ETSI/IQC Quantum Safe Cryptography Conference 2026

Progress toward global assurance of QKD systems

Presented by:
Dr. Chris Erven, Founder & CCO, chris.erven@kets-quantum.com
Dr. Robert Starkwood, Head of Performance

17 June 2026

Overview

- State of play for **QKD standards**, **security assurance**, and **certification**
- QAssure
  - Overview
  - Principles based assurance
  - QKD hardware testing
  - Lessons learned and remaining gaps
- Addressing shortcomings of early solutions
- Call to action

KETS

QKD Certification and Security Assurance

Standards	Security Assurance	Certification
Standards define the rules	Assurance provides the evidence	Certification provides the independent validation
A **security standard** defines what security properties are required and how they should be implemented, measured, or evaluated.	**Security assurance** is the justified confidence that a system satisfies its security requirements and will perform its security functions as intended.	**Security certification** is the independent verification and formal recognition that a system meets specified security standards or assurance requirements.
HIGH MATURITY With many different standards published: ETSI ISG-QKD (e.g. ETSI GS QKD 016 v2.1.1 Common Criteria Protection Profile), NCSC Principles Based Assurance, ISO / IEC, IETF (QIRG), ITU-T, IEEE	**LOW-MODERATE AVAILABILITY** Emerging with: NSR/KRISS/TTA/ITSCC Nostradamus (EuroQCI) 	**EXTREMELY LOW AVAILABILITY** South Korea's National Intelligence Service (NIS)

KETS

QAssure: Overview

- Main aim: To extend the state of the art for creating an assurance case for QKD links and QKD networks
- Consortium of UK organisations
- Utilized the UK's National Cyber Security Centre's (NCSC) recommended Principals Based Assurance (PBA) approach
- Draft assurance cases constructed and reviewed using the NCSC's CRT-APC base framework for hardware cyber security devices
- Followed a secure-by-design approach to cyber security that covers not only hardware and software properties but also more holistic aspects such as design processes, supply chain security, updates and lifecycle management

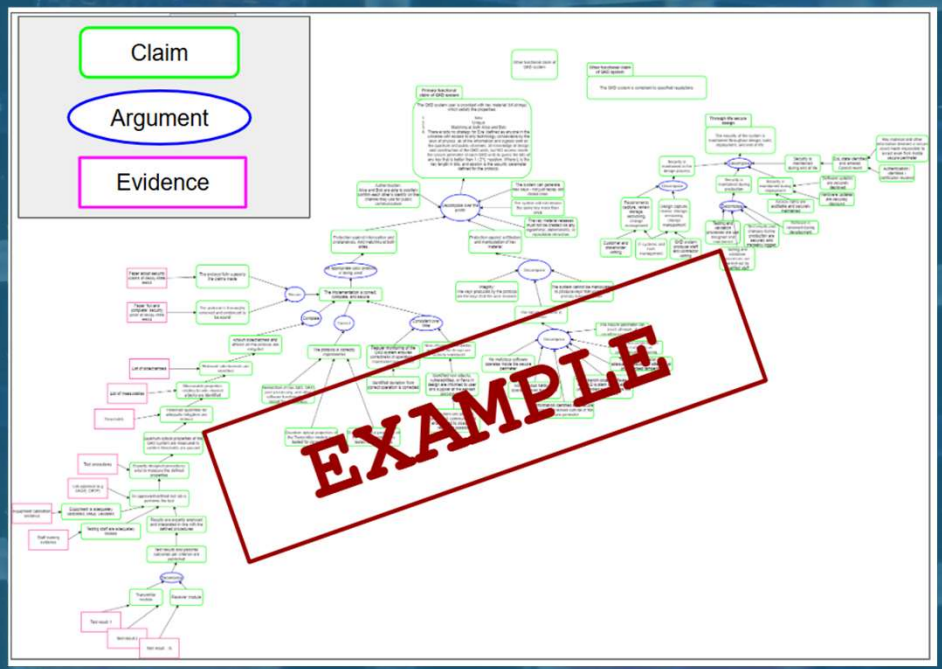
https://qassure.org/

Innovate UK funded project no. 10102791, part of the Quantum Challenge within the UK National Quantum Technologies Programme.

KETS

QAssure: Principals Based Assurance

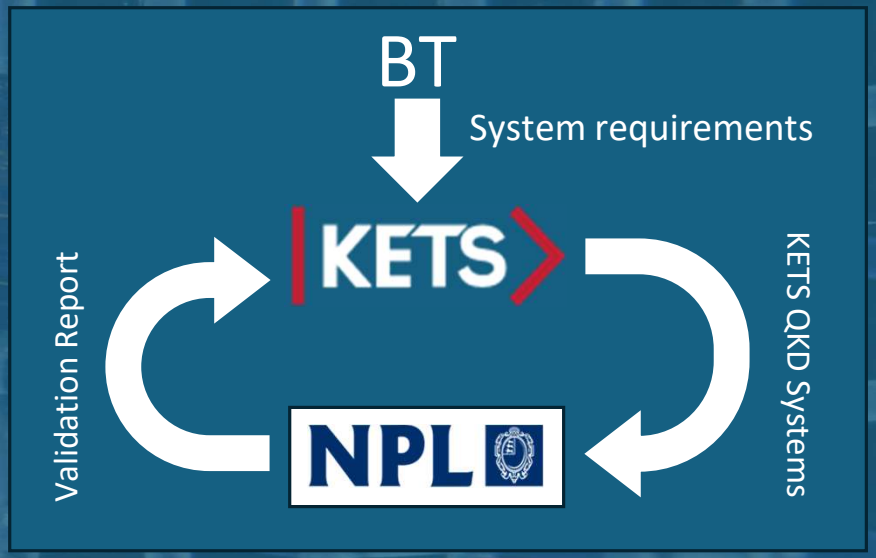
- Principals Based assurance is a risk-centric technology assurance methodology developed by the NCSC for application across a spectrum of cyber security products
- Assurance case constructed from a “tree” of claims comprised of multiple specific arguments which in turn are supported by individual pieces of evidence
  - Example claim = “The probability of an eavesdropper correctly guessing a secret key (length l) is less than $2^{-l}+\varepsilon$ ”
  - Example argument = “The QKD system under test sufficiently implements the QKD security proof, with adequate countermeasures against known side-channels”
  - Example argument = “The QKD system under test was measured in accordance with ISO/IEC 23837-2, by an accredited test lab”
  - Example evidence = Measurement data and analysis results.



KETS

QAssure: Independent hardware testing

- KETS QKD system independently tested at NPL on two separate occasions
- Testing focused on security properties of quantum channel hardware – following measurement standards ISO/IEC 23837-2 and ETSI GS QKD-011, including:
  - Transmitter state encoding accuracy, intensities, spectrum, and stability
  - Receiver properties such as detector efficiencies, after-pulse probabilities, dark count rates, and dead times



7.2	Test if emissions are consistent with photon number distribution(s) of optical pulses that are expected to be emitted by the TX module under test
7.3	Test if mean photon number of optical pulses generated in TX module under test, as well as its stability in time, are consistent with requirements of the implemented QKD protocol
7.4	Test if intensities of emitted pulses for each intended intensity are independent of underlying intensity modulation pattern
7.5	Test if quantum states emitted by TX module under test are encoded sufficiently accurately to match those required by implemented QKD protocol
7.7	Test if global phase of optical pulses is randomly distributed, as required by implemented QKD protocol
8.2	Test if detection probabilities output from RX module under test are consistent with model of implemented QKD protocol
8.7	Test if raw data generated by RX module under test excludes any detection events generated during dead time of any of the SPDs

KETS

QAssure: Lessons learned and remaining gaps

- **Assurance is possible**
  - To be commercially viable at scale, verifying that hardware is operating securely should be an order of magnitude faster and cheaper
- **The project didn't get to a "complete" PBA assurance case for a QKD system**
  - Further testing time would be required to complete all relevant elements of ISO/IEC 23837-2 and further side-channel analysis
  - Further technical analysis is required to link measurement data to quantified pass/fail requirements of the QKD security proof
  - The assurance case was not evaluated for completeness and soundness by an authoritative body
- **Detailed independent expert review of the assurance case must be done if transparency is to be achieved and trust earned**

KETS

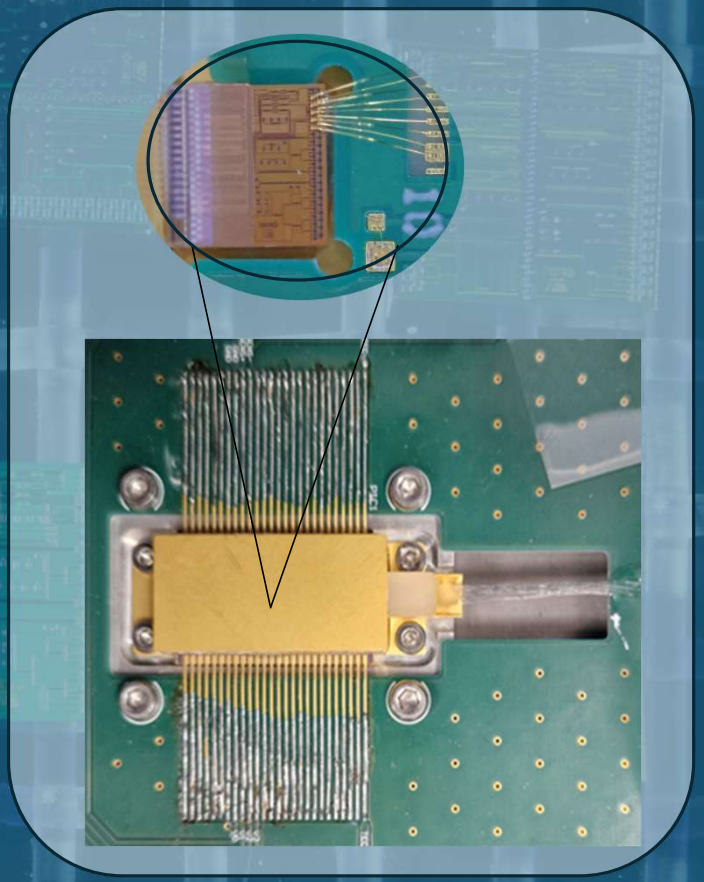
Addressing shortcomings of early solutions

	Criticism	Progress
Red Herring	Denial-of-service	Solution: redundant, resilient QKD networks. Really about cost and operational complexity.
	Authentication	Solution: pre-shared key, PQC for 1st bootstrap
	Low key rates	Current key rates sufficient for AES-rekeying and OTP in CNI
Scalability	Large form-factor & high-cost	KETS CUbIQ KEEQUANT
	Requires dark fibres (high cost)	LUXQUANTA TOSHIBA KETS
	Operational complexity (high cost)	NOKIA evolution KETS CUbIQ
	Distance limit	Honeywell Aerospace ses Micius
Security	Security proof gap	Q*bird evolution
	Security assurance	IDQ TOSHIBA KETS

*A sampling of quantum-safe companies tackling key challenges

KETS

KETS Contribution: Chips = road to scalability



Low form-factor

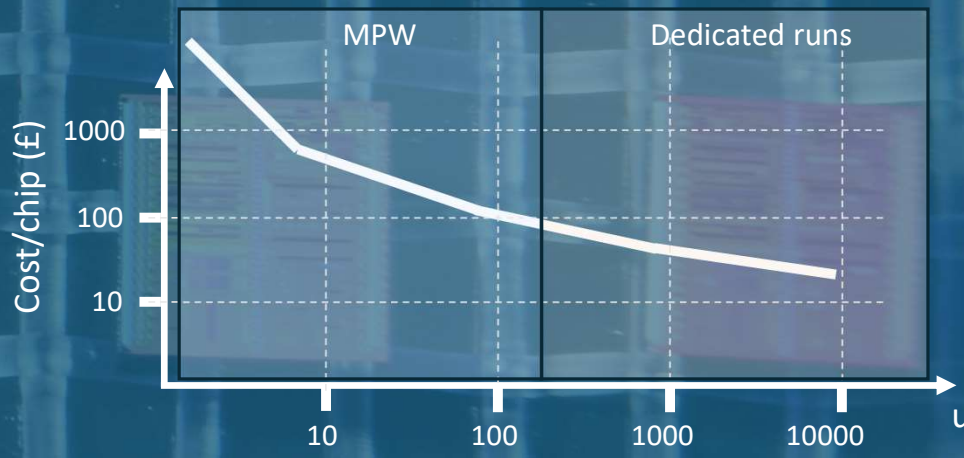
Lower costs at scale

Improved performance

Enhanced security

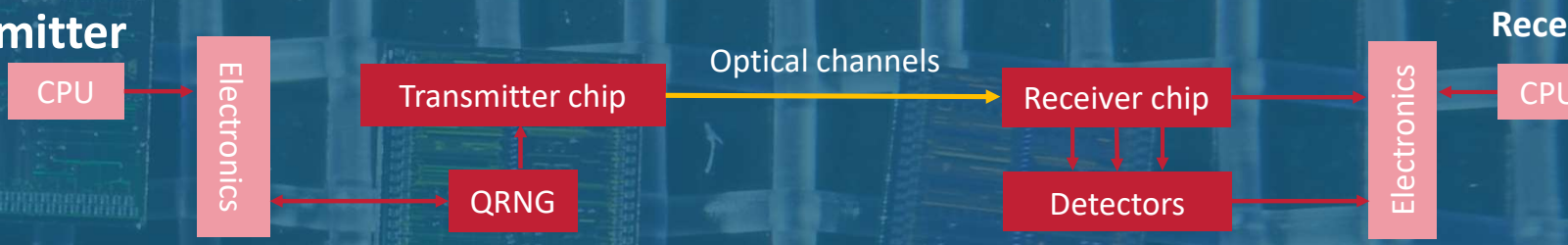
Lower driving power

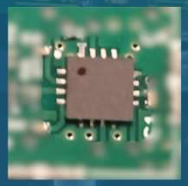
Readily scalable



KETS

Where is KETS?

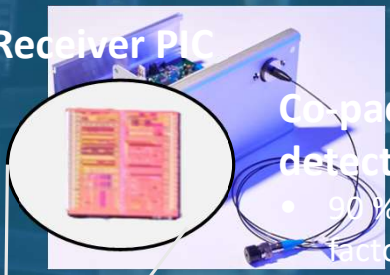




Transmitter PIC
Monolithic PIC to produce qubits. Volume-ready opto-electronic package

QRNG PIC
Optically-self contained QRNG chip. 5mm x 5mm QFN package. 5 Gbps quantum entropy

Detectors



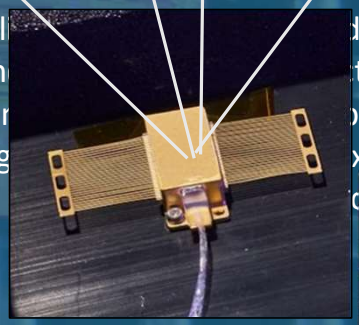
Receiver PIC

Co-packaged PIC and detectors

- 90 % reduction in form factor
- Down to one single optical component at the receiver
- Standard butterfly packaging

Receiver PIC
Monol
in stan
telecor
packag

Detectors
l SPADs
tors with ~ 2
bandwidth in a
x 8 cm x 10 cm

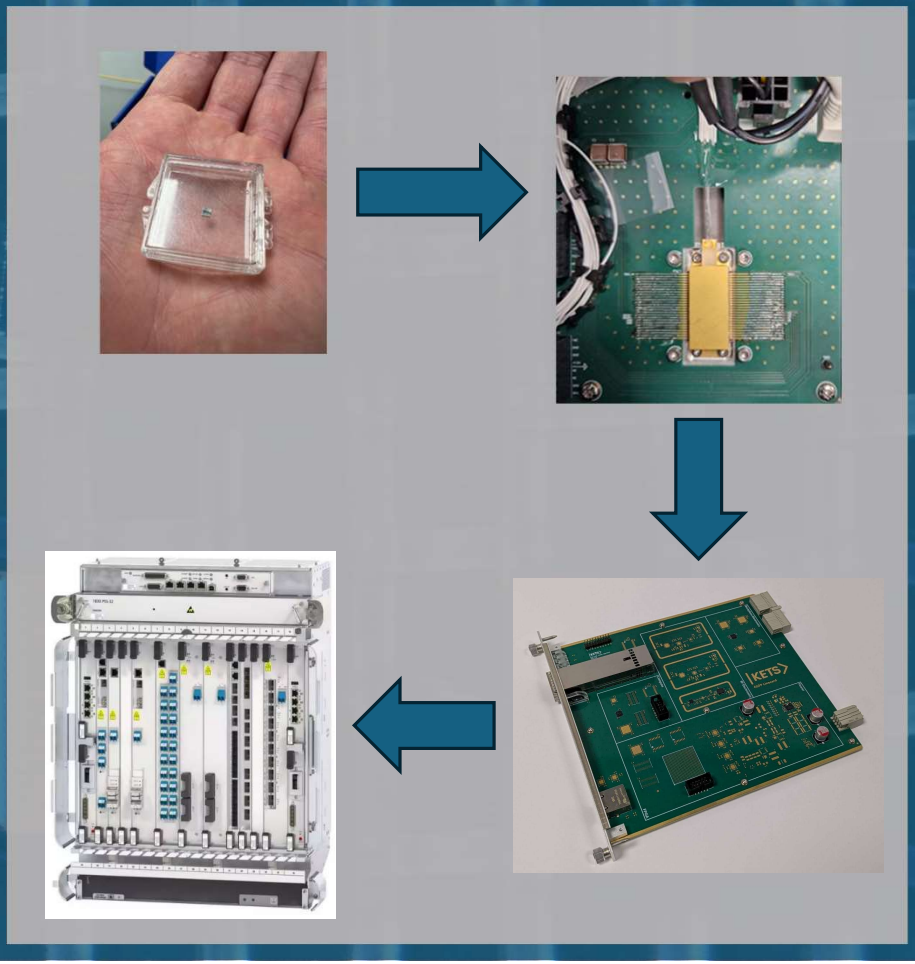


KETS

KETS Vision: QKD as a network feature

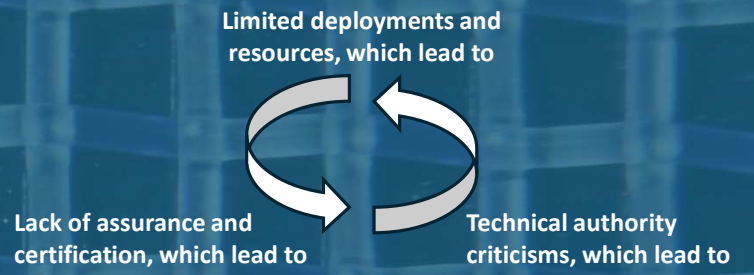
- QKD functionality **embedded inside** standard networking equipment
- Keeps CapEx **and OpEx** costs low
- Integrate into existing deployment and maintenance workflows
- Compatible with established equipment partners
- No adaptations to existing key management layer required

*Delivering a **tightly integrated** quantum-safe solution **at scale** and at **mass-deployable price point***



KETS

Call to action



- ETSI should:
  - clarify the relationship between QKD standards and conformity assessment,
  - align assurance expectations across national regulatory regimes,
  - highlight trusted organisations already capable of evaluating quantum properties (NPL, Nostradamus, NSR/KRISS/TTA/ITSCC) and encourage more,
  - galvanise security agencies / trusted bodies to get involved with certification
  - enable operators to perform defensible cost–risk trade-offs
- Customers need the guidance and assurance that can be provided by certification and guidelines. Without that coming from the QKD space, customers will move forwards without QKD

KETS