ETSI GS QKD 002 V1.1.1 (2010-06)

Group Specification

Quantum Key Distribution;
Use Cases

Reference

DGS/QKD-0002_UserReqs

Keywords

quantum cryptography, quantum key distribution,
use case

ETSI

650 Route des Lucioles
F-06921 Sophia Antipolis Cedex - FRANCE

Tel.: +33 4 92 94 42 00 Fax: +33 4 93 65 47 16

Siret N° 348 623 562 00017 - NAF 742 C
Association à but non lucratif enregistrée à la
Sous-Préfecture de Grasse (06) N° 7803/88

Important notice

Copyright Notification

Contents

Intellectual Property Rights

IPRs essential or potentially essential to the present document may have been declared to ETSI. The information pertaining to these essential IPRs, if any, is publicly available for **ETSI members and non-members**, and can be found in ETSI SR 000 314: *"Intellectual Property Rights (IPRs); Essential, or potentially Essential, IPRs notified to ETSI in respect of ETSI standards"*, which is available from the ETSI Secretariat. Latest updates are available on the ETSI Web server (http://webapp.etsi.org/IPR/home.asp).

Pursuant to the ETSI IPR Policy, no investigation, including IPR searches, has been carried out by ETSI. No guarantee can be given as to the existence of other IPRs not referenced in ETSI SR 000 314 (or the updates on the ETSI Web server) which are, or may be, or may become, essential to the present document.

Foreword to the Present 1st Edition

This Group Specification (GS) has been produced by ETSI Industry Specification (ISG) Group Quantum Key Distribution (QKD).

This is the first edition of the ‘Quantum Key Distribution; Use Cases' Group Specification. For that reason, the present document contains introductory clauses *not common to typical use cases Group Specifications*. These parts shall at the present time provide to the reader an introduction on QKD as cryptographic primitive, as well as an introduction to the work program of the ISG-QKD. These clauses shall be removed (or moved to other Group Specifications) in future releases.

At the same time, the present document lacks clauses which are *common to typical use cases Group Specifications*. This reflects the fact that QKD as technology on the whole is subject to ongoing scientific research and development. Yet, these parts are properly identified and shall be supplied in future releases of the present document.

According to the implementation plan, the present document will be superseded with a new revision in November 2010.

In detail the aforementioned clauses are:

- The introduction 1.2 **'QKD versus Other Solutions':** This clause provides an introduction to the technology used in QKD, as well as a classification of QKD as cryptographic primitive. Moreover, the security which can be achieved with QKD is discussed. This clause will later be moved to the Group Specification 'QKD; Ontology, vocabulary, and terms of reference', which is currently under development in work item WI7 of the ISG_QKD.

- The overview 1.1 **'QKD Evaluation Context':** This overview, including the work item numbers in Figure 1, is not exactly appropriate for a Group Specification. Yet, the additional information presented in this clause is essential for understanding the overall context of the work towards a framework for security certification of QKD systems, as it is performed by the ETSI ISG-QKD. Future releases of the present document will have this clause removed (and moved to the Group Specification 'QKD; Ontology, vocabulary, and terms of reference').

- The present document lacks the '**Definitions**' as well as the '**Abbreviations**' clause (clause 3). These clauses were completely removed from the document as they are not necessary since all terminology has been harmonized to the vocabulary in the "QKD: Ontology, Vocabulary, Terms of Reference" group specification (GS), which is currently under development. These clauses are not crucial for the understanding of the present document as particular attention was paid to explain technical terms and abbreviations whenever they appear first in the text.

- Although the ultimate goal of the 'QKD; Use Cases' Group Specification is to derive functional requirements from the listed use cases, the 'Requirements' clause of clause 7 is completely left blank for the present first issue of the GS. This is owed to the fact that the present document is the first effort towards a systematic collection of use cases for QKD and will likely be strongly revised until its next release in November 2010.

- A scenario workshop with representatives from potential users, customers, system integrators, as well as policy and decision makers shall be organized for June 22, 2010. One of the main goals of the scenario workshop is to discuss and revise the six use cases presented in the present document. The use cases shall subsequently be adapted according to the findings of the workshop and requirements derived for the November 2010 2nd issue of the 'QKD; Use Cases' Group Specification.

1 Scope

The Use Cases Document shall provide an overview of possible application scenarios in which Quantum Key Distribution (QKD) systems ([i.1]) can be used as building blocks for high security Information and communication technology (ICT) systems.

QKD systems are commercially available today - there are a handful of small enterprises producing and selling QKD systems. Even more QKD systems are being developed in research laboratories of big enterprises and at research centers and universities. All these systems have in common, that they consist of two units, usually for 19" rack mount, connected by a quantum channel of up to 100 km - either optical telecom fiber, or a free space channel through-the-air between two telescopes. They use quantum physical properties of light to generate and simultaneously output identical but random bit strings in the two units on both ends of the quantum channel.

The output of a QKD system can serve as a shared secret in any computer security system from which cryptographic key can be generated.

The laws of quantum physics ensure that it is virtually impossible to eavesdrop on this key distribution process on the quantum channel without the two stations immediately noticing it ([i.3] and [i.4]). More precisely, QKD systems never output insecure key. The net effect of eavesdropping is a decrease, or eventually, a stop in the key output. The degree of security of the keys is cryptographically denoted as "information-theoretical security". In broad terms this implies that the key is almost perfectly random, while the state of knowledge of the eavesdropper is almost zero. The deviations of these "ideal properties" are measurable and it is in the hand of the legitimate operators to make them arbitrarily small at the expense of a small reduction in the key generation rate.

The actual implementations of the QKD devices vary strongly and belong to a number of broad technological realization classes: discrete variable realizations, continuous variable realization, and distributed phase-reference realizations (for a detailed technical description of QKD, see [i.2], [i.12] and the documents referenced therein). However, the basic functionality of a QKD system as an information-theoretically secure key-distribution facility is universal. All these implementations have an optical subsystem with components used for the preparation and measurement of quantum information in photons of light, as well as complex computer systems for transforming measured results into digital data. These implementations are, like any security system, subject to several side channels through which information may eventually leak out of a secure boundary. Besides the showcase "use cases", the present document presents the specifications and mechanisms for driving development towards a security certification of QKD systems - an indispensable requirement for their qualified and dependable use.

2 References

References are either specific (identified by date of publication and/or edition number or version number) or non-specific. For specific references,only the cited version applies. For non-specific references, the latest version of the referenced document (including any amendments) applies.

Referenced documents which are not found to be publicly available in the expected location might be found at http://docbox.etsi.org/Reference.

NOTE: While any hyperlinks included in this clause were valid at the time of publication ETSI cannot guarantee their long term validity.

2.1 Normative references

The following referenced documents are necessary for the application of the present document.

Not applicable.

2.2 Informative references

The following referenced documents are not necessary for the application of the present document but they assist the user with regard to a particular subject area.

[i.1] "Quantum Cryptography: Public Key Distribution and Coin Tossing, Proceedings of IEEE International Conference on Computers Systems and Signal Processing", Bangalore India, C.H. Bennett and G. Brassard, December 1984, pp 175-179.

NOTE: Online at http://www.research.ibm.com/people/b/bennetc/bennettc198469790513.pdf.

[i.2] "Quantum cryptography, Reviews of Modern Physics", Nicolas Gisin, Grégoire Ribordy, Wolfgang Tittel and Hugo Zbinden, Vol 74, 145-195 (2002).

NOTE: Online at http://www.gap-optique.unige.ch/Publications/PDF/QC.pdf.

[i.3] "The security of practical quantum key distribution", Valerio Scarani, Helle Bechmann-Pasquinucci, Nicolas J. Cerf, Miloslav Dušek, Norbert Lütkenhaus, and Momtchil Peev, Vol. 81, 1301-1351 (2009).

NOTE: Online at http://arxiv.org/abs/0802.4155.

[i.4] "Security of quantum key distribution with imperfect devices", D. Gottesman, H.-K. Lo, N. Lütkenhaus, and J. Preskill,Vol. 5, 325-360) (2004).

NOTE: Available at http://arxiv.org/abs/quant-ph/0212066.

[i.5] "White Paper on Quantum Key Distribution and Cryptography", Preprint arXiv:quant-ph/0701168, Alléaume R, Bouda J, Branciard C, Debuisschert T, Dianati M, Gisin N, Godfrey M, Grangier Ph, Länger T, Leverrier A, Lütkenhaus N, Painchault P, Peev M, Poppe A, Pornin Th, Rarity J, Renner R, Ribordy G, Riguidel M, Salvail L, Shields A, Weinfurter H, Zeilinge, A, 2006 SECOQC.

[i.6] UQC Report: "Updating Quantum Cryptography", Quantum Physics (quant-ph); Cyptography and Security. Donna Dodson, Mikio Fujiwara, Philippe Grangier, Masahito Hayashi, Kentaro Imafuku, Ken-ichi Kitayama, Prem Kumar, Christian Kurtsiefer, Gaby Lenhart, Norbert Luetkenhaus, Tsutomu Matsumoto, William J. Munro, Tsuyoshi Nishioka, Momtchil Peev, Masahide Sasaki, Yutaka Sata, Atsushi Takada, Masahiro Takeoka, Kiyoshi Tamaki, Hidema Tanaka, Yasuhiro Tokura, Akihisa Tomita, Morio Toyoshima, Rodney van Meter, Atsuhiro Yamagishi, Yoshihisa Yamamoto, and Akihiro Yamamura, 2009.

NOTE: Available at http://arxiv.org/abs/0905.4325.

[i.7] IETF RFC 1661: "The Point-to-Point Protocol (PPP)".

[i.8] IETF RFC 1968: "The PPP Encryption Control Protocol (ECP)".

[i.9] IEEE 802.3u.

[i.10] "Handbook of Applied Cryptography", (Boca Raton: CRC Press) Menezes A J, van Oorschot P C and Vanstone S A 1997.

[i.11] "Applied Cryptography", Schneier B 1996, (New York: John Wiley).

[i.12] "Quantum Cryptography Progress in Optics 49", Dusek, M, Lütkenhaus N and Hendrych M 2006, Edt. E. Wolf , Elsevier 381-454.

[i.13] "Principled Assuredly Trustworthy Composable Architectures Computer Science Laboratory", Neumann P G 2003, SRI International, Menlo Park.

[i.14] "The Case for Quantum Key Distribution Preprint arXiv:0902.2839v1 [quant-ph]", Stebila D, Mosca M and Lütkenhaus N 2009.

[i.15] "A Method for Obtaining Digital Signatures and Public-Key Cryptosystems Communications of the ACM 21,2 120-6", Rivest R L, Shamir A and Adleman L M 1978.

[i.16] "Communication theory of secrecy systems Bell Systems technical Journal", 28 656-715 Shannon C E 1949.

[i.17] "New directions in cryptography IEEE Transactions on Information Theory", 22 644-54, Diffie W and Hellman M E, 1976.

[i.18] "How to Break MD5 and Other Hash Functions Proc. EUROCRYPT 2005, Lecture Notes in Computer Science" 3494 19-35, Wang X, Yu H, 2005.

[i.19] "Finding Collisions in the Full SHA-1 Lecture Notes in Computer Sciences", 3621 17-36, Wang X, Yin Y L and Yu H, 2005.

[i.20] "New Hash Functions and Their Use in Authenticaton and Set Equality Journal of Computer and System Sciences", 22 265-79, Wegman M N and Carter J L, 1981.

[i.21] "Why Quantum Cryptography?", Preprint arXiv:quant-ph/0406147, Paterson K G, Piper F, Schack R, 2005.

[i.22] "On fast and provably secure message authentication based on universal hashing Proc. Crypto "96, Lecture Notes in Computer Science", 1109 313-28, Shoup V, 1996.

[i.23] ETSI GS QKD 001: "Quantum Key Distribution (QKD); Development and Production of QKD systems; Security Assurance Requirements".".

NOTE: This reference is cited as WI 1 in the present document.

[i.24] ETSI GS QKD 003: "Quantum Key Distribution (QKD); Requirements for QKD systems; Components and Interfaces Requirements".".

NOTE: This reference is cited as WI 3 in the present document.

[i.25] ETSI GS QKD 004: "Quantum Key Distribution (QKD); Requirements for QKD systems; Application Interfaces Requirements Study".".

NOTE: This reference is cited as WI 4 in the present document.

[i.26] ETSI GS QKD 005: "Quantum Key Distribution (QKD); Security evaluation of QKD Systems; Generic Framework for Security Proofs".".

NOTE: This reference is cited as WI 5 in the present document.

[i.27] ETSI GS QKD 007.

NOTE: This reference is cited as WI 7 in the present document.

[i.28] ETSI GS QKD 008.

NOTE: This reference is cited as WI 8 in the present document.

[i.29] ETSI GS QKD 009.

NOTE: This reference is cited as WI 9in the present document.

3 Definitions and abbreviations

NOTE: The Definitions and Abbreviations clauses were completely removed from the document for reasons indicated in the 'Foreword to the Present 1st Edition' above.

4 QKD - A Security Technology Innovation

4.1 Classification of QKD as cryptographic primitive

Quantum key distribution can be seen as atomic cryptographic primitive and as such it covers only one part of the cryptographic functionality which is necessary to build a secure communication system([i.10] and [i.11**]**). The common notion 'quantum cryptography' for quantum key distribution is unfortunately misleading and it shall be clearly noted that QKD is not a replacement for 'classical cryptography' but a supplement for specific cryptographic requirements.

In the following the minimal set of cryptographic primitives for a secure communication system shall be evaluated with respect to the level of security that can be achieved. In order to secure the integrity and confidentiality of a message, as well as the authenticity of its origin, an encryption primitive and an authentication primitive must be combined with a key distribution primitive. As the overall security of a security system is at maximum as strong as its weakest link, or even weaker ([i.13]), encryption, authentication, and key distribution primitives with a comparable level of security shall be identified. (For a thorough discussion of cryptographic primitives and their relation to QKD see also [i.5] and [i.14]).

4.1.1 Encryption primitives

Encryption has been used from ancient times to protect the confidentiality of messages while they are transmitted. Today many kinds of information and communications technology (ICT) applications use a variety of encryption methods and algorithms for this goal. These include symmetric block and stream ciphers, where sender and receiver share two (identical or trivially related) keys, and asymmetric key algorithms, where two keys are related in such a way, that the private decryption key cannot easily be derived from the public encryption key. Examples for symmetric key algorithms are DES, the Data Encryption Standard, and its variant Triple DES, and the currently popular Advanced Encryption Standard AES. Examples for contemporary asymmetric key algorithms are the RSA algorithm ([i.15]) and the family of elliptic curve algorithms.

These symmetric and asymmetric algorithms have in common that the security for maintaining the confidentiality of the encrypted message is computational, i.e. it is based on the assumption that an attacker is constrained in available computing power for the attack or the available time for carrying it out. For asymmetric cryptography the security additionally depends on the assumption that no efficient algebraic method exists to reverse the utilized cryptographic functions. These assumptions require constant attention (see the web site for cryptographic key length recommendations www.keylength.com) and have in some cases required costly migration to another algorithm when their security was challenged e.g. because of the rapid increase computing power.

However, one symmetric cryptographic algorithm is different: the one time pad. If properly employed, it is the one and only information theoretically secure encryption method. Information theoretically secure refers to the fact that it can be formally proven that the amount of information an eavesdropper may have about the message is below an upper bound, which can be made arbitrarily small. The one time pad was invented in the early nineteen-twenties based on work of Gilbert Vernam and Joseph O. Mauborgne and it took almost thirty years until its 'perfect secrecy' could be proven by Claude Shannon in 1949 ([i.16]). For applications with highest security requirements the one time pad is still in use today, despite of its impractical prerequisites: It requires a truly random key with exactly the same length as the message to be encrypted.

4.1.2 Key distribution primitives

The generation of two identical streams of truly random bits at two distinct locations connected by a quantum channel is exactly what QKD can provide. As mentioned before, this can be achieved with information theoretically guaranteed security.

Other methods for distributing secret keys make either use of a given secure channel or rely on public key cryptography. Examples for a given secure channel are the trusted courier who carries a USB flash drive filled with a random bit sequence, or a digital channel that is secured with a previously distributed secret key. In the latter case the security level for the distribution process, and hence the security level of the subsequent encryption is certainly lower than the security level of the secure channel.

An example for a key distribution method using public key cryptography is the Diffie-Hellmann key agreement ([i.17]), which is e.g. used in the Secure Sockets Layer protocol (SSL/https) or in the Internet Key Exchange protocol (IKE) for setting up security associations in the IPSec protocol. In contrast to QKD, the security of both the secure channel and the public key agreement is again based on assumption. The advantage of public key distribution lies in its ability to establish a secret key between two parties without prior mutual knowledge. But it is also clear that without prior mutual knowledge the identities of the parties cannot be authenticated and a man-in-the-middle attack cannot be ruled out. The authentication of the communicating parties is usually solved with a public key infrastructure involving a trusted third party.

Quantum key distribution, too, requires authentication of the parties to rule out man-in-the-middle attacks. This is done by public discussion on the classical channel which uses a message authentication primitive to guarantee message integrity.

4.1.3 Message authentication primitives

For a secret communication system, message authentication, that means ensuring message integrity (i.e. that a message was not altered during transmission) and the identity of the sender are common goals. The QKD primitive itself requires message authentication for the messages its two peers exchange for the key distillation protocol.

Again, this goal can be accomplished using various technologies. A common approach is to apply digital signatures (**[**i.17**]**) by condensing a given message to a block of data with fixed size using a cryptographic hash function and subsequently signing it using a private key. The receiver can apply the corresponding public key and is thus able to verify not only the integrity of the message, but also the authenticity of its origin. Another method for message authentication is using conventional message authentication code (MAC) algorithms. MAC algorithms can be constructed using a block cipher or be derived from cryptographic hash functions. They use the same key for computing and verifying the MAC value and require prior distribution of symmetrical keys.

The security of both digital signatures and MAC algorithms depends on computational assumptions and there has always been progress in developing new cryptanalytic attacks leading to significantly reduced effort for brute force attacks, as this was the case for the widely used MD5 and RIPEMD in 2004 ([i.18]), or SHA-1 in 2005 **([**i.19**])**.

Provably secure authentication can be achieved with hash functions, which are selected from a class of universal-2 hash functions according to a secret both parties share. This system was initially proposed by Wegman and Carter in 1981([i.20]).

In QKD, a small fraction of the continuously generated key can be used for information theoretically secure message authentication, but when a link is taken into operation, a pre-distributed initial secret is necessary to authenticate the public channel before the first quantum keys become available. This is comparable to digital signature schemes, where the public key (mostly in the form of identity certificates) of the sender, or the public key of a trusted third party, when transitive trust relations are applied, must be pre-distributed (e.g. with the web browser). Insofar the necessity of a pre-distributed secret constitutes no principal disadvantage of information theoretically secure authentication schemes, as opposed to signature based or MAC based authentication systems, as this is claimed e.g. in [i.21].

4.1.4 Synopsis

Table 1 lists the encryption, key distribution, and message authentication primitives discussed above together with the principle on which their security is based on.

Table 1 Security foundation of cryptographic primitives

Encryption	**Security based on**
Symmetrical block or stream cipher (key shorter than message)	Assumption
Public key cryptography	Assumption
One time pad	Information theory
Key distribution	**Security based on**
Secure channel	Assumption
Public key cryptography	Assumption
Quantum key distribution	(Quantum) information theory
Message authentication	**Security based on**
Public key cryptography	Assumption
MAC	Assumption
Universal-2 hash functions	Information theory

It is evident that QKD is ideally being combined with one time pad encryption and universal-2 hashing to form a secret and authentic communication system with an unprecedented level of theoretical security. The mere combination of QKD with universal-2 hash hashing for a highly secure authentic and public communication systems is also imaginable.

The combination of the three listed information theoretically secure cryptographic building blocks in a network for highly secure communication was also one of the major achievements of the SECOQC project of the 6th Framework Programme of the European Community. The SECOQC network combines QKD with an efficient implementation of universal-2 hashing authentication ([i.22]) and alternatively one time pad or AES with frequent key change for payload encryption.

5 ISG-QKD Work Plan

The present document is part of a series of Group Specifications (GS) which are established according to the work plan of the ETSI ISG-QKD. The GS shall address indispensible, but hitherto missing prerequisites for actual deployment and qualified use of QKD systems. These prerequisites are related to the security certification of QKD systems, and their integration into existing infrastructures. Complementary work is carried out to assess user needs and expectations as well as political, legal, and societal basic parameters in order to identify potential promoters and inhibitors of widespread QKD deployment. Furthermore, future potential and challenges of QKD shall be assessed through expert and stakeholder consultations.

5.1 QKD Security Certification

Qualified practical use of QKD requires that QKD systems are trusted by its users, which is usually achieved in a complex accreditation procedure including security specification, evaluation, and certification according to a standardized methodology.

For the security certification of QKD system, there are requirements on both system hard- and software, as this is the case for other cryptography modules. In addition, QKD systems have an optical sub-system, introducing a new vector for attacks through theoretical weaknesses in the processing of quantum information, as well as through implementation dependent side channels. These issues are addressed in a series of Group Specification documents, their relationship being depicted in Figure 1 "QKD Evaluation Context". The black squares refer to GS that are produced by the ISG-QKD. The (WI x) indications denote that the respective document is an output of ISG-QKD Work Item x.

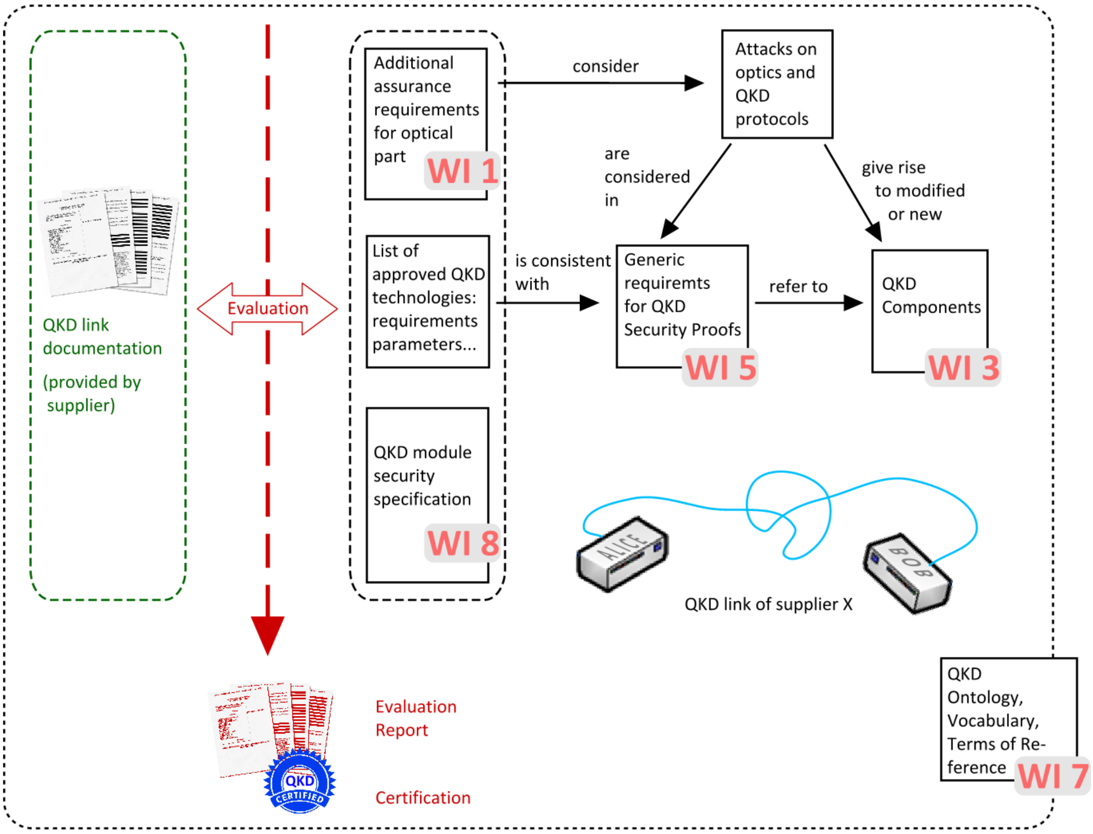
QKD link documentation
(provided by supplier)
Evaluation
Additional assurance requirements for optical part
WI 1
consider
Attacks on optics and QKD protocols
are considered in
give rise to modified or new
List of approved QKD technologies: requirements parameters...
is consistent with
Generic requiremts for QKD Security Proofs
WI 5
refer to
QKD Components
WI 3
QKD module security specification
WI 8
ALICE
BOB
QKD link of supplier X
QKD Ontology, Vocabulary, Terms of Re-ference
WI 7
QKD CERTIFIED
Evaluation Report
Certification

Figure 1: QKD Evaluation Context

In the following, the single GS are presented in more detail.

5.1.1 QKD; Ontology, Vocabulary, Terms of Reference

(Output of work item WI 7 [i.27]; Target date for initial publication: July 2010)

The document shall properly define all the vocabulary for describing the concepts, the metrics, the labels, and all the related items used by scientists, producers, and users in the QKD domain. It shall include a clarification to some definitions/concepts conveniently borrowed and adapted from the cryptographic world.

5.1.2 QKD; Assurance requirements

(Output of work item WI 1 [i.23]; Target date for initial publication: November 2010)

The document shall list typical security assurance requirements for the optical sub-system. Security assurance shall be given through groups of requirements based on QKD system developer practices and activities, as well as requirements on the security evaluation (e.g. on testing and vulnerability assessment), and the implementation of sound procedures for life cycle support and flaw/attack monitoring and remediation.

5.1.3 QKD; Module security specification

(Output of work item WI 8 [i.28]; Target date for initial publication: November 2010)

The document shall specify security requirements for QKD systems used within broader communications security systems protecting sensitive telecommunication information. Following the methodology used in conventional cryptographic security modules and systems, eleven security aspects have been identified, and the present document shall establish the minimum requirements that QKD systems will need to fulfill to be in accordance with the present document. The document shall not include security requirements for the optical sub-systems of a QKD system (which are included in 'List of approved QKD technologies' and in 'QKD; Assurance Requirements').

5.1.4 List of approved QKD technologies

The list of approved QKD technologies is currently targeted for an annex to the "QKD Module security specification" of work item WI 8 [i.28]. It will contain specific security requirements on the implementation and operation of the optical subsystem and the QKD key distillation protocols, including valid ranges for certain parameters of components which are listed in the "QKD: Components and Internal Interfaces" document.

Furthermore, specific security requirements for different quantum optical sub-systems shall be given in the form of Additional security requirements may specify how exactly and how often these parameters shall be measured in a running system to determine if they are in a secure regime.

5.1.5 QKD; Threats and Attacks

(Not associated to a work item; STF output; Target date for initial publication: November 2010)

Based on a comprehensive literature research, the document shall include a catalogue of known attacks on QKD systems - specifically side channel attacks on the optical sub-system. It also shall include information on measures and strategies for remediation which serve as basis for additional functional and assurance requirements for QKD systems. The document shall also define a procedure for keeping the catalogue up to date through a regular update and publication cycle.

5.1.6 QKD; Security Proofs

(Output of work item WI 5 [i.26]; Target date for initial publication: November 2010)

The document shall define generic requirements for quantum information theoretical security proofs for the quantum optical sub-system of different QKD technologies, from discrete variables, distributed reference pulses, and continuous variables domains.

This information shall serve as a reference for the construction of requirements and evaluation criteria for practical security evaluation of QKD Systems which are listed in the "List of Approved QKD Technologies".

5.1.7 QKD; Components and Internal Interfaces

(Output of work item WI 3 [i.24]; Target date for initial publication: November 2010)

Irrespective of the underlying technologies, there are certain components that appear in most QKD quantum optical sub-systems. These are on the one hand hybrid components with both classical and quantum optical sub-components, and on the other hand purely quantum optical components. Hybrid components include photon sources and photon detectors, while pure optical components include highly integrated structures, like waveguide assemblies, as well as much simpler passive discrete optical components, like lenses, steering mirrors, wave blades, polarizers and filters. For these components, relevant properties and parameters shall be defined. The actual valid, secure operational ranges of parameters for QKD systems shall be defined in the "QKD; Security Proofs" document.

Furthermore, a catalogue of relevant requirements for interfaces between components shall be established, supporting the definition of internal interfaces.

5.2 QKD Integration into Existing Infrastructures

The following documents include specifications for interfacing QKD to applications and for integrating QKD into shared fiber infrastructures.

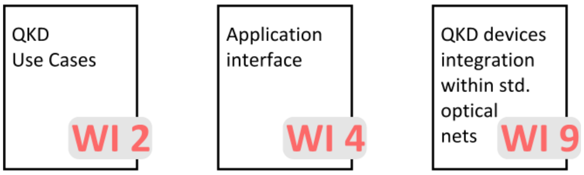

Figure 2: QKD Integration and Interfacing

5.2.1 QKD; Use Cases

(The present document, Output of work item WI 2)

The present document describes some basic point-to-point use cases for QKD and the technical characteristics derived from these use cases. The technical characteristics allow the identification of both functional and security requirements for the implementation of QKD, intended for qualified use in existing and future ICT networks.

5.2.2 QKD; Application Interface

(Output of work item WI 4 [i.25]; Target date for initial publication: November 2010)

The document shall define the interface which connects a QKD system to an ICT system. It shall specifically address the mechanisms for the delivery and management of keys, as well as for the management of the QKD system from applications in the ICT system.

5.2.3 QKD devices integration within standard optical networks

(Output of work item WI 9 [i.29]; Target date for initial publication: November 2010)

The document shall define prerequisites and requirements for the integration of QKD systems into common shared optical infrastructures. It shall establish functionalities and limits to maximize the amount of hardware and software shared by quantum signals and conventional signals, in particular mechanisms for system management and optical power limits.

5.3 Complementary Research

The following documents shall complement the specifications listed above.

Figure 3: Complementary Research

5.3.1 Promoters and Inhibitors for QKD

(Output of specialist task force STF 367 with no associated work item; Target date for initial publication: July 2010)

The document shall give an overview on promoters and inhibitors of QKD in general as reflected by recent studies and experts in the field. The paper shall be introduced to the ISG-QKD for critical discussion. It shall provide a valuable input for briefing the participants of a QKD scenario workshop which is scheduled to take place with the QKD#7 meeting in June 2010 in Vienna.

5.3.2 Prospects of QKD in Europe

(Output of specialist task force STF 367 with no associated work item; Target date for initial publication: July 2010)

The document shall assess fields of applications, user needs and expectations as well as potential risks against the successful introduction of QKD systems into the market. This shall include the identification of present and future promoters and inhibitors of QKD diffusion, applications, requirements and the framework constituting the notion of trust in this technology. by the development of systemic scenarios from consultations of researchers, industry, policy makers, prospective users, and other representatives from society.

6 Application scenarios for QKD

Quantum Key Distribution, with its unique long term security perspective (perfect forward security - the inability of an intruder who has recorded past traffic between a sender and receiver to decrypt that traffic if any future or past keying material is compromised), is an important cryptographic primitive for building dependable high security ICT systems. Other cryptographic functions that may use quantum keys (e.g. message encryption, integrity protection and authentication) have to be supplied by additional components.

In an ICT system, there is no obvious or preferred point, or layer, where an interface to a QKD system can most suitably be placed. With this respect, QKD is not different from other available key distribution primitives, which are attached to communication systems at various layers. We present here different possibilities for the integration of QKD to ICT systems following the common Open Systems Interconnection Reference Model, the seven-layer OSI model [i.6].

The layer of QKD integration into ICT systems is not specifically relevant to the single use cases presented in clause 6 of the present document - for most of the use cases, the integration of QKD is possible at various levels.

6.1 Data Link Layer

On the Data Link Layer, QKD may be used as a part of the **Point to Point Protocol** (PPP) protocol. The PPP **(RFC 1661 [**i.7**])** is a layer 2 protocol widely used to connect two sets of nodes in a network. The encryption functionality in PPP is the **Encryption Control Protocol (ECP - RFC 1968 [**i.8**])** which allows the use of encryption in PPP frames. QKD may be used as a key exchange protocol for PPP.

QKD may also be used to provide keys for **the IEEE 802.1 MACsec** layer 2 protocol. MACsec provides a connectionless service that supports data confidentiality, integrity, and authenticity for authorized systems attaching to a local area network (LAN) or interconnecting LANs.

As QKD is today mainly implemented as point to point link involving two endpoints connected by a quantum channel, it is reasonable to combine a QKD link with a link encryptor to form a **QKD Link Encryptor**. A link encryptor is a network-transparent cryptographic system. A QKD link encryptor is a Quantum Cryptography appliance for point-to-point link encryption which may also be referred to as Virtual Private Network VPN tunnel. The link encryptor usually uses the keys supplied by QKD as keys for a symmetrical block cipher (for example the Advanced Encryption Standard AES) or steam cipher (One Time Pad for highest security) and can be used for example to encrypt traffic on an Ethernet of Fiber Channel link. The QKD Link encryptor may be used to support communications between two adjacent network nodes employing QKD or it may provide protection for communications end-to-end across a network of nodes as a VPN tunnel. Key management is integrated in the link encryptor. For example, this solution may securely bridge two Fast Ethernet (IEEE 802.3u [i.9]) networks.

6.2 Network Layer

Internet Protocol Security (IPsec) is a layer 3 protocol suite for securing Internet Protocol (IP) communications by authenticating and encrypting the IP packets of a data stream.

Internet Key Exchange (IKE or IKEv2) is the protocol used to set up a security association in the IPsec protocol suite. IKE uses a Diffie-Hellman public key exchange to set up a shared session secret, from which cryptographic keys are derived. Public key techniques or, alternatively, a pre-shared key, are used to mutually authenticate the communicating parties.

QKD may be used by a modified IKE protocol to provide the shared secret for IPsec payload encryption. The shared secret provided by QKD may either be used in a conventional block or stream cipher for One-Time-Pad payload encryption in a high security context.

6.3 Transport Layer

Transport Layer Security (TLS) and its predecessor **Secure Sockets Layer (SSL)** are layer 4 protocols, which provide end-to-end security for network communication services. A session key, usually established with public key exchange, is used e.g. to secure the transmission of credit card information in e-commerce transactions. In a scenario involving QKD, the session key may be replaced by a QKD key, or the QKD keys may immediately be used for One-Time-Pad encryption of transmission data. QKD keys may also be used for message authentication, replacing Hash-based Message Authentication Codes (HMACs) as used in TLS, or the pseudo-random functions of standard SSL.

6.4 Application Layer

Above the transport layer, QKD systems may be integrated in layer 7, the Application Layer of the OSI model. This may be useful for applications using pre-shared keys for user authentication or for the acquisition or certain rights, or as encryption keys for payload transmission between instances of the application.

7 Use Cases

7.1 Use Case 1: Offsite Backup / Business Continuity

7.1.1 Goal

The protection of backup and other business continuity processes and transactions

7.1.2 Description

An enterprise owns a private network or leases access to a fiber from an infrastructure provider. It has centralized the main data processing at a site which we will name "Primary site". To assure business continuity it has decided to add a new centre ("Backup site") and regularly perform a remote backup of the primary site. In case of data loss at the primary site data is recovered from the secondary site. For protection against major disaster, the secondary site can be equipped and configured to fully take over control and operation.

As strict confidentiality of data is required, an encryption system is mandatory. In this case a QKD link encryptor may be used: The cryptographic keys shall be established and exchanged between primary and secondary site with a QKD link and fed into a link encryptor which uses a symmetrical block or steam cipher to encrypt traffic on an Ethernet of Fiber Channel link. The key in the link encryptor may be renewed as frequently as the key generation rate of the QKD system allows, depending on the security requirements of the enterprise.

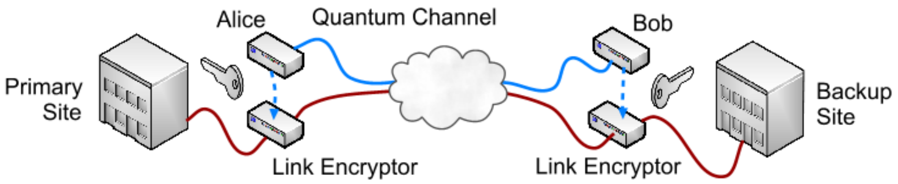

Figure 4: QKD link encryptor

Current offsite backup installations do in most cases not use any encryption at all, as encryption requires more processing time at the operational and backup servers and more bandwidth on the communication line between the primary and backup site.

7.1.3 Concept of Operation

The data transferred between primary and backup site may be different depending on the amount of data transferred, the bandwidth available and the security requirements. We may distinguish the following situations:

- **Daily Backup:** In this case the backup is performed once a day, usually at night, or at any other time outside of office hours. Data is transferred at certain fixed hours and the process is triggered automatically, managed by a backup tool. The backup manager is located at the primary site. A software agent is located in every server of the primary site. All data is managed through the primary site backup manager and sent to a remote backup server which is located at the backup site. Both backup servers have secondary storage devices attached to them.

  In the case of a restore, the information may be recovered from the point when the backup was made. All data generated between the time of the backup and the time of the crash may, in the worst case, be lost. It shall be considered that the backup process is an intense network bandwidth consumer, both in the primary site and in the inter-site link.

  The nature of the data being transferred may be standard static files or database information. In case of database information a special procedure shall be triggered before backup and after recovery to assure the consistency of data in the database. Usually the procedure is to put the database in backup mode, so that data is not written directly to the database but in redo log files. The database raw files are then copied and when the backup is completed the pending redo log files are applied to the database.

  The communication is asynchronous.

- **Storage snapshots:** Another option for implementing an offsite backup is to make periodical snapshots of the primary storage of certain critical servers at certain points of time. If the data being copied are also database files, the same procedure as for database backup shall be carried out to assure database consistency. In case of a crash, the complete storage snapshot is recovered from the backup site.

- **Storage Area Network (SAN) mirroring:** In case that a daily backup becomes insufficient we may opt for a fully functional mirroring solution. This case shall be treated with more detail in Use Case 2, as it is not a proper backup scenario (batch processing) but rather an interactive scenario requiring continuous availability of the secure link.

- **Database replication:** Another option is to have the complete database software replicated at both sites and to replicate operations in both sites too. The database at the backup site may be used just for auxiliary readings (only reading operations and no writings) or to gain control in case of a disaster at the primary site. This replication may be asynchronous or synchronous and consistency of data shall be assured as described in the 'Daily Backup' operation.

7.1.4 Actors

The actors in this use case are: The **enterprise**, which has two sites. A **primary site** holds the main data center and a **backup site** holds the data backup for business continuity. The **enterprise** owns the connecting fiber infrastructure, or leases it from an **infrastructure provider**.

7.1.5 Actor Specific Issues

The **enterprise** owns the QKD link encryptor. The Alice and Bob devices are under effective control of the **enterprise** The Alice and Bob devices are located inside the security perimeter of the **enterprise.**

The **enterprise** wants to create, share and mange their keys autonomously.

The security requirements may vary depending on the type of business the **enterprise** is engaged in.

The **enterprise** shall consider that the overall security level of the QKD Link Encryptor is determined by both the QKD component, and the link encryptor component. This specifically means that the resulting QKD link encryptor is not information theoretically secure:

- The **enterprise** wants a fast connection as backup is very bandwidth consuming.

- The **enterprise** may be required by legal regulation to adequately protect its data transfer.

7.1.6 Actor Specific Benefits

- The **enterprise** may rely on a secure data transfer.
- The **enterprise** may rely on completely transparent encryption. There is no need for key management at application level.
- The encryption does not consume processing time at the servers of the **enterprise**.

7.1.7 Operational and Quality of Service Considerations

The achievable key refresh rate of the link encryptor depends on the secret key rate of the QKD link, which again depends on the typical key generation rate of the QKD technology used as well as on the overall attenuation and other properties of the quantum channel.

If the top level application requires continuous data transfer, the QKD link encryptor requires a mechanism for providing recalibration sequences.

The (symmetrical) key of the link encryptor may be renewed as frequently as possible, depending on the bandwidth available and the user security policy.

The optical fiber of the quantum channel may be physically protected by an arming mantle or just be dug into the ground without any additional security protection.

The length and duration of data transactions may vary from very short data packets to continuous streams of data.

7.1.8 Functional Characteristics

The QKD link may be a dedicated links (dark fiber) or a shared links (WDM - Wavelength division multiplexed, or TDM - Time division multiplexed).

The QKD link encryptor shall operate completely independent from the business servers.

The QKD link shall be properly initialized (equipped with an initial secret) which is usually done at equipment setup.

When the data transaction is completed, the link between the two sites shall be terminated.

7.2 Use Case 2: Enterprise Metropolitan Area Network

7.2.1 Goal

Protection of infrastructures and services in Enterprise MAN networks.

7.2.2 Description

An enterprise or a government agency owns a private network or leases access to a fiber from an infrastructure provider, which connects one or more data centers with their branch offices. The enterprise uses the network for central applications serving the branch offices. These applications may be communication applications (email, telephony, video...) or database and application servers in the data centers with respective clients in the branch offices. As there are no direct connections between branch offices, communication between branch offices is routed through the data centers.

The enterprise or government agency requires a high level of confidentiality, integrity, and authenticity of the communication system and therefore a dedicated security system is mandatory. The single network connections between the sites shall be secured with QKD Link Encryptors (see Figure 2). The cryptographic keys which are continuously generated by the QKD links are fed into link encryptors using a symmetrical block or steam cipher for transparent traffic encryption on an Ethernet or Fiber Channel link.

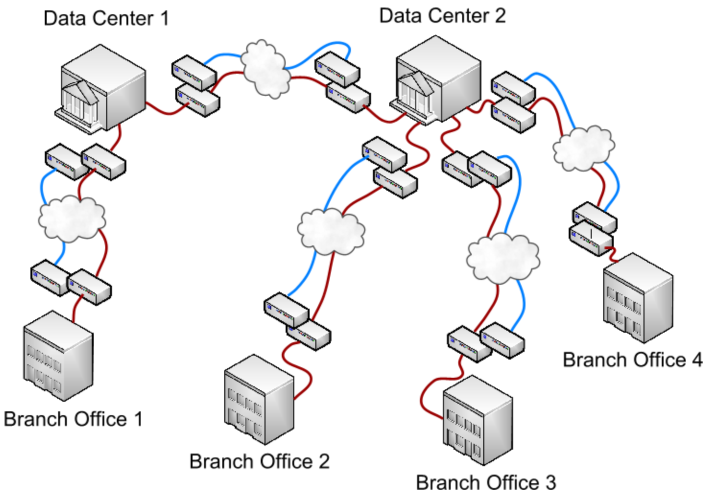

Figure 5: Enterprise MAN using QKD link encryptors

Current solutions employ secure Virtual Private Networks based on IPsec (network layer) or TLS (transport layer) to authenticate and encrypt the traffic between data centers and branch offices.

7.2.3 Concept of Operation

The entire traffic between the sites is encrypted and authenticated on the OSI data link layer. This provides security for all the higher layer protocols of the TCP/IP suite and all common communication applications in the higher layers. Applications use the secure links transparently.

7.2.4 Actors

An **enterprise** or a **government agency** has one or more **data centers** and some **branch offices** which are connected to the data center. The **enterprise** either owns the QKD link encryptors and the connecting fiber infrastructure or leases them from an **infrastructure provider**.

7.2.5 Actor Specific Issues

NOTE: The enterprise or government agency has to consider the applicability of 'Actor Specific Issues' of the QKD link encryptor of Use Case 1.

7.2.6 Actor Specific Benefits

It is not necessary to modify an application when migrating to the QKD enabled secure network.

On the other hand, the secure enterprise MAN allows the development of new innovative applications (High security, possibly One-Time-Pad protected communication systems).

7.2.7 Operational and Quality of Service Considerations

NOTE: The enterprise or government agency has to consider the applicability of 'Operational and Quality of Service Considerations' of the QKD link encryptor of Use Case 1.

The amount of data and the timing profile of the data transmission between a **data center** and a **branch office** may be different from the data transfer between two **data centers**.

Depending on different types of transmissions, the operational and quality of service requirements on the QKD link encryptors between **data centers** and **branch offices** may be different from the requirements on QKD link encryptors between two **data centers**.

The data transfers may be initiated manually by an employee or automatically by a predefined schedule.

The length and duration of data transactions between **data centers** and **branch offices** may vary from very short data packets to a continuous stream of data. Data transactions may be carried out periodically (e.g. at a certain time of day), or after a specific period of time, or once the amount of new data exceeds a certain, predefined threshold.

The two **data centers** may implement one of the high availability scenarios of Use Case 1.

7.2.8 Use Case Variant: QKD Secured Key Server

An enterprise or a government agency operates a central key management server to supply cryptographic objects (keys, certificates) to encryption system clients in several locations within a metropolitan area. The client requests, as well as the server replies and deliveries are sent over communication channels secured by QKD-Link-Encryptors which employ information theoretically secure One-Time-Pad encryption and Wegman-Carter authentication in order to achieve the highest possible security level.

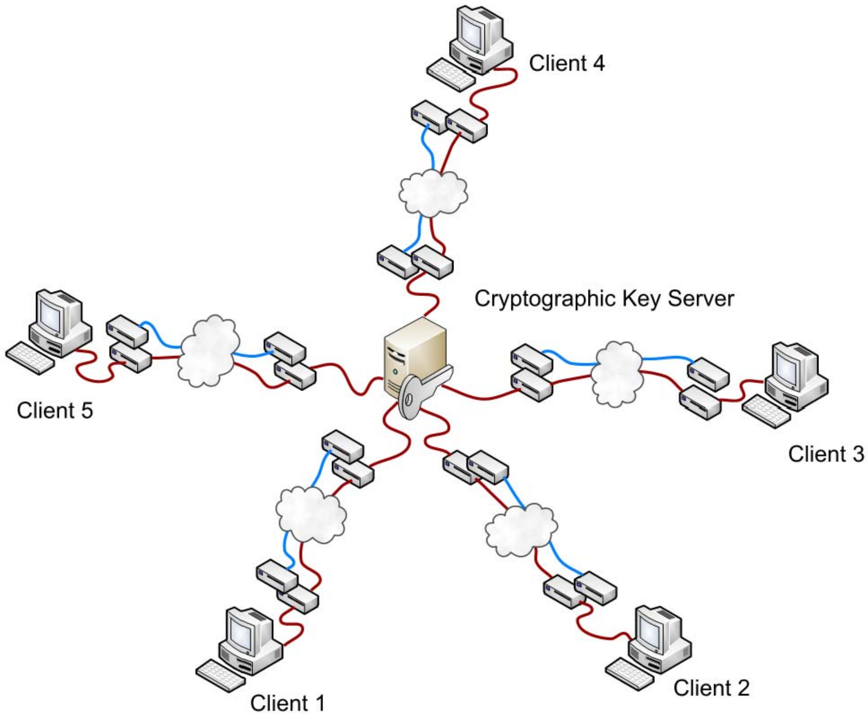

Figure 6: Central Key Server with QKD Distribution Channels

Current key client/server solutions rely on TLS/SSL, i.e. asymmetrical cryptography for securing the key distribution channel.

7.2.9 Functional Characteristics

NOTE: The enterprise or government agency has to consider the applicability of 'Functional Characteristics' of the QKD link encryptor of use case 1.

7.3 Use Case 3: Critical Infrastructure Control and Data Acquisition

7.3.1 Goal

Protection of communication in a critical infrastructure supervisory control and data acquisition (SCADA) system.

7.3.2 Description

In industrial countries the functioning of society and the economy depends on the continuous and intact availability of certain infrastructures, so-called critical infrastructures. Examples of critical infrastructures are communication services, services for water supply, services for production and distribution of electric energy, gas and oil and their derivates, financial services, health services, transportation systems, food production and distribution systems, and national security services. The internet can also be considered as critical infrastructure, as essential communication services are increasingly being provided over the internet (e.g. IP telephony). Other critical infrastructures use supervisory control and data acquisition systems which critically depend on virtual private overlay networks built on top of the internet.

SCADA systems rely heavily on communication infrastructure subsystems. Besides availability, most of these communication subsystems have to provide communication confidentiality, while it may be the case that communication authenticity and integrity are more important than confidentiality. This may be the case e.g. for a railway control system or for a water distribution control system where it may be of greater importance that the control commands for rail switches, or for water valves are authentic (i.e. that the messages originate from the legitimate control center) and integrity protected (arrive unaltered at the legitimate receiver), than that the actuator commands remain confidential.

The following description shall point out how a railway network may be protected with quantum key distribution: The routing schedule and train control of a railway network are done in a railway control center. The center reads and processes input from sensors which are placed along the rail network on section boundaries, crossings, in stations etc. In the other direction, the centre issues commands to signals, switches, crossing gates, displays etc. The communication is carried out via lines that run along the rail network, together with other communication lines and power lines. It is of greatest importance to secure the authenticity of the messages; but for the prevention of specific malicious attacks it may also be required to relay certain messages encrypted and integrity protected. These properties shall be ensured using cryptographic keys distributed with QKD.

7.3.3 Concept of Operation

The overall network structure is that of a private wide area network (WAN). The key distribution shall either be carried out on the link layer, Figure 4, or by using a dedicated trusted repeater type QKD network, Figure 5. Because of the distance limitations of quantum links, both approaches require that the links between the single WAN network nodes shall not exceed the typical length which can be spanned by a QKD link. In the railway system these WAN network nodes may typically be set up at railway stations where a secure perimeter can be installed and controlled by trustworthy personnel.

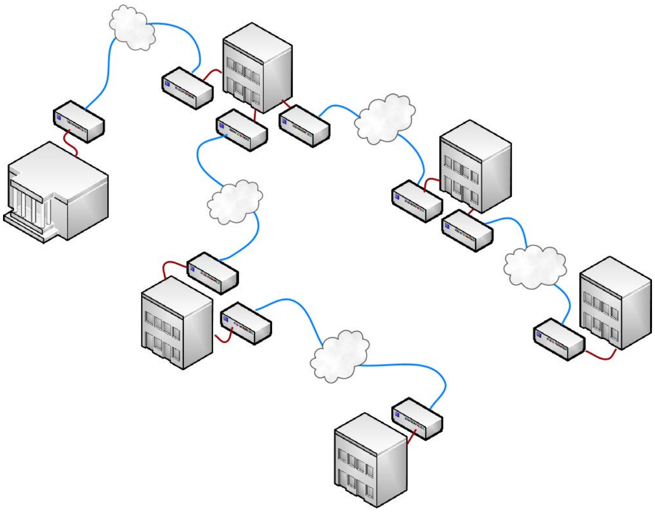

Figure 7: WAN using single QKD links

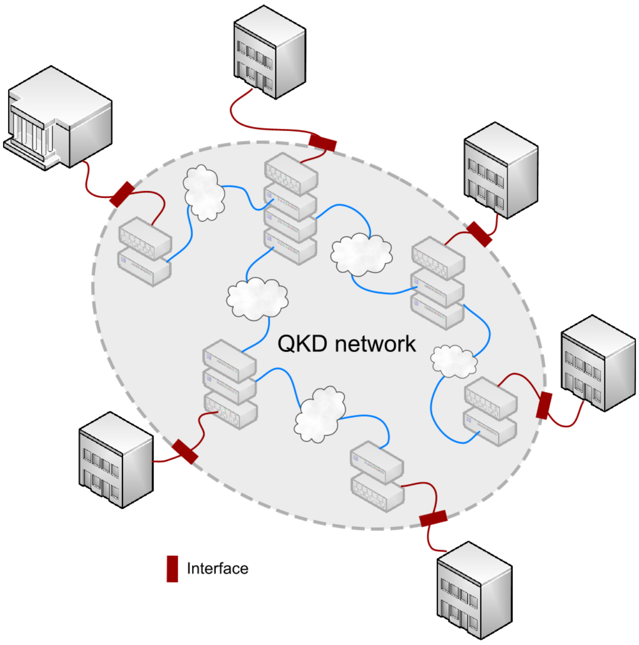

Figure 8: WAN using a QKD network

The two approaches of Figures 7 and 8, differ in the way cryptographic keys are managed. In a WAN set up from single QKD links, the management of cryptographic keys (buffering, key forwarding for key exchange between nodes which are not directly connected) has to explicitly be taken care of in the network nodes, while a QKD network usually provides integrated key management and is accessed over a dedicated interface.

7.3.4 Actors

The **critical infrastructure operator** is responsible for the uninterrupted and undisturbed availability of the critical infrastructure. The **infrastructure operator** owns the network nodes, and the QKD links or the QKD network. The **infrastructure operator** owns the connecting fiber infrastructure, or leases it from a **carrier**.

7.3.5 Actor Specific Issues

The **critical infrastructure operator** owns the QKD link encryptors.

The Alice and Bob devices are located inside the security perimeter of the **critical infrastructure operator**. They are under effective control by the **critical infrastructure operator**.

The fiber between the Alice and Bob devices is located outside of the security perimeter of the **critical infrastructure operator**. It is not under the effective control of the **critical infrastructure operator**.

The **critical infrastructure operator** wants to create, share and mange the cryptographic keys autonomously.

The **critical infrastructure operator** requires the highest level of security for cryptographic key distribution, encryption, and authentication.

The **critical infrastructure operator** requires the highest availability of the critical infrastructure.

7.3.6 Actor Specific Benefits

- The **critical infrastructure operator** may rely on dependably secure data transfer.
- The **critical infrastructure operator** may rely on a long term security perspective and may avoid difficult and expensive upgrade process.

7.3.7 Operational and Quality of Service Considerations

- The required high availability of the critical infrastructure requires special precautions to provide recalibration phases of the employed QKD links.

- The mandatory high availability of the critical infrastructure requires special precautions to cope with outage of single QKD links due to malfunction, denial of service attack or any other reason.

The length and duration of data transactions may vary from very short data packets to continuous streams of data.

7.3.8 Functional Characteristics

The QKD links may be dedicated links (dark fiber) or shared links (WDM - Wavelength division multiplexed, or TDM - Time division multiplexed).

The initialization of newly integrated, redundant QKD links into the critical infrastructure shall be done with manually distributed pre-shared secrets, or by distributed secrets established over a redundant path.

7.4 Use Case 4: Backbone Protection

7.4.1 Goal

Use QKD for security services between the nodes of a backbone network.

7.4.2 Description

The basic idea behind the present use case is that any QKD compatible fiber link in a network provider infrastructure interconnecting several access networks has the intrinsic potential resource of a quantum channel. This quantum channel can be used to exchange quantum information - or remain idle and unused.

Current networks are evolving towards optical, passive infrastructures both for access networks and also for metropolitan area network backbones. Metro networks are logically divided into backbone and access parts. The backbone is specialized in high speed communications. This is a point to multipoint network, with one end connected to the backbone at the carrier company premises, while the other gives service to several clients. A shared link goes from the backbone to some form of splitter that is located in the vicinity of the clients.

Metropolitan area networks consist usually of a fiber ring and optical add-drop multiplexers (OADM) or more recently, reconfigurable OADMs (ROADM). An OADM is a device used in wavelength-division multiplexing systems for multiplexing and routing different channels of light into or out of a single mode fiber (SMF).

A reconfigurable optical add-drop multiplexer (ROADM) is a form of optical add-drop multiplexer that adds the ability to remotely switch traffic from a WDM system at the wavelength layer. This allows individual or multiple wavelengths carrying data channels to be added and/or dropped from a transport fiber without the need to convert the signals on all of the WDM channels to electronic signals and back again to optical signals.

In a backbone link which uses WDM technology for multiplexing multiple channels on one single optical fiber, one specific channel (fixed or agreed between both ends) is used as quantum channel of a QKD system. The QKD system produces a continuous stream of symmetrical secrets on both ends of the backbone link, which are subsequently used for security services on the other channels of the optical link.

The generated keys can be used for specific cryptographic tasks on the level of the infrastructure provider, like validating the authenticity of transmissions, or encrypting specific communication protocol messages with high security. Another usage of the continuously generated keys is to use them with defined encryption algorithms for selective message encryption/integrity protection/authentication services provided to customers by a service provider.

7.4.3 Concept of Operation

This use case requires an uninterrupted optical path between the two ends of a backbone link, compatible with distance limitations and other characteristics of the employed QKD technology. It requires wavelength division multiplexing (WDM) systems which are capable of multiplexing and demultiplexing quantum signals to and from an appropriate channel of the attached optical fiber.

Moreover, compatibility with other equipment like reconfigurable optical add-drop multiplexers (ROADMs), optical switches, optical amplifiers, or other integrated optical circuits (IOCs) is required.

7.4.4 Actors

An **infrastructure provider** operates a backbone network interconnecting several subnetworks. The backbone links are implemented in wavelength division multiplexing (WDM) technology providing multiple digital channels, as well as a quantum channel. The QKD generated keys are used by the **infrastructure provider** to secure confidentiality, integrity, and authenticity of all or selected data transmitted on digital channels of the backbone links, or to provide secrets to a **service provider** operating on the provided infrastructure for specific commercial services the **service provider** offers to its **customers**.

7.4.5 Actor Specific Issues

The **infrastructure provider** owns the backbone network.

The **infrastructure provider** wants to effectively control the authenticity and integrity of the network control and management subsystems.

The **infrastructure provider** wants to provide reliable and secure infrastructure to the **service provider**, and vice versa the **service provider** wants to rely on a reliable and secure infrastructure.

The backbone nodes are under effective control of the **infrastructure provider** (trusted nodes).

7.4.6 Actor Specific Benefits

The **infrastructure provider** can protect the network control and management plane (routing, signaling, link management) of his backbone network.

The infrastructure provider can provide an additional service to the service provider.

The **service provider** can provide additional services to its **customers.**

7.4.7 Operational and Quality of Service Considerations

System administration and management shall be integrated in WDM system management.

The QKD system shall be compatible with common fiber infrastructure (e.g. fibers, splices, connectors).

The QKD system shall not decrease the overall throughput of the WDM system by more than 10 %.

The QKD system shall be installed and maintained by common WDM system operators without specific knowledge of in quantum physics.

7.4.8 Functional Characteristics

Not available in the present document - see 'Foreword to the Present 1st Edition'.

7.5 Use Case 5: High Security Access Network

7.5.1 Goal

Provide communication security in a passive optical network.

7.5.2 Description

A QKD system is used to distribute cryptographic keys to end users attached to a Passive Optical Network (PON), as they are common in Fiber to the Home access network architectures.

A Passive Optical Network (PON) connects one Optical Line Terminal (OLT) with multiple Optical Network Units (ONUs). The OLT is usually installed at a facility of a service provider while the ONUs are installed near the end users. One OLT today serves between 32 and 128 ONUs, and information is broadcast downstream from the OLT to all ONUs, while the upstream is realized in a wavelength division multiplexing scheme.

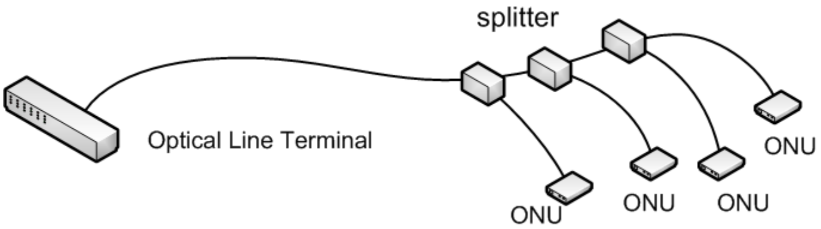

Figure 9: Passive optical network (PON)

A PON uses only passive components and each ONU sees the entire downstream from the OLT. Therefore encryption has to be used to prevent eavesdropping of ONUs for content which is not intended for them. Current solutions employ shared symmetrical keys for downstream encryption/decryption which may be distributed with smart cards, or with asymmetrical methods (Diffie-Hellman) in combination with an authentication scheme (identity certificates and PKI).

7.5.3 Concept of Operation

The same path which is used to relay the classical information from the OLT to the end user ONU can be used to exchange quantum information encoded in single photons or weak pulses. But contrary to the classical information, where each bit is encoded in a light pulse consisting of thousands of photons, so that each ONU can receive a comparable share of an original pulse issued by the OLT, a single photon can only arrive at one ONU. The probability of a photon arriving at a certain ONU is proportional to the share of the classical signal arriving at that ONU. The QKD photons are measured at the ONU and through a system of synchronized clocks the ONU and the OLT can identify corresponding measurements when distilling a mutual secret key.

The QKD system involved in this use case consists of a highly asymmetrical setup, where one central unit serves many leaves of a tree-like structure. In principle, the direction of operation is not fixed in this use case. A single source can be at the OLT and the detection can be done at each of the ONUs or the other way round. Yet, the current situation in which detectors are by far more expensive than sources, suggests a solution where one detector at the OLT serves a herd of sources at the individual ONUs.

7.5.4 Actors

A **service provider** is operating the Optical Line Terminal, and is also usually the owner of the fiber infrastructure. The **content provider** is providing the stream content. Examples for **content providers** are: ICT service providers or cable network operators. The parties connected to the many Optical Network Units of the PON are the **end users**. The **end users** may be **content providers** themselves.

7.5.5 Actor Specific Issues

The **service provider** wants to provide communication connections with reliable security and availability expectations.

The **content provider** shall trust the **service provider** as regards the security of the downstream content (e.g. confidentiality and non-repudiation by media consumer).

In the case of the **end user** being the **content provider**, s/he shall have reason to trust the security provided by the **service provider** for downstream, as well as for upstream content.

7.5.6 Actor Specific Benefits

The **service provider** may offer a service with a long term security perspective.

The **content provider** may build upon a service with a long term security perspective:

- Continuous secrets generation in the QKD enabled PON mitigates the key revocation problem.

7.5.7 Operational and Quality of Service Considerations

The relatively short distances in PON structures allow QKD with high key rates. This is of importance, as the entire key generation capacity is shared by all end nodes in the PON. As PONs are usually designed for high bandwidth IP based services (video, telephony, www) it is likely that the distributed secrets are used in symmetrical block- or stream ciphers, although specific use of secrets for provably secure One-Time-Pad encryption of selected sensitive data is also conceivable.

This high security access network is a potential entry level application for QKD with relaxed requirements on QKD link lengths resulting in higher QKD key rates.

7.5.8 Use Case Variant: QKD Authenticated Sensor Network

A variant of the use case makes use of an equivalent infrastructure for the authentication of sensor and actuator devices and their data in a local sensor network (e.g. at an airport or in a power plant). The sensor network has one central control station, which operates one side of a common QKD link (either the source side, or the detector side) while the many sensors and actuators have many instances of the other side of a common QKD link (many Alice devices or Bob devices, usually the less expensive side, i.e. today the source). The central QKD device generates shared keys with any of the peripheral QKD devices (TDM scheme, run length identification scheme, frequency multiplexing scheme).

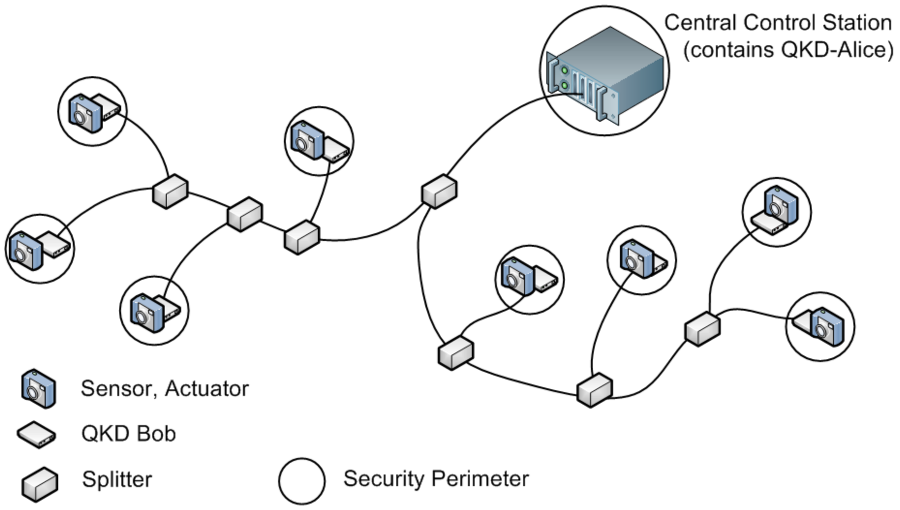

Figure 10: QKD authenticated sensor network

7.5.9 Functional Characteristics

Not available in the present document - see 'Foreword to the Present 1st Edition'.

7.6 Use Case 6: Long-Haul Service

7.6.1 Goal

Facilitate highly secure key distribution between far remote sites without trust assumptions on intermediary nodes.

7.6.2 Description

Ground stations A and B are the two nodes in a network separated by a very long distance (long-haul) such as a submarine communications cable on two shores of an ocean. A satellite passes over A and B once daily and enables them to share a common secret. The secret is used in a symmetrical encryption scheme to secure the data transmission across the long-haul communications path.

Contrary to the cases where communicating parties are either directly connected by QKD links, or are relying on an intermediary network infrastructure for quantum key distribution, we consider here the case of a long-haul connection between remote sites which are served, one after the other, via a free space QKD link by an aircraft or by a low orbiting space satellite (at about 300 to 800 kilometers altitude).

Different types of suitable aircraft include planes and possibly also High Altitude Platforms (HAPs), which are basically stationary aircraft or aircraft with limited cruising radius operating at heights of about 20 km. The HAPs can supply a metropolitan area region with secrets from above, covering a potentially larger area than what can be achieved in direct line of sight, especially in a metropolitan area.

A variant of this use case involves several satellites, interconnected via free 'space' links, which are able to exchange keys over long distances at very high key distribution rates due to the significantly lower attenuation of space compared to the terrestrial atmosphere. This variant again involves low orbiting satellites. Geosynchronous or geostationary satellites are not a viable option as their altitude of orbit of between 36 000 km (circular orbit) and 42 000 km (inclined orbit) requires optical telescopes with infeasible apertures of about 10 meters.

7.6.3 Concept of Operation

Two ground stations A and B have free space QKD systems with movable directional telescopes capable of pointing and tracking a moving target C in the sky.

First, C passes over ground station A and establishes a mutual symmetrical secret *a* with A. The QKD system in C is considered trustworthy and secure because it is located in a high flying craft.

Later, C passes over ground station B and establishes another symmetrical secret *b* with B. It then uses it to One-Time-Pad-encrypt the secret it previously exchanged with A and passes the cryptogram (*a* xor *b*) trough a conventional classical communication channel to B who can recover the secret *a* which A already has.

The ground stations A and B now share a common secret that can be used for any cryptographic task.

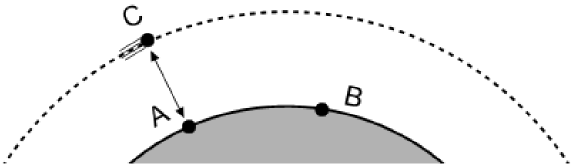

Figure 11: C and A exchange a secret *a*

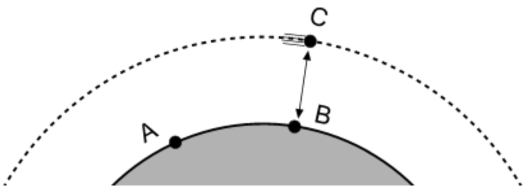

Figure 12: C and B exchange a secret *b*

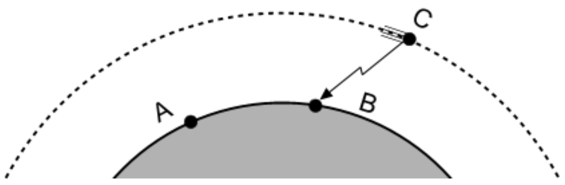

Figure 13: C sends encrypted secret (*a* xor *b*) to B using a classical channel

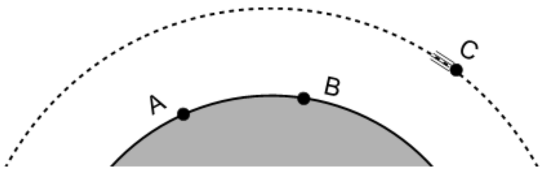

Figure 14: A and B share a common secret *a*

7.6.4 Actors

Actors are the two **ground stations** A and B, and the **moving target** C, which passes over A and B, one after the other. The moving target can either belong to a **service provider** (operator, carrier), or to the **owner of the ground stations** that are provided with secrets.

7.6.5 Actor Specific Issues

The **ground stations** can theoretically be on any two points on the surface of the earth, as long as these points are covered by the **moving target**.

The **owner of the ground stations** has very high security requirements (e.g. governmental sector, critical infrastructure provider, military).

The **ground stations** can be owned by one **owner**, or by different ones.

7.6.6 Actor Specific Benefits

Allows key distribution with highest security level spanning arbitrary distance between **ground stations.**

The **service provider** can offer a unique service giving the **service provider** a competitive edge:

- The **ground stations** can be moving on the ground or be stationary.

7.6.7 Operational and Quality of Service Considerations

Free space QKD is susceptible to attenuation by atmospheric conditions, caused by weather and pollution for example.

The refractive index of air varies between layers of different temperature and humidity. These phenomena can make QKD entirely impossible at adverse conditions, or significantly reduce the achievable key generation rate.

The availability of a long-haul service can only be guaranteed in combination with additional redundant key distribution channels as a fall back solution.

The window of opportunity for QKD is very small due to a fast **moving target**:

- The **moving target** cannot be easily accessed when it is deployed in space. This can be an advantage for preserving its physical integrity, or a disadvantage in case of malfunction/failure requiring repair.

7.6.8 Use Case Variant: Flying QKD Node

- A variant of the use case makes use of a moving platform to link two parts of a network separated by a long-haul path but in this case the Flying QKD Node makes a physical connection to the network at each end of the long-haul path.

- As described by figures 5 to 8 the platform C forms a physical link and separate QKD communications to the network nodes located at A and B. In this example the Flying QKD Node operates as if it is a Trusted Relay but with a time delay between each network link (determined by the travel time between A and B).

7.6.9 Functional Characteristics

Not available in the present document - see 'Foreword to the Present 1st Edition'.

8 Requirements

Not available in the present document - see 'Foreword to the Present 1st Edition'.

Annex A (informative): Authors and Contributors

The following people have contributed to the present document:

- Rapporteur DGS/QKD-0002_UserReqs
- Thomas Länger, Austrian Institute of Technology, www.ait.ac.at

Associated STF Expert:

- Mercedes Soto Rodriguez, Telefónica Investigacion y Desarrollo (www.tid.es)

Contributions by:

- Momtchil Peev, Austrian Institute of Technology (www.ait.ac.at)
- Romain Alléaume, Institut Télécom (www.institut-telecom.fr), and SeQureNet (www.sequrenet.fr)
- Alan Mink, Telcordia Visiting Researcher (www.telcordia.com)
- Brian Lowans, QinetiQ Group plc (www.qinetiq.com)
- Gaby Lenhart, European Telecommunications Standards Institute (www.etsi.org)

Annex B (informative): Bibliography

Renato Renner, Security of Quantum Key Distribution, Int. J. Quant. Inf., Vol. 6, 1-127 (2005) (online at http://arxiv.org/abs/quant-ph/0512258).

N Lütkenhaus and A J Shields, Focus on Quantum Cryptography: Theory and Practice, New J. Phys. Vol., 11 045005 (2009), (34 publications reflecting the current state of the art, available at http://www.iop.org/EJ/abstract/1367-2630/11/4/045005).

S. Ghernaouti-Hélie, I. Tashi, T. Länger, and C. Monyk, SECOQC Business Whitepaper(2008). (online http://arxiv.org/abs/0904.4073).

"How QKD can improve the security level of future e-commerce transactions", M.A Sfaxi I. Tashi S. Ghernaouti H´elie ISI - University of Lausanne CH-1015 Switzerland.

"Quantum Key Distribution (QKD) and Commodity Security Protocols: Introduction and Integration, National Institute of Standards and Technology (NIST)" , 100 Bureau Dr., Gaithersburg, MD 20899 A. Mink, S. Frankel and R. Perlner International Journal of Network Security & Its Applications (IJNSA), Vol 1, No 2, July 2009 101, (online http://airccse.org/journal/nsa/0709s9.pdf).

"ETSI Standardization of quantum key distribution and the ETSI standardization initiative", ISG-QKD, New J. of Phys. 11 055051 (16pp), Länger T and Lenhart G 2009. (online http://iopscience.iop.org/1367-2630/11/5/055051).

"The SECOQC quantum key distribution network in Vienna", Peev M, Pacher C, Alléaume R, Barreiro C, Bouda J, Boxleitner W, Debuisschert T, Diamanti E, Dianati M, Dynes JF, Fasel S, Fossier S, Fürst M, Gautier JD, Gay O, Gisin N, Grangier P, Happe A, Hasani Y, Hentschel M, Hübel H, Humer G, Länger T, Legré M, Lieger R, Lodewyck J, Lorünser T, Lütkenhaus N, Marhold A, Matyus T, Maurhart O, Monat L, Nauerth S, Page JB, Poppe A, Querasser E, Ribordy G, Robyr S, Salvail L, Sharpe AW, Shields AJ, Stucki D, Suda M, Tamas C, Themel T, Thew RT, Thoma Y, Treiber A, Trinkler P, Tualle-Brouri R, Vannel F, Walenta N, Weier H, Weinfurter H, Wimberger I, Yuan ZL, Zbinden H, Zeilinger A 2009 New J. of Phys. 11 075001 (37pp). (online http://iopscience.iop.org/1367-2630/11/7/075001).

History

Document history		
V1.1.1	June 2010	Publication