# Towards a North American QKD Backbone with Certifiable Security

**Nino Walenta[1], Dario Caselunghe[2], Sylvain Chuard[2], Mathias Domergue[2], Michael Hagerman[1], Randall Hart[1], Don Hayford[1], Raphaël Houlmann[2], Matthieu Legré[2], Todd McCandlish[1], Laurent Monat[2], Alex Morrow[1], Grégoire Ribordy[2], Damien Stucki[2], Maurice Tourville[1], Patrick Trinkler[2], Rick Wolterman[1]**

*[1]Battelle Memorial Institute, 505 King Avenue, 43201-2696 Columbus, Ohio*
*[2]idQuantique S.A., Chemin de la Marbrerie 3, CH-1227 Geneva, Switzerland*
*Author e-mail address: walenta@battelle.org*

**Abstract:** We have developed architecture and hardware for a telecom-compatible QKD network, which allows distributing highly secure symmetric cryptographic keys without any constraints concerning maximum number of users or range, making a scalable and cost-efficient integration of QKD possible on a national scale. The QKD network equipment is compactly integrated in ATCA form factor and has been designed in compliance with security certification standards for information systems. Here, we present our design and first experimental results.

## 1. Introduction

Despite the obvious benefits and strengths of quantum key distribution (QKD) of continuously distributing highly secure symmetric cryptographic keys [1], different reasons have so far hindered its widespread commercial adoption and industrialization. As a potent building-block for information security systems and applications, QKD targets a market which extensively relies on standardized methodologies for independent security evaluation and certification in order to verify correct implementation and increase confidence and trust by users and clients. Although different efforts have been made and are currently ongoing [2, 3], so far no implementation and evaluation standard for QKD systems and their components exist, with restricting consequences on their practical use in production and especially governmental environments which strictly require security certification.

Furthermore, the maximum distance of direct QKD links, limited to a few hundred kilometers, and the physical point-to-point connectivity are too restrictive for its widespread adoption in secure communication infrastructures. While quantum repeaters which can increase the distance are still under development, current approaches to overcome both limitations and enable long-distance QKD in multi-node fiber networks are based on the trusted repeater paradigm and have been demonstrated in e.g. [4-8]. Another important aspect is related to the operational expenses of network security device, which are not only linked to the implementation costs, but also to the physical volume of the hardware and its easy integration into existing infrastructures and workflow of clients. Hence, reducing the volume of QKD device and using widely used, familiar hardware standards also reduces the operational expenses of this technology and foster market acceptance.

Based on careful analysis of the expectations from potential users we have designed an architecture framework and developed the respective hardware which addresses all aforementioned limitations. Our approach for a telecom-compatible QKD trusted node network removes any constraints concerning number of users or range, making a scalable and cost-efficient integration of QKD possible on a national scale. Its hardware is compactly integrated in small-size ATCA (Advanced Telecommunications Computing Architecture) modules, and, importantly, has been designed to comply with existing security certification standards for information systems, such as FIPS 140-2 (security level 3), ISO/IEC 19790 and Common Criteria (EAL 4). At the frontier between QKD technology and information security market, the results of our development not only broaden the research scope within the QKD community, but also help further reducing gaps to the telecommunication and security industries by tailoring QKD technology closer to their needs.

## 2. The QKD network system

The approach taken here is a modification of the trusted node (TN) paradigm. In the presented architecture as sketched in Figure 1, secret user keys (labeled *K* in Figure 1) are distributed between any two network nodes by hopping over intermediate nodes while being two-fold protected. First, highly secure QKD keys (labeled *QK* in Figure 1) are continuously distributed between adjacent nodes, and used to protect the end user keys while they hop from node to node via a public network. Due to the symmetric encryption with QKD keys, this protection layer ensures the quantum-safe forward security of the user key transmission. In extension to other trusted repeater QKD networks, an additional second layer of encryption based on conventional public key cryptography (labeled *PK* in Figure 1) increases the protection within intermediate nodes and facilitates compliance with certification standards.

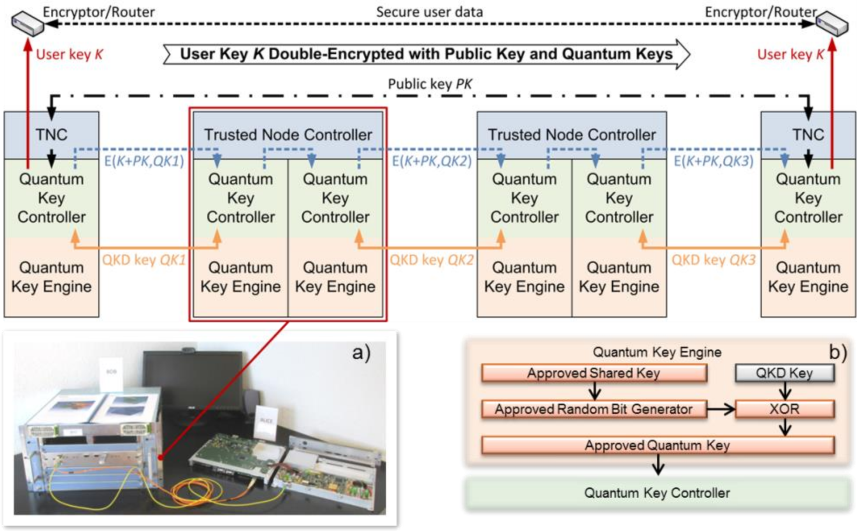

Figure 1. Top: Principle of TN-QKD for secure key distribution between two users (see text for details). E(*x*, *y*) denotes symmetric encryption of *x* using *y*. Inset a) shows an ATCA based TN-QKD node, configured with a single Bob quantum blade (left), and an opened Alice quantum blade with its quantum key controller and quantum key engine including all optical components (right). Inset b) illustrates our approved method for generating quantum keys in compliance with the FIPS 140-2 certification standard.

For seamlessly integration into existing telecommunication infrastructures, the node hardware is implemented in the ATCA form factor, an equipment standard widely used in the US telecom industry that provides standardized mechanical, power and data interfaces, and a scalable architecture. Each individual node is housed in an ATCA shelf with a redundant Trusted Node Controller (TNC), and can be configured with multiple quantum blades depending on the desired network topology. The TNC provides administration interfaces, is responsible for node discovery, but most importantly provides route tables of the QKD network for routing and managing key transactions between blades within a node and with remote nodes. It uses a dynamic routing algorithm based on the Dijkstra least cost path algorithm [9] and chooses alternate routes or multiple paths when available in order to balance security and quality of service without the need of a centralized server.

Depending on the number of adjacent nodes, each ATCA shelf node comprises in addition to the TNC several quantum blades which realize the QKD links and provide the cryptographic functionalities to securely distribute the user keys across the network. This flexible configuration of individual nodes allows implementing not only a simple chain network topology as exemplarily sketched in Figure 1, but any much more complex topology as required in a specific scenario while maintaining a small footprint. Each quantum blade comprises a quantum key engine (QKE) for the actual QKD links and quantum random number generation, and a quantum key controller (QKC). The QKC contains a high security module, which stores all critical security parameters including the quantum keys continuously provided by the QKE in an encrypted memory, and actively zeroizes them in response to a tamper-detection. The QKC also performs all cryptographic functions like encryption and decryption with the public keys of the end nodes and the QKD keys provided by the QKE in order to securely send the user keys over the network.

While the principle architecture is independent of the underlying QKD protocol and allows adoption of different QKD systems in one network, our quantum key engine is based on a 625 MHz clocked implementation of the coherent one-way (COW) QKD protocol (see [10] and references therein). It features an FPGA (field-programmable gate array) based key distillation engine, commercial free-running detector modules and quantum entropy sources, and is compatible with wavelength-division multiplexing technologies to operate, at minimum, over only one fiber. The FPGA-based key distillation engine uses a block size of $10^6$ bit keys and allows secret key rates up to 4 Mbit/s. Real-time forward error correction is based on low-density parity-check codes, and privacy amplification uses universal hashing with Toeplitz matrices. The QKD service channel is Wegman-Carter authenticated, using QKD keys for one-time pad encryption of the authentication tags. The total QKD security parameter is $\varepsilon = 4 \cdot 10^{-9}$. As shown in inset b) of Figure 1, the QKE further applies a bitwise XOR between the QKD key and an additional key which has been shared between both quantum blades of a QKD link using an approved method. This method renders the QKD key compliant with the requirements by the security certification standards for its approved use in certified security systems, while importantly it maintains the information-theoretical security of the QKD key.

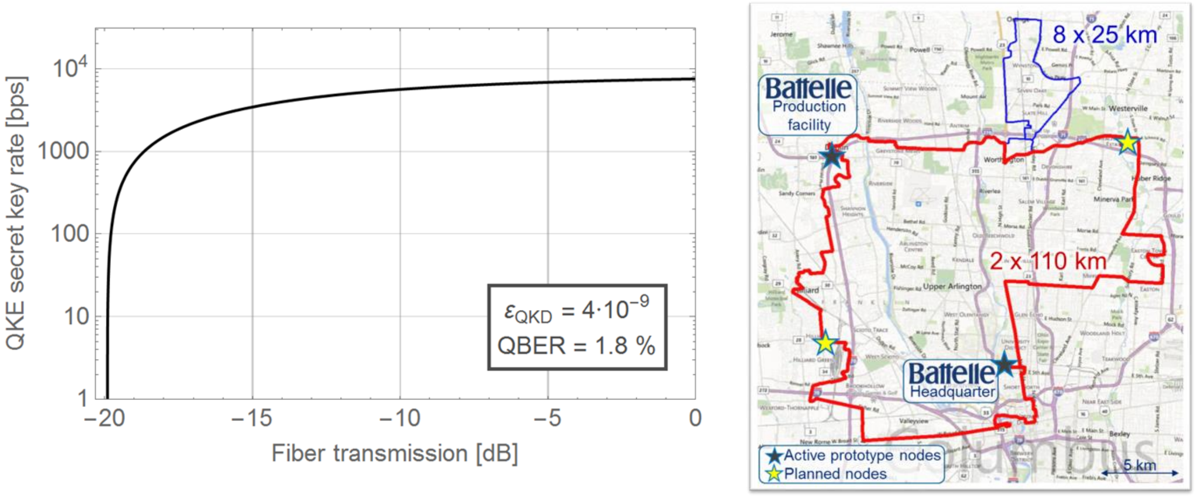

Figure 2. Left: Results of the design validation for the ATCA quantum blades based on a quantum key engine implementing the COW QKD protocol. Right: Layout of the Battelle QKD fiber network in the metropolitan area of Columbus (Ohio), which currently employs commercial QKD systems (Cerberis, idQuantique) to protect all communication between Battelle's headquarters and its production facility in Dublin (Ohio).

## 3. Results and outlook

As shown on the right of inset a) in Figure 1, all security relevant hardware and modules including the QKC and QKE with its quantum random number generator, QKD distillation hardware, single photon detectors and all other optical components, are completely encapsulated by a metallic, tamper-resistant enclosure in compliance with highest security standards for cryptographic modules. Each quantum blade measures only 322 x 280 x 61 mm$^3$, being the smallest volume of a complete QKD system demonstrated to date.

In a first experimental validation with all hardware and optics implemented in the ATCA quantum blades, the quantum key engine provides a QKD secret key rate of more than 1 kbit/s over fiber links with less than -19 dB fiber transmission as shown in Figure 2 (left). Note that here we optimized the system and detector parameters for -16 dB transmission, but higher key rates over lower losses are possible by adapting these parameters.

In order to accompany and facilitate the development of our Trusted Node network, Battelle established in the metropolitan area of Columbus (Ohio) the first commercially funded QKD network in the US, which is operational since September 2013 and open for researchers in the field on a non-profit basis. It comprises over 400 km of dark fibers, with one pair in a 100 km metropolitan sized loop around Columbus, and eight dark fibers in a 25 km loop (Figure 2, right). Over the next months we will deploy the new ATCA based trusted node hardware in this QKD network for field tests, and eventually replace the currently used commercial QKD systems (Cerberis, IDQ) to protect all of Battelle's communication between its different sites in the area. In subsequent phases, the network will be gradually extended to connect further Battelle facilities in the U.S.

## References

[1] N. Gisin, G. Ribordy, W. Tittel, H. Zbinden. "Quantum cryptography". *Review of Modern Physics* **74**, 145 (2002).

[2] T. Länger, G. Lenhart. "Standardization of quantum key distribution and the ETSI standardization initiative ISG-QKD". New Journal of Physics **11**, 055051 (2009).

[3] ETSI QKD Industry Specification Group. www.etsi.org/technologies-clusters/technologies/quantum-key-distribution

[4] M. Peev et al. "The SECOQC quantum key distribution network in Vienna". *New Journal of Physics* **11**, 075001 (2009).

[5] D. Stucki et al. "Long-term performance of the SwissQuantum quantum key distribution network in a field environment". *New Journal of Physics* **13**, 123001 (2011).

[6] M. Sasaki et al. "Field test of quantum key distribution in the Tokyo QKD Network". *Opt. Express* **19** (11), 10387 (2011).

[7] R. J. Hughes et al. "Network-Centric Quantum Communications with Application to Critical Infrastructure Protection". *arXiv*:1305.0305 [quant-ph] (2013).

[8] S. Wang et al. "Field and long-term demonstration of a wide area quantum key distribution network". *Opt. Express* **22** (18), 21739 (2014).

[9] E. W. Dijkstra, "A note on two problems in connexion with graphs". *Numerische Mathematik* **1**, 269-271 (1959).

[10] N. Walenta et al. "A fast and versatile quantum key distribution system with hardware key distillation and wavelength multiplexing". *New Journal of Physics* **16**, 013047 (2014).