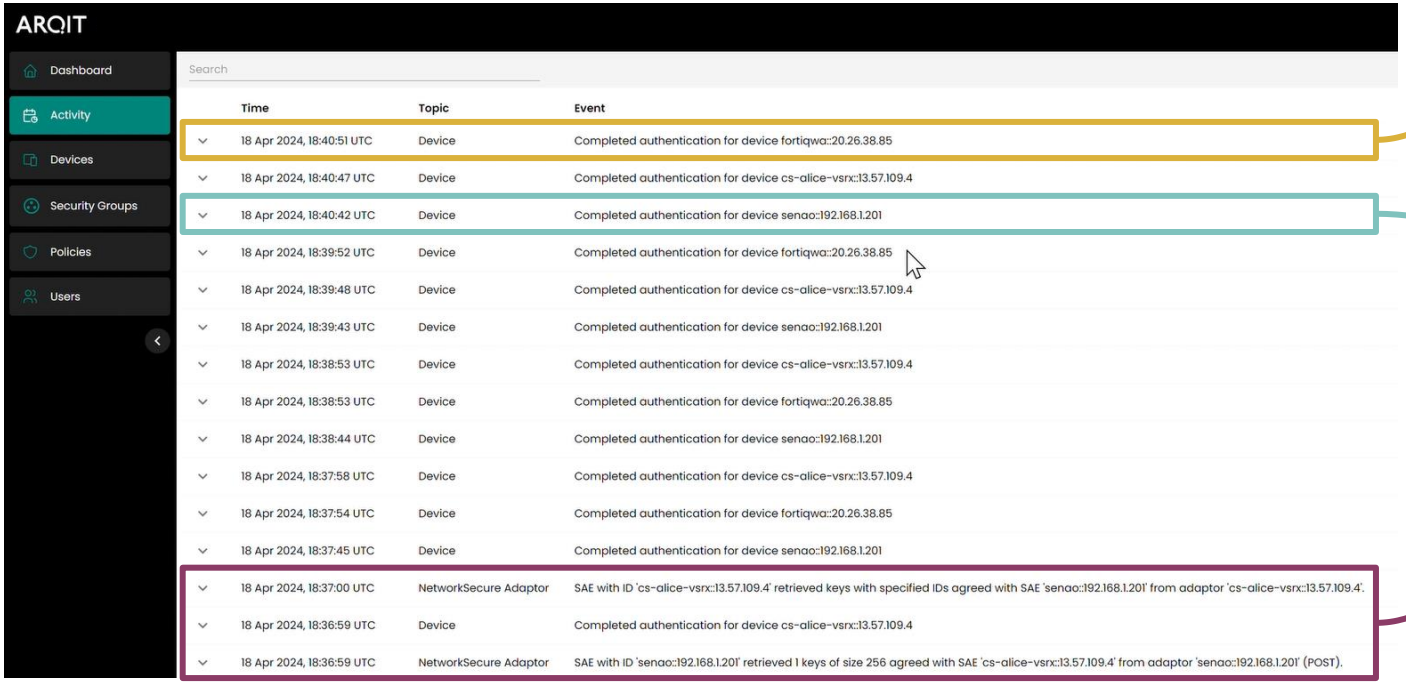


Stronger, simpler encryption

ARQIT

PQC solutions for next-gen firewalls

Deploy the components directly on the Intel®-based netsec accelerator



FORTINET

Intel® Netsec Accelerator Reference Design

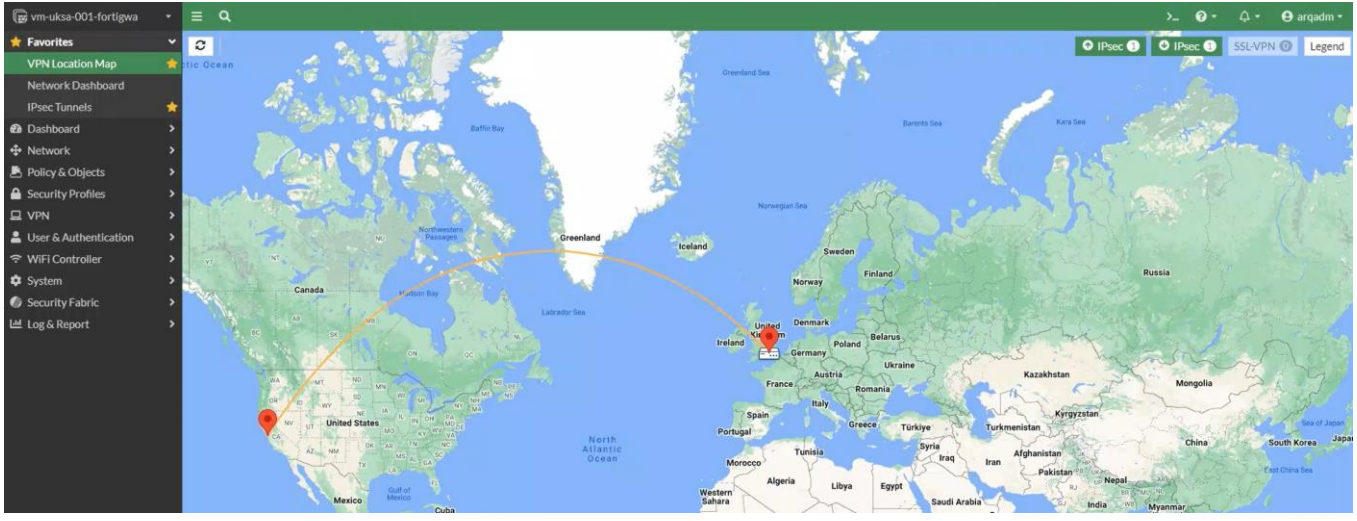
JUNIPER NETWORKS

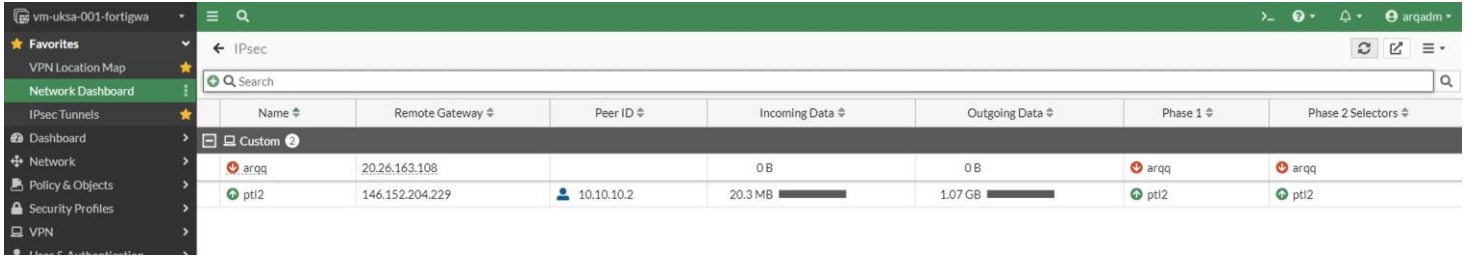
Stronger, simpler encryption

ARQIT

PQC solutions for next-gen firewalls

Quantum secure IPsec VPN for FortiGate NGFWs





FORTINET

Stronger, simpler encryption

ARQIT

PQC solutions for next-gen firewalls

Quantum secure IPsec VPN for Juniper vSRX NGFWs


```
ID: 522617 Virtual-system: root, VPN Name: alice
  Local Gateway: 10.1.1.4, Remote Gateway: 3.101.225.155
  Local Identity: ipv4(0.0.0.0-255.255.255.255)
  Remote Identity: ipv4(0.0.0.0-255.255.255.255)
  TS Type: proxy-id
  Version: IKEv2
  Quantum Secured: Yes
  PFS group: DH-group-20
  DF-bit: clear, Copy-Outer-DSCP: Disabled, Bind-interface: st0.0, Policy-name:
arq-ska
```

juniper NETWORKS

Stronger, simpler encryption

ARQIT

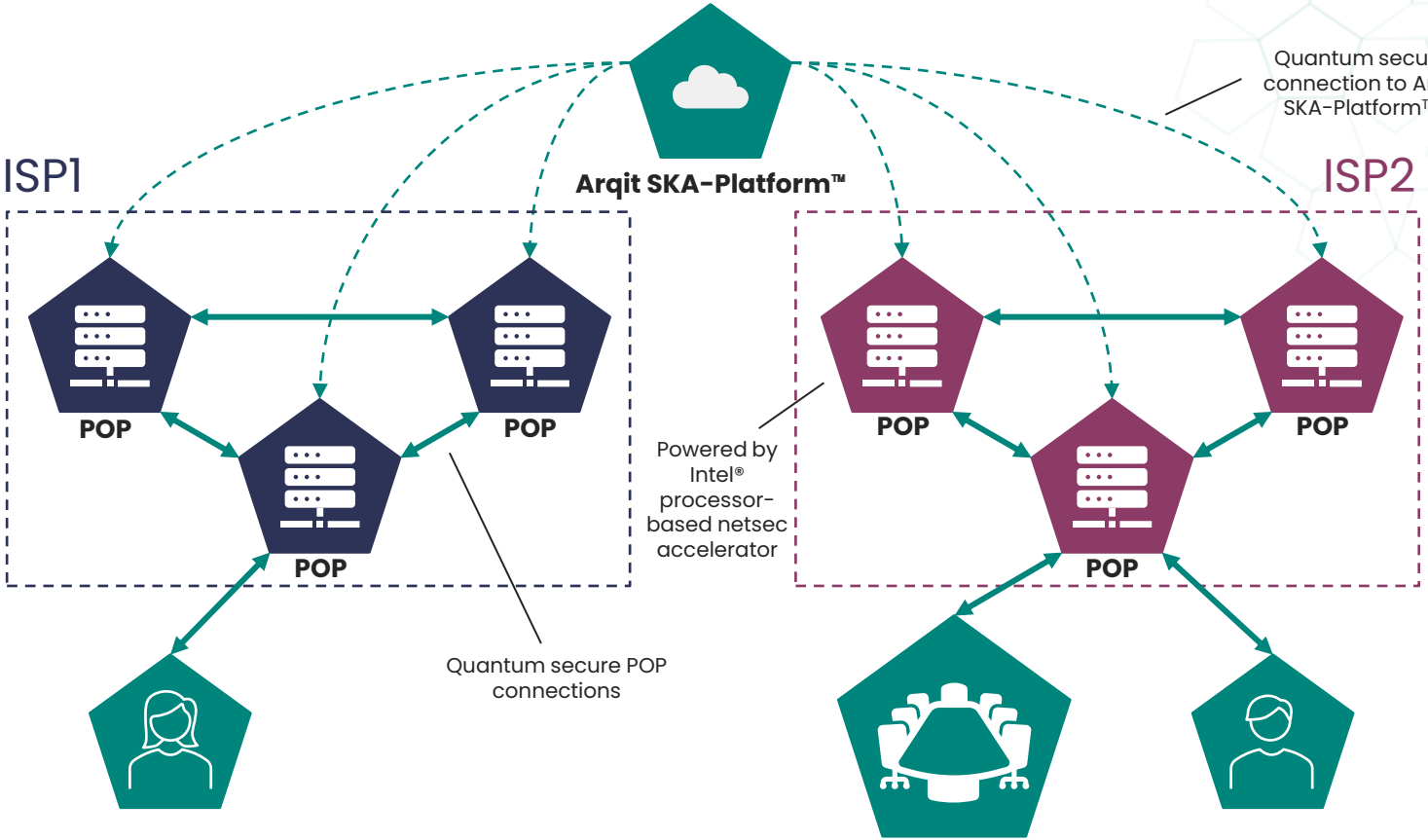
How can we use this technology in the real world?

Stronger, simpler encryption

ARQIT

Use Case: Point of Presence (POP) Servers

High performance POPs or flexible micro-POPs for Telcos



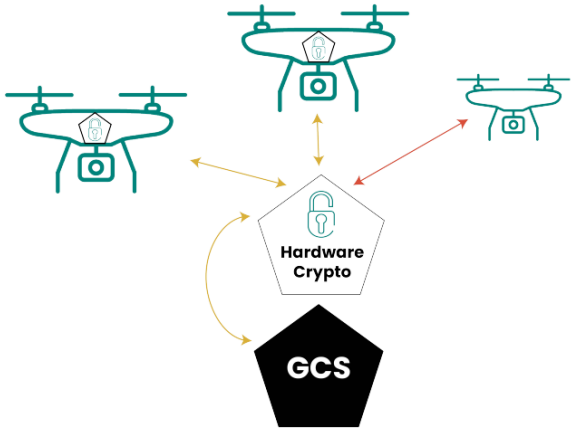
Stronger, simpler encryption

ARQIT

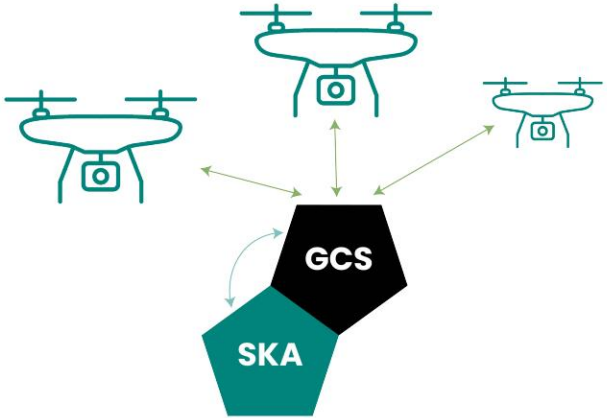
Use Case: Unmanned Aerial Systems (UAS)

Enabling the full potential of UAS operations

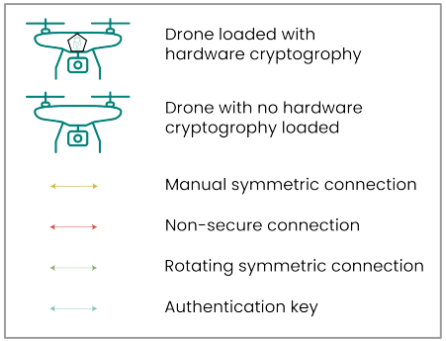
Cryptographic hardware manually loaded onto suitable UAS



Before



After



Executive Summary

1 The threat of quantum computers is real

Store now, decrypt later (SNDL) attacks are a critical threat and actions must be taken to prevent them today.

2 Secure your networks against quantum attack with Arqit SKA-Platform™

Arqit and Intel have produced an out-the-box post-quantum cryptography (PQC) solution that is available today – PQC without compromising performance.

3 Deploy optimized edge to cloud solutions with Intel

Intel has spectrum of options to ensure optimized form factor and compute resources – secure and high performance solutions for every scenario, from edge to cloud.

Thank you

Going to RSA Conference 2024 in San Francisco?

Meet us at our booth, #5377, North Expo

References

Intel

- https://networkbuilders.intel.com/solutionslibrary/fd-io-vpp-sswan-and-linux-cp-integrate-strongswan-with-world-s-first-open-sourced-1-89-tb-ipsec-solution-technology-guide
- Network Security at the Edge with Intel® NetSec Accelerator Reference Design
- Network Edge Transformation using Intel® NetSec Accelerator Reference Design
- https://github.com/intel/intel-ipsec-mb

Arqit

- https://arqit.uk/

Notices and Disclaimers

- Intel technologies may require enabled hardware, software or service activation.
- No product or component can be absolutely secure.
- Your costs and results may vary.
-