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

Individual copies of the present document can be downloaded from:
http://www.etsi.org

The present document may be made available in more than one electronic version or in print. In any case of existing or perceived difference in contents between such versions, the reference version is the Portable Document Format (PDF). In case of dispute, the reference shall be the printing on ETSI printers of the PDF version kept on a specific network drive within ETSI Secretariat.

Users of the present document should be aware that the document may be subject to revision or change of status. Information on the current status of this and other ETSI documents is available at
http://portal.etsi.org/tb/status/status.asp

If you find errors in the present document, please send your comment to one of the following services:
http://portal.etsi.org/chaircor/ETSI_support.asp

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.