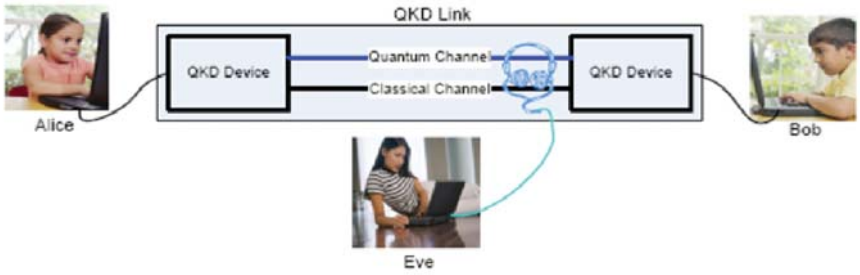
Quantum Key Distribution

During recent years quantum cryptography has been the object of vivid activity and rapid progress, and it is now extending into a competitive industry with commercial products.

It sounds like science fiction, but quantum key distribution will bring new levels of confidentiality and privacy of communication in the future ICT world and thus become the river for the success of numerous services in the fields of e-government, e-commerce, e-health, transmission of biometric data, intelligent transport systems and many others. Due to the ashtonishing effects of quantum physics, quantum encrypted messages are totally immune from eavesdropping. Its power stems from the fact that quantum communication allows for a new primitive, which permits two parties to establish a secret key from a short pre-shared secret and a public exchange, something that was never possible with classical, non-quantum means.



1. Alice generates a random stream of classical bits and encodes them into a sequence of non-orthogonal quantum states of light, sent over the quantum channel

2. Bob performs some appropriate measurements leading him to share some classical data correlated with Alice's bit stream upon reception of those quantum states

3. The classical channel tests these correlations

If the correlations are high enough, it is statistically implied that no significant eavesdropping has taken place on the quantum channel and thus, with very high probability, a perfectly secure symmetric key can be distilled from the correlated data shared by Alice and Bob. Otherwise, the key generation process has to be aborted and started again. The speed with which the key buffer empties is a strong indication to Alice and Bob if an Eve is present or not.

Analysing the cryptographic implications of Quantum Key Distribution is a very complex task. It requires a combination of knowledge belonging to separate academic and industry communities, ranging from classical cryptography to fundamental quantum mechanics and network security. ETSI's newly-launched Quantum Key Distribution (QKD) initiative is aimed at successfully transferring quantum cryptography out of the controlled and trusted environment of experimental laboratories into the real world, where business requirements, malevolent attackers, and societal and legal norms have to be respected.

As a cryptographic tool, QKD is unconditionally secure, able to deliver provable security even in the face of attackers with unlimited computational power. QKD is vastly superior to current key systems such as those used in the Secure Socket Layer protocol and the Internet Key Exchange protocol (IKE). Used in point-to-point schemes, QKD can form the essential building block for unconditionally secure communication.

ETSI's QKD Industry Specification Group

A number of industrial players, both ETSI members and non-members, have already heavily invested in QKD R&D as part of projects under the umbrella of the European Union's Framework Programs 6 and 7.

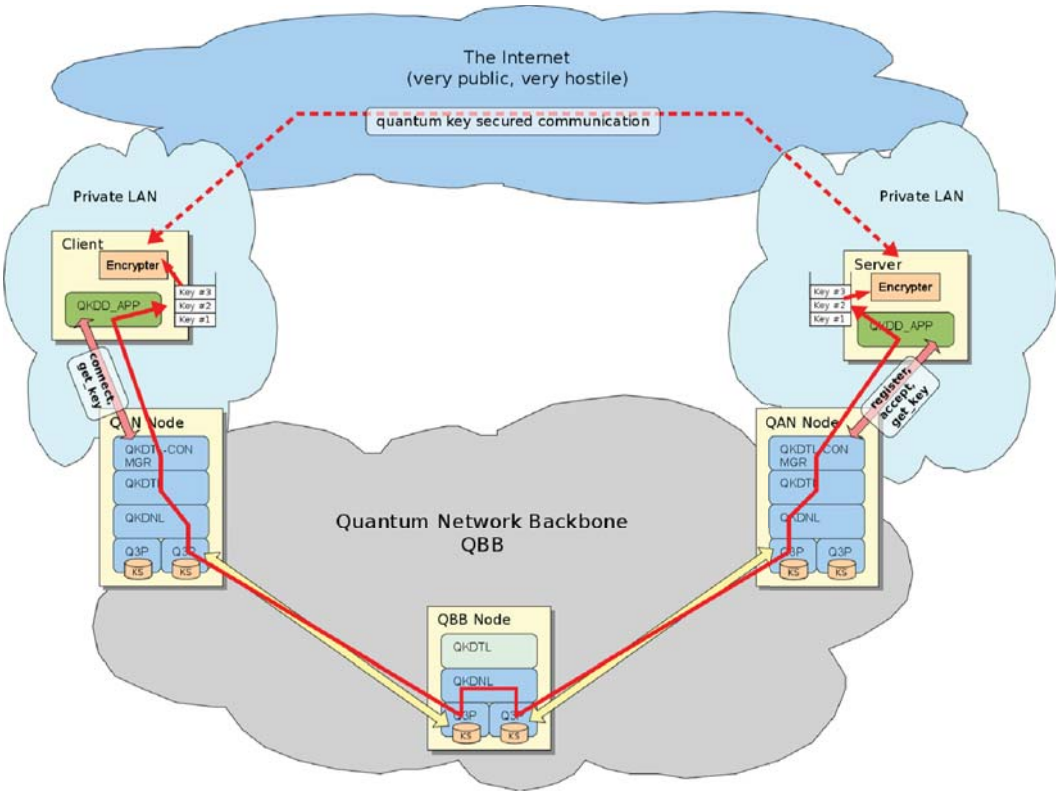
The FP6 SECOQC project, for example, was the leading European research activity on QKD, and most of its members have been behind the establishment of a QKD Industry Specification Group (ISG) at ETSI.

An important goal of the group's activity is to bring the scientists and prospective commercial users together to allow them to learn from each other what the technology is able to deliver and what is needed for practical application.

ISGs supplement ETSI's conventional standards development process and provide a mechanism for the speedy preparation of technical requirements or specifications for well-defined, specific issues, typically in response to a need expressed by a subset of the ETSI membership.

Membership of the QKD group is open to ETSI members and other companies who agree to sign the relevant ISG Agreement.

Functional QKD Architecture



For further details on QKD please visit: http://www.etsi.org/qkd

Q4 2015

ETSI produces globally-applicable standards for Information and Communications Technologies (ICT), including fixed, mobile, radio, converged, aeronautical, broadcast and internet technologies and is officially recognized by the European Union as a European Standards Organization. ETSI is an independent, not-for-profit association whose more than 800 member companies and organizations, drawn from 64 countries worldwide, determine its work programme and participate directly in its work.

For further information, please visit: www.etsi.org

ETSI, 650 Route des Lucioles, 06921 Sophia Antipolis Cedex, France. Tel: +33 (0)4 92 94 42 00 - info@etsi.org