Stronger, simpler encryption

Quantum Security For Mobile Private Networks -ARQIT

June 23 Uptime Italy

Ayan Ghosh

Stronger, simpler encryption

ARQIT

Our mission

To use our world leading encryption platform to keep safe the data of our governments, enterprises and citizens.

Stronger, simpler encryption

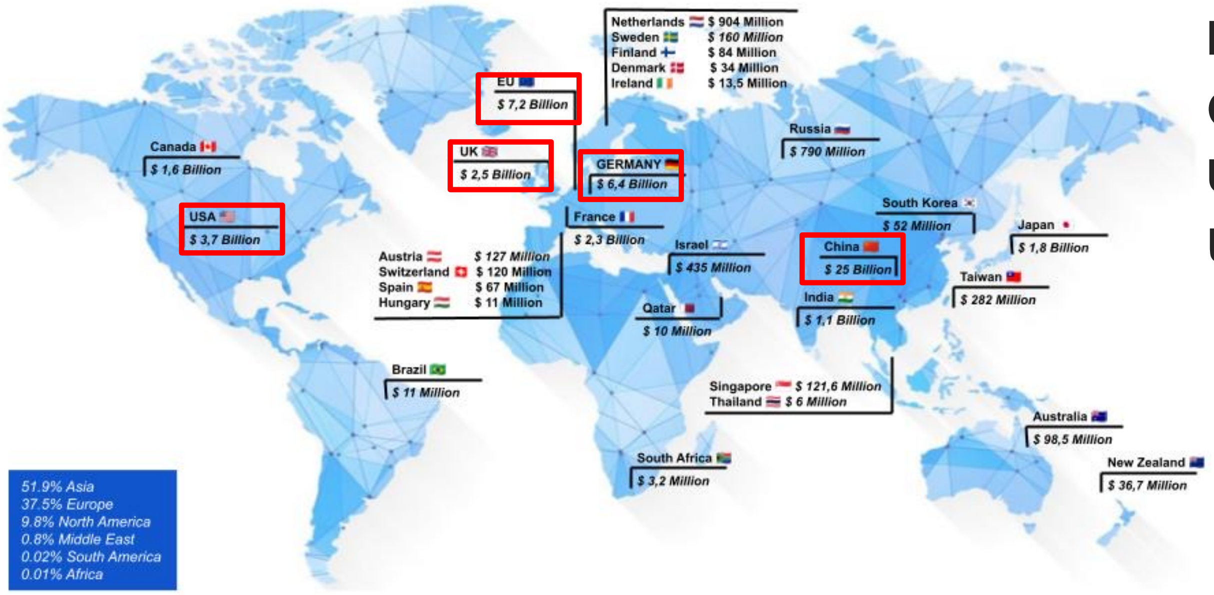
ARQIT

Who is investing in quantum computers?

What is the threat risk?

Government funding in Quantum Tech 01/23

29 total initiatives with a total of $ 55.4 Billion in funding



Source: Global Quantum Intelligence, LLC | All rights reserved, 2023 © | www.global-qi.com

China: $25.0b

EU: $7.2b

Germany: $6.4b

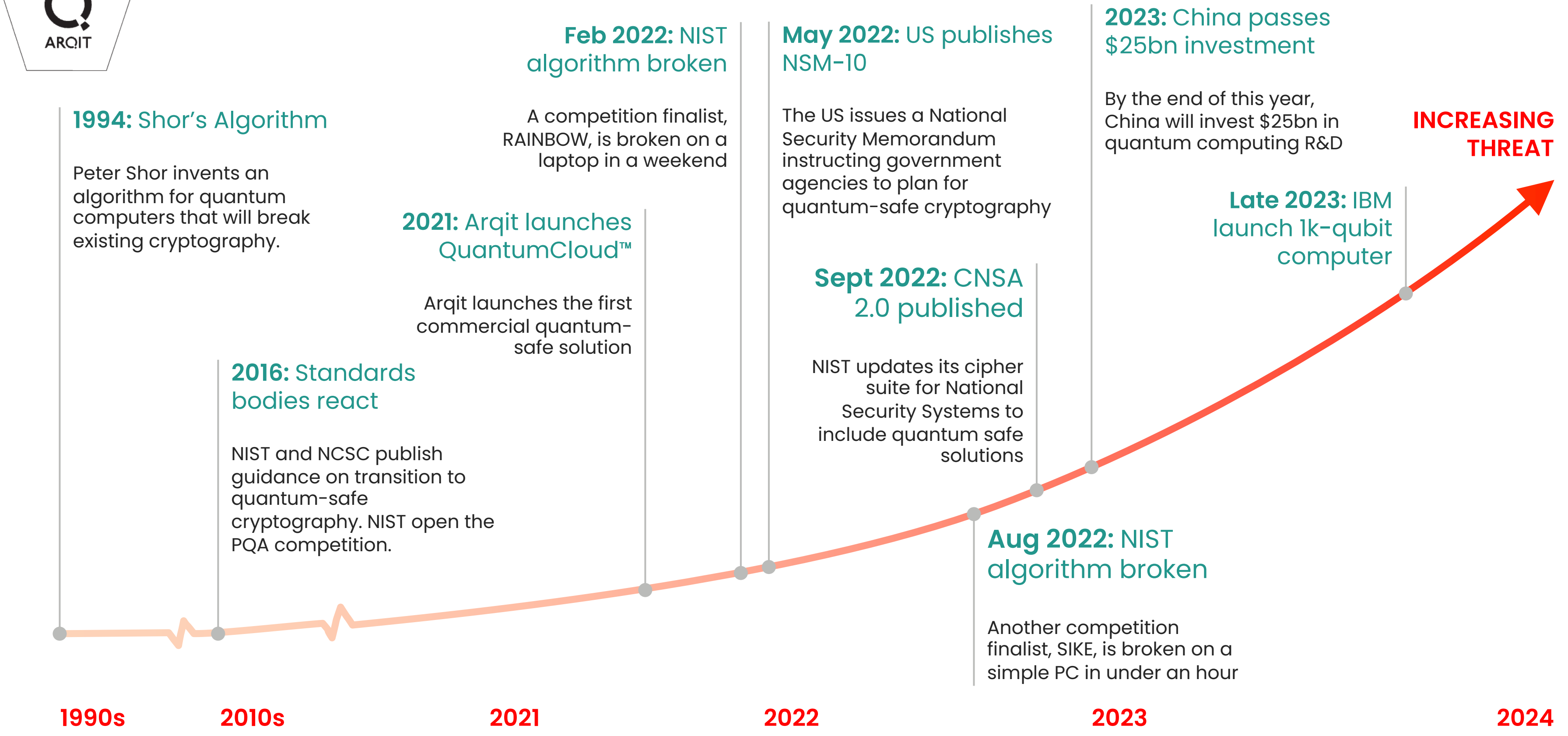
USA: $3.7b

UK: $2.5b

Stronger, simpler encryption

ARQIT

The threat is increasing over time



1994: Shor's Algorithm

Peter Shor invents an algorithm for quantum computers that will break existing cryptography.

2016: Standards bodies react

NIST and NCSC publish guidance on transition to quantum-safe cryptography. NIST open the PQA competition.

2021: Arqit launches QuantumCloud™

Arqit launches the first commercial quantum-safe solution

Feb 2022: NIST algorithm broken

A competition finalist, RAINBOW, is broken on a laptop in a weekend

May 2022: US publishes NSM-10

The US issues a National Security Memorandum instructing government agencies to plan for quantum-safe cryptography

Aug 2022: NIST algorithm broken

Another competition finalist, SIKE, is broken on a simple PC in under an hour

Sept 2022: CNSA 2.0 published

NIST updates its cipher suite for National Security Systems to include quantum safe solutions

2023: China passes $25bn investment

By the end of this year, China will invest $25bn in quantum computing R&D

Late 2023: IBM launch 1k-qubit computer

Data is at risk ***today!***

1 PKC weaknesses

Many well-publicised threats and breaks of PKC in the last decade

2 Store now, decrypt later

A serious threat to the long-term secrecy of information

3 Scaling issues

Meeting the challenge of exponential connected endpoint growth

Stronger, simpler encryption

ARQIT

Quantum-safe Solution Strategies

PQA

Uses even harder mathematical problems than we use today

ADVANTAGES

✓ Natural extension of existing PKC techniques

✓ Doesn't require prior knowledge between parties

✓ Will become international standard

CHALLENGES

? Cannot be proven secure

? Slower and more memory and energy intensive

? Long timescales to standardization

ARQIT

QuantumCloud™ Symmetric Key Agreement

A cloud-based service to scale symmetric key agreement, strong authentication, and create quantum-safe channels

ADVANTAGES

✓ Split-trust symmetric key agreement protocol that's provably unbreakable

✓ Can secure every endpoint over shared networks

✓ Active authentication and permissions

✓ Fast and lightweight cryptography

✓ Promotes zero-trust and secure-by-design principles

CHALLENGES

? Requires a suitable root of trust process

QKD

Use quantum phenomena to deliver key material which is provably secure by the laws of physics

ADVANTAGES

✓ Best possible provable security based on laws of physics

✓ Offers 'eavesdropper detection' on communication channels

CHALLENGES

? Difficult to scale

? Requires specialist and expensive equipment

Stronger, simpler encryption

ARQIT

QuantumCloud™ is a quantum-safe symmetric key agreement platform

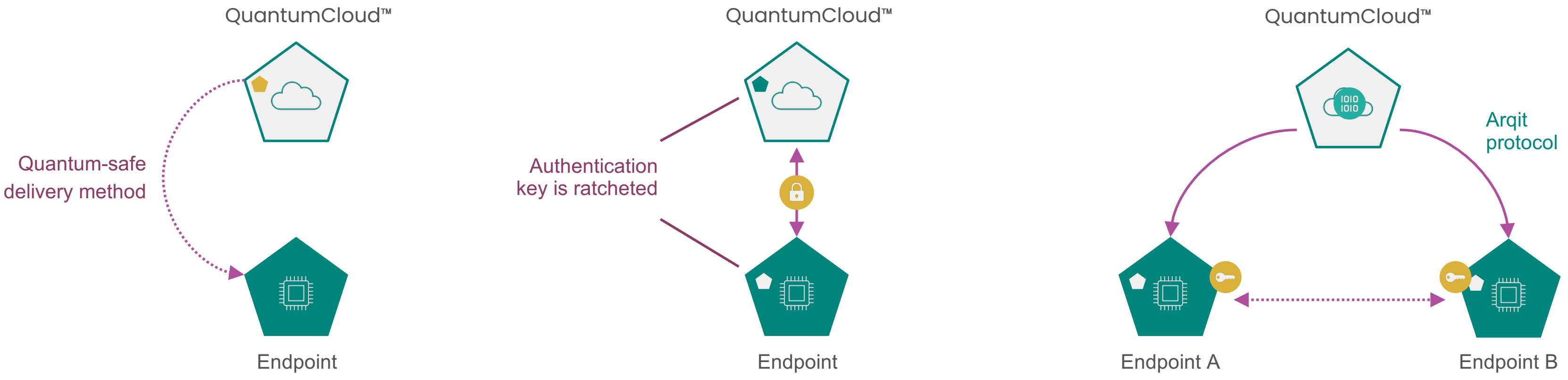
Safe against "store-now, decrypt-later" attack from quantum computers

Global cloud-based service which is scalable, flexible and lightweight

Compatible with **existing standardised AES256** encryption alongside existing PKI and applications

Stronger, simpler encryption

Provisioning, authentication, and key agreement



1

Every endpoint is securely provisioned once with a “bootstrap” key (root of trust)

2

Endpoints strongly, mutually authenticate with perfect forward secrecy

3

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

Arqit NetworkSecure™

Quantum-safe VPN Encryption Solution

Integrated, automated solution provides on-demand quantum-safe encryption for enhanced protection of VPN data communications

1

Quantum-safe

Creates quantum-safe data links and supports quantum-secure deployments over zero-trust networks

2

Low effort integration

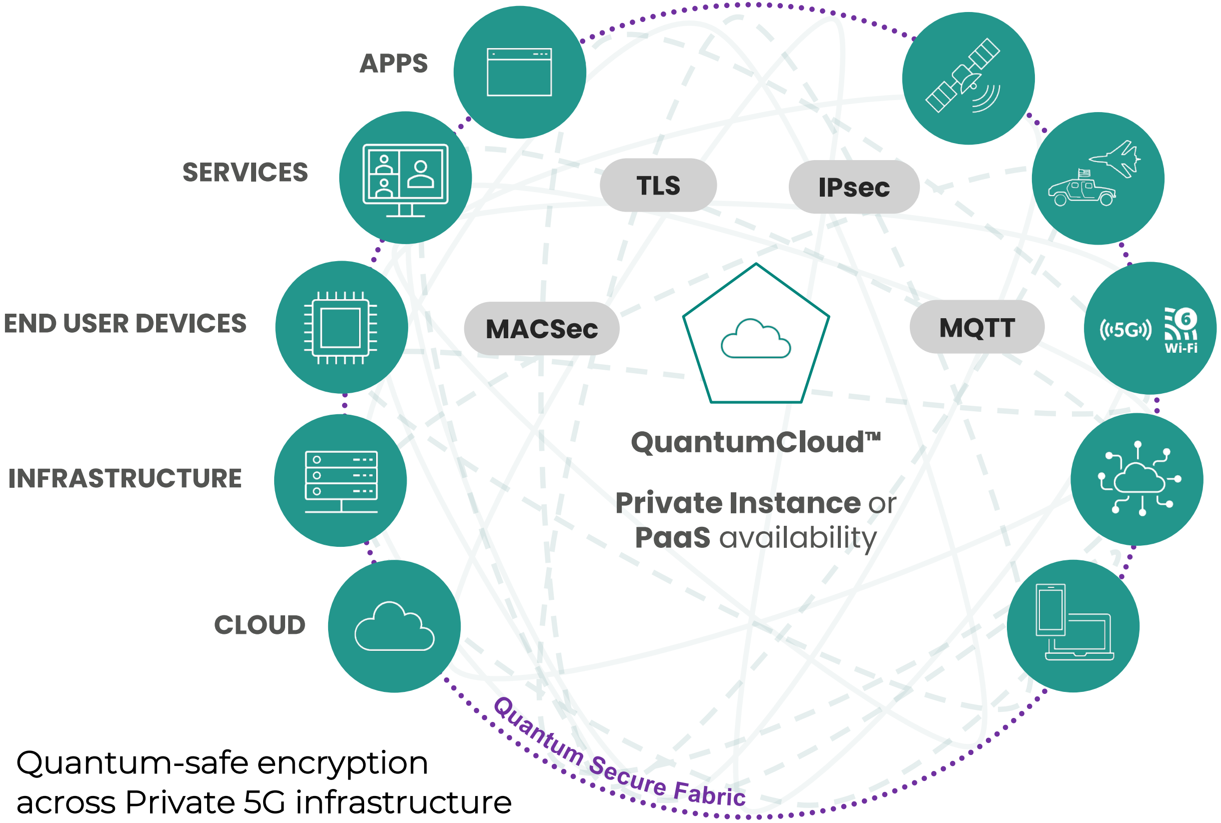
Provides enhanced security, operational efficiency, and cost reduction through on-demand key rotation

3

Standards-based

Usable with existing and proven data encryption standards, such as AES256

Arqit NetworkSecure™



Quantum-safe encryption
across Private 5G infrastructure

Quantum-secure any channel

- Symmetric keys provide the most efficient and provably secure form of encryption
- Keys can be used in many different types of encrypted channel
- Greater levels of encryption control applied within the application layer ("crypto-agility")
- Encryption policy enforcement selectively applied to all application and infrastructure layers
- Layers on top of PKI or can remove dependency → 'Secure by Design'

Stronger, simpler encryption

Security Enhanced Virtualised Networking for 5G (SEViN-5G)

Innovate UK project aligned with DSIT Telecoms Diversification Strategy

Background: Evolving network architectures (virtualisation & cloudification, open networks, private cellular…) have potential to create new security concerns and requirements

Objective: explore security considerations of Private 5G

- Demonstrate the feasibility and performance of quantum-resistant encryption in Private 5G
- Develop reference deployments and testbeds for secure distributed Private 5G deployments (*on-premise, public cloud, virtualised macro-network slice, etc.*)
- Continuous encryption capability analysis to identify weakness and exposures within and across the Private 5G network
- IoT device traffic pattern fingerprinting to identify divergence from normal (*e.g. compromised device, rogue device, misdirected data streams*)

5G industry news Security

UK 5G Innovation Network

Assessing security vulnerabilities in 5G Private Networks

2 minute read Published on 8 Feb 2021 - Last modified 25 Feb 2021

The UK Department for Digital, Culture, Media and Sport (DCMS) are conducting an engagement with industry, academia, government, technical authorities, standards bodies and wider public sector to assess potential security challenges

enisa

EUROPEAN UNION AGENCY FOR CYBERSECURITY

ENISA THREAT LANDSCAPE FOR 5G NETWORKS

Updated threat assessment for the fifth generation of mobile telecommunications networks (5G)

DECEMBER 2020

POTENTIAL THREAT VECTORS TO 5G INFRASTRUCTURE

2021

DARKReading The Edge DR Tech Sections Events

Threat Intelligence | 8 MIN READ | ARTICLE

An Emerging Threat: Attacking 5G Via Network Slices

A successful attack against 5G networks could disrupt critical infrastructure, manipulate sensor data, or even cause physical harm to humans.

Tara Seals
Managing Editor, News, Dark Reading

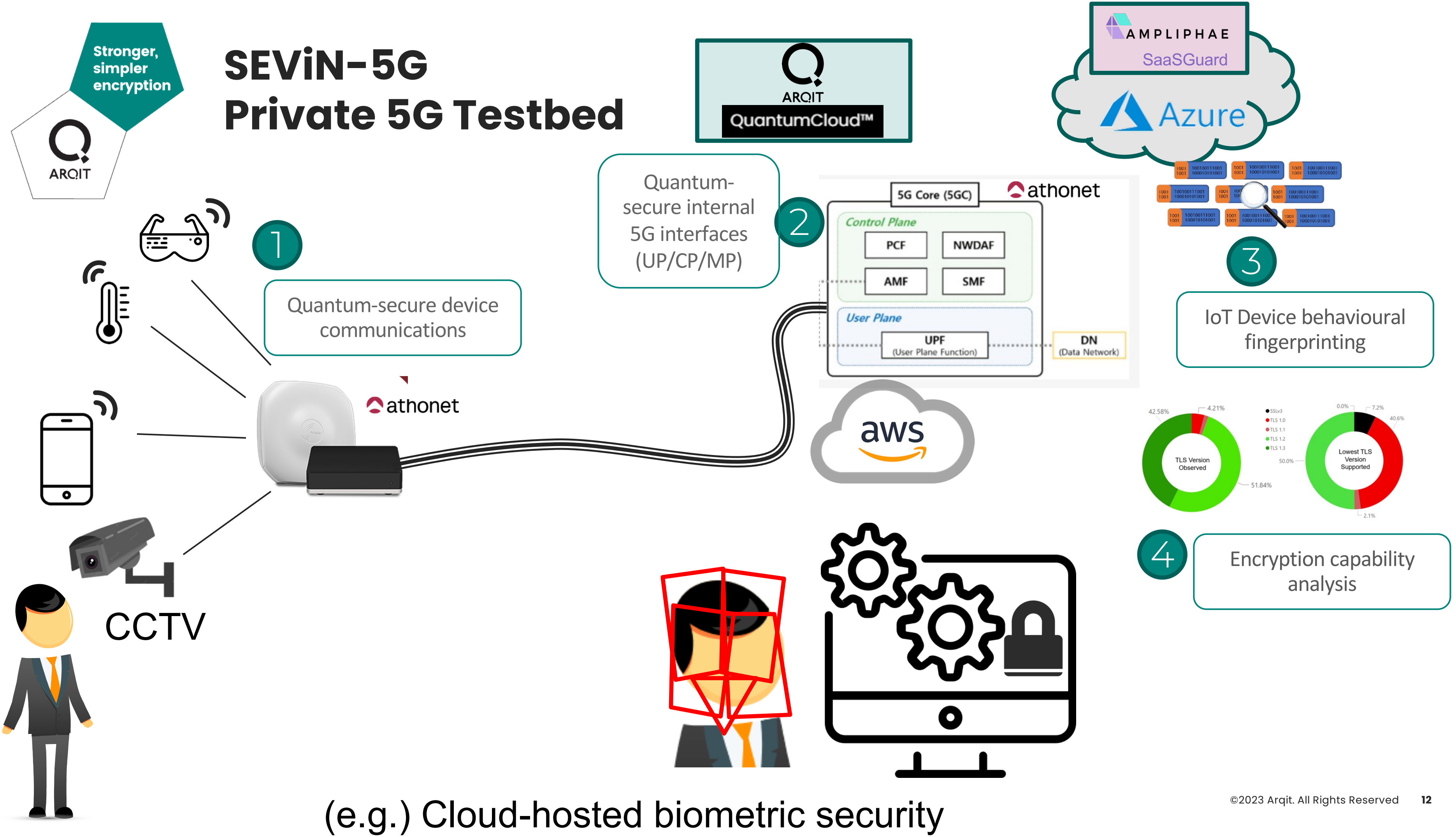
June 08, 2022

Partners: AMPLIPHAE ARQIT UKRI Innovate UK

Suppliers: athonet aws Azure

SEViN-5G will deliver a quantum-secure Private 5G testbed with security analytics by end of calendar year 2023

SEViN-5G
Private 5G Testbed



1 Quantum-secure device communications

2 Quantum-secure internal 5G interfaces (UP/CP/MP)

3 IoT Device behavioural fingerprinting

4 Encryption capability analysis

(e.g.) Cloud-hosted biometric security

Thank you