Redefining Security

QUANTUM-SAFE SECURITY APPLICATION NOTE

Quantum Technologies for 5G

February 2019

ID QUANTIQUE SA
Chemin de la Marbrerie 3
1227 Carouge/Geneva
Switzerland
T +41 22 301 83 71
F +41 22 301 89 79
info@idquantique.com
www.idquantique.com

Table of contents

ID Quantique SA

Ch. de la Marbrerie, 3

1227 Carouge

Switzerland

Tel: +41 (0)22 301 83 71

Fax: +41 (0)22 301 83 79

www.idquantique.com

info@idquantique.com

Information in this document is subject to change without notice.

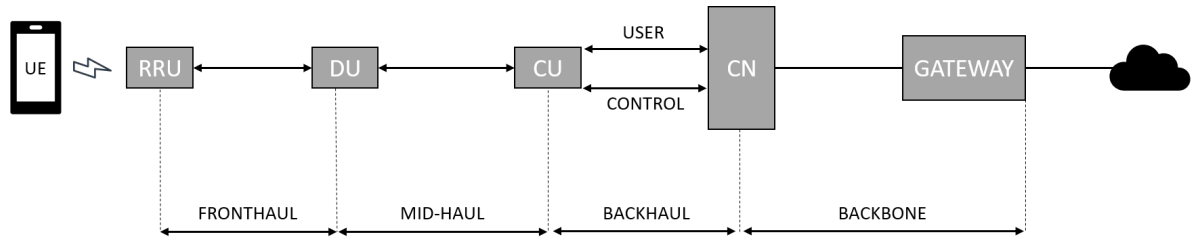
Introduction

The objective of this application note is to explain why it is critical for Telecom Service Providers (TSP) to define a quantum-safe strategy when rolling out 5G mobile networks. ID Quantique has developed quantum-safe solutions enabling TSPs to provide quantum-safe services to their customers. This document focuses specifically on securing fibre optical networks by implementing Quantum Cryptography, also known as Quantum Key Distribution (QKD), and using Quantum Random Number Generation (QRNG) on the radio link to strengthen existing security mechanisms. However, various quantum-safe solutions would potentially apply to other components of the 5G networks. The final objective is to ensure that the end-to-end mobile communications are quantum-safe.

Overview of 5G architecture

Although the 5G standard is not completely finalised and network architectures may vary between mobile networks, the objective of this section is to provide a working definition of the main elements of a 5G network[1] . The standard should be fully finalised by the ITU in 2020 (IMT-2020 focus group[2]).

For the purposes of this application note, we consider a 5G mobile network to made up of the UE (User Equipment), Remote Radio Unit (RRU), Distribution Unit (DU), Central Unit (CU), CN (Core Network) and Gateway connecting mobile users to Internet and other network providers.



5G architecture overview

[1] https://www.itu.int/dms_pub/itu-t/opb/tut/T-TUT-HOME-2018-PDF-E.pdf

[2] https://www.itu.int/en/ITU-T/focusgroups/imt-2020/pages/default.aspx

ID QUANTIQUE SA
Chemin de la Marbrerie 3
1227 Carouge/Geneva
Switzerland
T +41 22 301 83 71
F +41 22 301 89 79
info@idquantique.com
www.idquantique.com

Security, a rising concern in mobile networks

Although mobile networks were initially designed to provide mobile voice services, overtime data services such as internet, file transfers, and streaming have now become the primary usage - not only for consumers but also for private and public organisations. Consequently, the volume and criticality of data carried over mobile networks has increased significantly, and it will continue to do so with the next mobile generation under development. Indeed, 5G is aiming to be the main network used for connected vehicles, Internet of Things (smart offices, cities, factories, home), and, of course, to also connect people. Critical data is transmitted over mobile networks by enterprise and government. Applications in the medical, critical infrastructure, military and transportation fields will use 5G which means that human lives become dependent on the mobile network. Therefore, 5G requires the highest level of security available when being designed and deployed. This is obviously acknowledged and recognised by 5G standard institutes[3]. Among the various security topics, this application note focuses on quantum cryptography in 5G networks. These networks should remain robust against quantum attacks for the next 20 years, when quantum computers are expected to be available on the market, making it critical to think and act now.

5G networks, key component of the hyper-interconnected world, present new defence challenges:

- **Rapid advancements in technology** will add new attack vectors which were not conceived of or were not feasible at the time mobile networks were originally deployed. For instance, SIM cards are prone to massive remote hacking[4].
- The **scalability of the attack vectors** is unprecedented, where a single successful hack could affect millions of devices[5]. So far, such attacks have been relatively benign, but this could change. This means that many previously isolated or siloed systems and devices forcibly become part of a networked critical infrastructure. For example, in the past, if one car crashed it was a matter for the police and possibly an ambulance. However, in the world of ubiquitous IoT, if a hack can cause an entire smart city infrastructure to fail, or the entire self-driving car or rail network to go down, then it becomes an issue of national security.

Why a mobile service should be quantum-safe?

Recent breakthroughs in quantum computing have brought about a credible threat to the widely-used cryptographic primitives which underpin our infrastructures and networks – notably to public key cryptography, such as RSA, Elliptic Curve Cryptography & Diffie Hellmann. Scientists have known about this threat since 1994 when a mathematician, Peter Shor, published his now-famous quantum

[3] https://5g-ppp.eu/new-security-group-5g-ppp-white-paper-phase-1-security-landscape/

[4] https://srlabs.de/bites/rooting-sim-cards/

[5] https://www.enisa.europa.eu/publications/info-notes/major-ddos-attacks-involving-iot-devices

ID QUANTIQUE SA
Chemin de la Marbrerie 3
1227 Carouge/Geneva
Switzerland
T +41 22 301 83 71
F +41 22 301 89 79
info@idquantique.com
www.idquantique.com

algorithm for factoring large numbers into primes and finding discrete logarithms much faster than any classical algorithm. These are precisely the mathematical problems underpinning the above-mentioned primitives. A quantum computer running Shor's algorithm will therefore break all the cryptographic systems based on these primitives.

The exponential speed-up brought about by quantum computers stems from the fact that they act as massively parallel computers. This is made possible by a weirdness of quantum mechanics known as "superposition". Crudely put, it is the ability for a quantum bit (or qubit) to be both a one and a zero at the same time. Properly implemented (and this is by no means an easy task), this weird property extends to any numbers of qubits. Ultimately, the whole quantum computer can now be in a superposition state, which provides exponential computing power.

Although thought of as a futuristic technology, quantum computers already exist – albeit with a restricted number of qubits and great engineering challenges to overcome. IBM has launched the first quantum computing cloud, which allows external users to experiment with a small number of qubits[6]. Google has set itself a target for proving quantum supremacy (the ability of a quantum computer to resolve certain problems faster than the best available conventional processors)[7]. D-Wave was the earliest to market and has already launched its 2000Q System quantum computer which – luckily for today's security – uses a quantum computing process which cannot run Shor's algorithm.

So, the question is: when will a universal quantum computer run Shor's algorithm (or any variation thereof) on enough quality qubits to be able to break today's crypto primitives? One estimation is provided by Dr Michele Mosca from the Institute for Quantum Computing in Canada, who also runs a quantum risk assessment practice[8]: he estimates that large-scale quantum computing is a decade away, and that there is a 1 in 7 chance of crypto primitives being affected by quantum attacks in 2026, and a 1 in 2 chance by 2031.

This may sound a long time away but given the timescales for developing and deploying new mobile network generations – which are in the field for 20+ years (2G was launched in the nineties), it is critical to start preparing the 5G quantum-safe network now.

Data is considered as a key asset by many companies and may need to be protected for 10+ years. This is even more significant when it gets to protect government secrets (50 years), and medical data or intellectual property (lifetime). Data sovereignty laws such as GDPR are very strict concerning data protections and are associated to potential penalties (fines of up to 4% of global revenues). Additionally, there is the threat of "store now, decrypt later" which is a major concern for most organisations. These are fundamental justifications to implement quantum-safe solutions today, and not to wait any longer.

[6] https://www.forbes.com/sites/aarontilley/2017/03/06/ibm-quantum-computing-cloud/#4d9eba8277a2

[7] https://www.technologyreview.com/s/612381/google-has-enlisted-nasa-to-help-it-prove-quantum-supremacy-within-months/

[8] https://globalriskinstitute.org/publications/3423-2/

Impact on mobile network encryption algorithms

As explained in the previous section, all systems using public-key cryptography such as RSA, DH, ECDSA, or ECDH for authentication or key exchange are not quantum-safe and are used in TLS, DTLS, IKEv2, certificates, and MIKEY-SAKKE. For instance, DTLS protocol, like TLS, uses RSA or DH for the authentication and initial private key exchange[9], even the latest version of TLS v1.3[10] is subject to cryptography breaches[11]. These cryptography solutions are widely used in mobile networks including 5G[12]. DTLS is used in several communications between the mobile network and user equipment, like on the N2 interface carrying the NAS Signaling (Non-Access Stratum) traffic to the UE. Hacking the private key would generate a security breach for DTLS. IKEv2 also is used extensively in mobile networks, an example being the UE authentication (UE-N3IWF).

New cryptographic techniques have emerged in recent decades that do provide protection against quantum threats. These techniques are termed "quantum-safe" and consist of both techniques based on quantum properties of light that prevent interception of messages (Quantum Key Distribution or QKD[13]), as well as new algorithms (known as Quantum Resistant Algorithms – QRA, also sometime referred to a post quantum algorithms) that are believed to be resistant to known quantum attacks, like Shor's. Quantum technologies can also be used to improve the overall safety of mobile networks by improving cryptographic key generation thanks to Quantum Random Number Generators, or QRNGs.

One solution could be to use only quantum resistant algorithms instead of RSA, DH and ECDSA. Even if it would improve the security level significantly, quantum resistant algorithms, when approved and standardised[14] (the process will take another 5 to 7 years), will be resilient to known quantum attacks but may not prove to be permanently quantum-safe. However, using QKD and encryption solutions (quantum cryptography) which are already available today would provide a quantum-safe mobile core optical network and can be combined with QRA when ready[15].

On the other hand, symmetric algorithms such as AKA authentication and the radio encryption algorithms are quantum-safe assuming the secret key are based on truly random generation and are kept secure. 128-bit algorithms such as UEA1, UIA1, UEA2, UIA2, EEA1, EIA1, EEA2, EIA2, EEA3, EIA3, and AES-128 offer sufficient security today but should be upgraded to 256-bit for the coming quantum era. NIST plans to define 256-bit algorithms AES-256 and SHA-256 as quantum-safe. However, the authentication and ciphering algorithms use many keys which should be random and secure. For the

[9] https://tools.ietf.org/html/rfc6347, and https://tools.ietf.org/html/rfc5246

[10] https://tools.ietf.org/html/rfc8446

[11] https://www.zdnet.com/article/new-tls-encryption-busting-attack-also-impacts-the-newer-tls-1-3

[12] https://portal.3gpp.org/desktopmodules/Specifications/SpecificationDetails.aspx?specificationId=3169

[13] For more information on QKD, see: https://www.idquantique.com/quantum-safe-crypto/qkd-overview/

[14] https://csrc.nist.gov/Projects/Post-Quantum-Cryptography

[15] The next section explains how to secure the backbone optical network by introducing Quantum cryptography

encryption, a secret key Ki and a random number runs through an algorithm (A8) to generate a new session Key (Kc). Random numbers are provided by the RAND function (called random challenge).

Random Number Generation (RNG) is essential to all crypto operations. Generating strong keys, based on true randomness, is the cornerstone of security – good keys must be unique, unpredictable and truly random. Having strong crypto algorithms with weak keys is akin to putting a huge padlock on your front door and then hiding the key under the mat[16]. Software-based RNGs are not sufficient, as the computer programs they run are purely deterministic and cannot generate true randomness without external entropy sources. Since many critical infrastructures and IoT deployments are in isolated locations with limited external interaction, such sources of external entropy are limited.

Quantum Random Number Generation is significantly improving the security level of these communications by providing true random numbers instead of pseudo-random numbers input to the symmetric algorithm. QRNG has already been deployed in live mobile networks thanks to the Quantis Appliance integration[17].

The Quantis Appliance was specifically designed to meet the requirements of high availability environments. Using an Ethernet port, the Quantis Appliance is a distributed device that can provide several systems with randomness. It is also an autonomous device, which integrates seamlessly into mobile networks.

Quantum Key Distribution on the 5G backhaul and backbone

The previous section explained how QRNG can significantly improve the security of authentication and ciphering of radio links so that they are ready for the quantum era. In order to provide an end-to-end quantum-safe communication, a solution should be found to solve the Public-Key cryptography quantum weakness that puts the 5G backbone at risk. Moreover, high speed and core links, carrying a high volume of data, are usually considered to have a higher criticality and therefore should benefit from the most secure solutions in the first place. It makes sense to start implementing state-of-the-art security solutions starting at the Core and moving towards the Edge of the Network. Since fibres can easily be tapped and eavesdropped, fibre optical networks need to be encrypted using safe keys. This would inherently benefit the upper network layers.

This section focuses on explaining how encryption combined with Quantum Key Distribution (QKD) can turn an optical 5G backbone into a quantum-safe communication network.

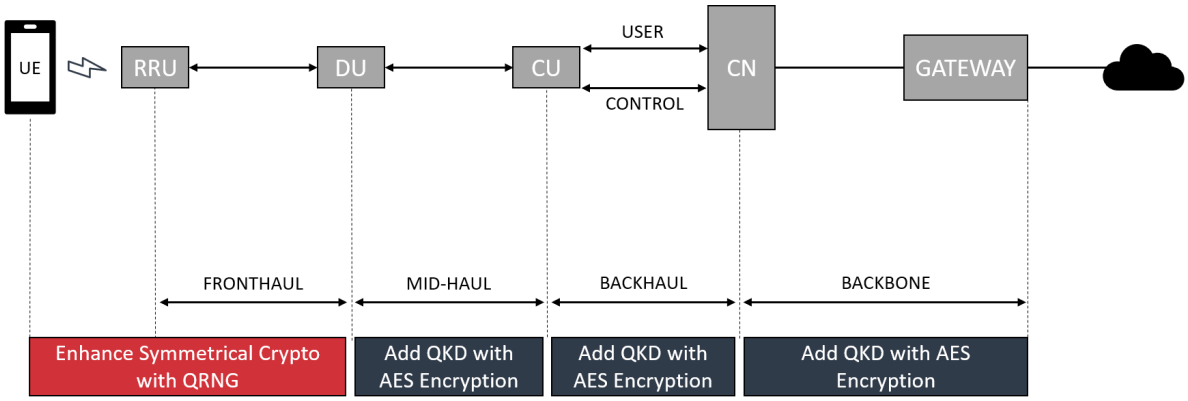
Major Optical Transport Network (OTN) vendors support symmetrical encryption modules (such as AES) on their optical equipment significantly improving the confidentiality of the data. A Public Key Agreement allows for exchanging the master key used to build the session key. However, a main

[16] A more scholarly version of this example is stated in Kerckhoff's principle: "A cryptosystem should be secure even if everything about the system, except the key, Is public knowledge". This encapsulates the importance of the encryption key in crypto systems.

[17] For more information on the QA, see: https://www.idquantique.com/random-number-generation/products/quantis-rng-appliance/

challenge remains: How to ensure that the key exchange and management is quantum-safe? Quantum Key Distribution ensures the exchange of a cryptographic key between two remote parties with proven security, guaranteed by the fundamental laws of physics. The quantum key can be renewed every second, and is then mixed with the standard session key to generate a new quantum-safe session key. This key can then be used securely with conventional (such as AES) or post-quantum cryptographic algorithms implemented into the optical equipment.

Most Backhaul and Backbone 5G network links are implemented over fibre links, meaning QKD can be added logically to the optical network as a key distribution layer.



5G architecture overview with Quantum Technologies

Combining QKD and quantum-safe encryption algorithms (aka quantum cryptography) solves the quantum threat to the core network. The radio links security relies on symmetric cryptography combined with random keys from trusted sources, such as QRNGs.

QKD advantage

Ensuring forward-secrecy for the most sensitive information, QKD works on the intrinsic and proven principles of quantum physics – i.e. that the generation of the quantum key is truly random, and that any interruption or eavesdropping of the data will perturb the system and can thus be detected. Each quantum key is independent and uncorrelated, and automatically updated every minute. Unlike classical encryption based on mathematical algorithms, QKD will not be compromised by mathematical progress or the continued increase in computing power and it is not vulnerable to fibre tapping. The cost of tapping a fibre on a core link is relatively low (a few thousand dollars typically) and provide a good ROI for a hacker. Such attacks are potentially the most dangerous as they are most often not even detected and compromise a large volume of data.

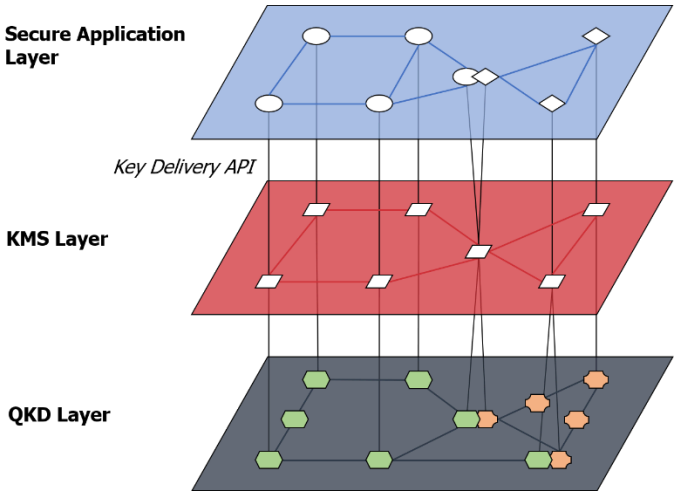
QKD is a quantum-safe technology, which is commercially available and deployed today in production environments.

Standard interface between the KMS and secure application layer

Thanks to an open interface between the OTN encryptors and the QKD platform, the key exchange can occur securely in the Point of Presence. ID Quantique's QKD now also supports the ETSI "GS QKD 014" interface which means that QKD can be added virtually to any compliant Optical Network as an overlay, with minimum impact on the solution already in place. The Key Management System (KMS) Layer ensures the generation, distribution and management of the cryptographic keys for upper devices and application layers.

A REST (REpresentational State Transfer) API is specified as a simple, scalable, widely deployed approach that is familiar to a large developer community. The REST API specifies the format of the URIs, the communication protocols (HTTPS), and the JSON (JavaScript Object Notation) data format encoding of posted parameters and responses, including key material.

REST-based APIs are simple and easy for developers to understand and are popular in many application domains. They have a large developer community and many libraries, implementations, and guidance documents are available to the community. REST-based APIs are lightweight and scale to the "Internet" level regarding both the number of nodes and the number of applications.



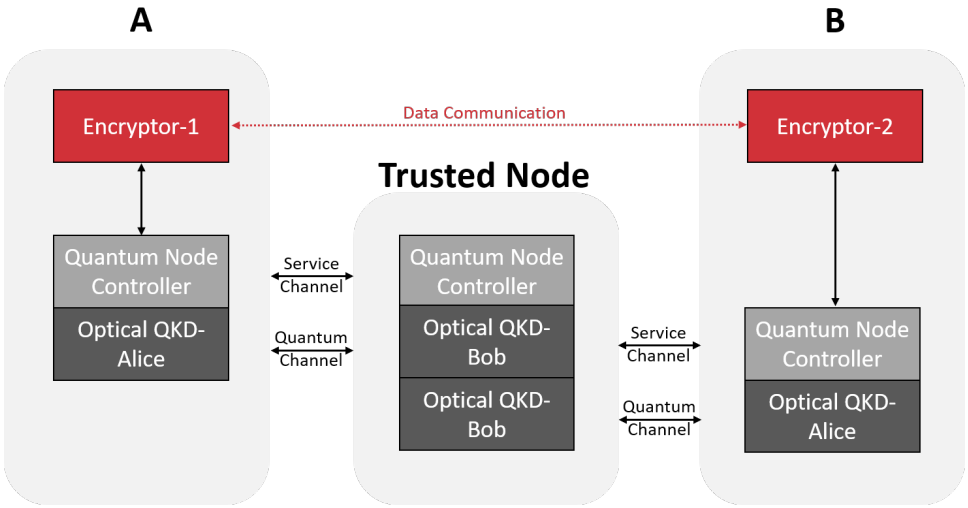
QKD Layer architecture

We can consider the QKD and KMS layer as a new physical and logical layer managing the secure transport and distribution of keys used by upper control, management and data planes, named here

the “Secure Application Layer”. The standard interface facilitates the integration of QKD with existing optical networks.

Trusted nodes

Since QKD has a distance limitation in a production environment of approximately 80 kilometres between 2 nodes (depending on the fibre quality), the concept of Trusted Nodes, positioned in highly secure locations, has been developed in order to extend the reach of the key exchange used by the encryptors. Data centres, for instance, have strict access rules with high security requirements to access the equipment. The Trusted Nodes themselves are also physically secured using standard FIPS level tamper detection (commonly used in Hardware Security Modules) to ensure protection of the keys within. Trusted node deployments have been rolled out now, enabling QKD deployments over nationwide distances. For instance, a live network using ID Quantique technology is running in the UK and more networks are under development over greater distances.



Trusted Node Overview

Beyond point-to-point topologies, ring topologies are now supported, which means that a given QKD node can connect to a remote QKD node through trusted nodes with add/drop or forward capabilities. Thanks to the KMS layer, other designs such as star or mesh topologies are also considered. The QKD design can now be mapped to the optical network design to ensure the secure key exchange between all optical nodes.

ID QUANTIQUE SA
Chemin de la Marbrerie 3
1227 Carouge/Geneva
Switzerland
T +41 22 301 83 71
F +41 22 301 89 79
info@idquantique.com
www.idquantique.com

WDM advantage

On top of the data communication channel, QKD uses a quantum channel exchanging quantum keys and a service channel for the communication between the Quantum Node Controller (QNC). By default, it is recommended to use a dedicated fibre network for the quantum channel to allow for longer distance between nodes. However, it is possible to optimise the use of the fibre infrastructure thanks to WDM.

Multiplexing the quantum channel with the service and data channel is technically possible although it significantly reduces the transmission distance. Indeed, the quantum, service and data channel do not have the same transmission requirements. However, in some cases (last mile for instance), where there is low fibre availability and shorter distances, it might be the optimal solution. Therefore, QKD on a single fibre has also been tested and deployed successfully over distances of up to 40 km by ID Quantique.

Value proposition for telecom service providers

Proposing a quantum-safe state-of-the-art solution is clearly a major differentiator in today's world. Many customers are sensitive to the security level of their communication and data. They need to trust that their service provider can support and offer the latest security technologies such as quantum cryptography.

Telecom Service Providers are uniquely positioned to propose the extra layer of security combining Quantum Key Distribution and Key Management Service Layer as an overlay of the existing network. Although this application note focuses on the optical transport of a 5G network, the QKD layer can actually benefit any application requiring secure keys for authentication or ciphering algorithms.

While there is a strong pressure on fixed and mobile network service pricing, QKD services can create a new value proposition on top of fibre optical networks by providing a higher level of security that is intrinsically quantum-safe. Some industries such as finance, banking, governments and healthcare have already recognised the value of quantum cryptography services. This is also a major differentiator compared to Over-The-Top service (OTT) providers mainly focussing on software-based solutions.

The expansion of optical networks up to the user location (Fibre-To-The-Home / Office / Building / Enterprise), is an enabler for offering QKD services up to the customer location or up to the Radio link of 5G networks. It only makes sense if the core network is already equipped with QKD, so that an end-to-end quantum-safe service is guaranteed.

As quantum computers are becoming more powerful, the threat increases and the time available to design and implement quantum-safe solutions is reduced. Service providers who have anticipated the introduction of this technology in their 5G network will benefit from a key advantage versus the competition, especially for supporting IoT and critical applications.

Conclusion

As explained in this application note, the development of quantum computers capable of breaking public-key cryptography increases the risk to data communication including upcoming 5G network services. ID Quantique's objective is to propose end-to-end quantum security solutions to 5G mobile providers. Two main challenges have been identified: securing public-key cryptography used in the 5G fibre optic backbone and improving the randomness in symmetric key-generation on the radio link.

Using a Quantum Random Number Generator, such as the Quantis Appliance, for the key generation process would increase the security level of the radio links. Some mobile providers have already implemented such a solution.

On the Backbone side of the network, Quantum Key Distribution (QKD) combined with the Key Management Layer would ensure a provably secure exchange of the secret keys in real time with the secure application layer thanks to a standardised interface.

Starting from the core towards the edge of the network is the logic adopted by some mobile providers, who started to validate the solution on live networks.

Comparing the estimated timelines between the commercial launch of the quantum computer, and the life time of the future 5G mobile services, it is critical that the design and rollout of new mobile networks should adopt quantum-safe technologies available from the beginning.

ID QUANTIQUE SA
Chemin de la Marbrerie 3
1227 Carouge/Geneva
Switzerland
T +41 22 301 83 71
F +41 22 301 89 79
info@idquantique.com
www.idquantique.com