JRC TECHNICAL REPORTS

Requirements of a Quantum Key Distribution Reference Platform

JRC Project 867 Quantum Cryptography Study

Adam Lewis, Carlo Ferigato and Lothar Breitenbach

2015

Report EUR 27039 EN

European Commission
Joint Research Centre
Institute for the Protection and Security of the Citizen

Contact information
Adam M. Lewis
Address: Joint Research Centre, Via Enrico Fermi 2749, TP 720, 21027 Ispra (VA), Italy
E-mail: Adam.Lewis@jrc.ec.europa.eu
Tel.: 39 0332 785786

JRC Science Hub https://ec.europa.eu/jrc

This publication is a Technical Report by the Joint Research Centre of the European Commission.

JRC93769

EUR 27039 EN

ISBN 978-92-79-44724-2

ISSN 1831-9424

doi:10.2788/76797

Luxembourg: Publications Office of the European Union, 2015

Requirements of a Quantum Key Distribution Reference Platform

JRC Project 867 Quantum Cryptography Study

Adam M Lewis, Carlo Ferigato and Lothar Breitenbach

Security Technology Assessment Unit
Institute for the Protection and Security of the Citizen
Joint Research Centre
2014

Background and Scope

A document stating requirements for a quantum key distribution (QKD) reference platform was planned as one of two deliverables from Project 867 Quantum Cryptography Study in 2014, the other deliverable being a feasibility study of JRC developing such a platform. By platform is meant a laboratory, or network of laboratories, which will evaluate QKD systems and report the results of the evaluations both publicly and privately, as needed. The advantage of separating the requirements and feasibility into different reports in this way is that it gives greater clarity as to which is which. The scope of this present report is therefore to define the required characteristics of a QKD reference platform which would make it useful for customers, manufacturers and policy-makers. Details, and where it is not immediately obvious, the rationale, are explained requirement by requirement. The applications which are at the moment of greatest interest for the JRC are also described.

The following key features of the sector have emerged from our study in 2014:

1. QKD technology is maturing, a number of start-up companies are offering products and there is also significant interest from large companies
2. Ambitious plans for QKD networks exist in US (Battelle), Japan (NICT) and China (QuantumCTek)
3. Standards for QKD systems have also already been drafted by an ETSI Industry Specification Group
4. The most important missing element needed for the sector to develop is a broad market.

Nevertheless, there do appear to be some significant challenges before a test and evaluation platform, which would offer something useful to users, could be implemented.

A list of companies may be found at http://www.quantiki.org/wiki/Private_sector_quantum_information_science . We are aware of one company listed which is no longer active in the field, and one which is active but not listed. Otherwise, the list appears to be up to date and comprehensive.
A recent discussion of the three networks outside Europe mentioned above took place at the 2014 QCRYPT conference and may be found on https://www.youtube.com/watch?v=fzFCOSuotWw .

The ETSI industry specification group (ISG) on QKD was set up with FP6 funding within the SECOQC (Secure Communication based on Quantum Cryptography) Project. It has established the following standards:

ETSI GS QKD 002 V1.1.1 QKD Use Cases
ETSI GS QKD 003 V1.1.1 QKD Components and Internal Interfaces
ETSI GS QKD 004 V1.1.1 QKD Application Interface
ETSI GS QKD 005 V1.1.1 QKD Security Proofs
ETSI GS QKD 008 V1.1.1 QKD Module Security Specification

At the moment, sales of QKD systems appear to be restricted to certain high-end financial systems and classified government communications. Further development requires diversifying into new applications. The JRC has experience of a number of public sector identity systems where quantum key distribution might potentially be applied. The exploratory research project of 2009 identified four, and two more have subsequently become apparent.

General Requirements

1. *Provide objective, independent and scientifically well-grounded evaluations of QKD technologies.*

2. *Support the standardization process, including as a user of standards*
   The reference platform should use the ETSI standards as the basis for its assessments. It would be very unhelpful and confusing to the community to start from scratch with different test methods, unless clear deficiencies were identified in the existing standards, which has not happened to date as far as we are aware. Proposals for improvements to the standards emerging from experience operating the reference platform should be presented to the ETSI ISG.

3. *Include both experimental and theoretical aspects in security assessments*
   QKD security depends on implementation of some QKD protocol, with well-understood security properties, by means of hardware and software that corresponds faithfully to the assumptions in that protocol. A reliable assessment of the strengths and weaknesses of any QKD system, or class of systems, requires a thorough understanding of both the QKD protocol itself and its practical implementation, as reflected in ETSI GS QKD 005 V1.1.1 QKD Security Proofs and ETSI GS QKD 008 V1.1.1 QKD Module Security Specification. It will be import to keep up-to-date on advances in QKD components, such as detectors and sources.

4. *Conduct security assessments using up-to-date knowledge about vulnerabilities*
   New vulnerabilities in QKD systems are discovered at approximately one per year. Some examples are the photon-number splitting attack, the detector blinding attack and exploitation of detector dead time. Any security assessment which fails to take into account the latest developments is worthless. It is essential to liaise closely with researchers, the so-called "quantum hackers", to stay up to date.

5. *Assess QKD systems for use in specific applications*
   At minimum this would involve analysis of the integration of QKD with the existing cryptographic systems used in context. This aspect is probably the most overlooked and the one that is critical to the adoption of the technology. Users of sophisticated information security technology are usually obliged to be conservative and can adopt new technologies only when they can be incorporated into existing systems with minimal risk and disruption. A complete evaluation for a specific application would also include a cost-benefit analysis.

6. *Cover (ideally all) different transmission paths and contexts*
   These are fibre optic and free space; for fibre, lit fibre and dark fibre, for free-space, terrestrial, airborne and satellite, and both static and mobile platforms.

7. *Cover (ideally all) different modes and protocols of QKD*
   These are single-photon and continuous wave, polarization-modulated and phase-modulated, non-entanglement based and entanglement-based, device-dependent, device-independent and partially device-independent protocols.

8. *Practise responsible disclosure of any security vulnerabilities detected*
   Companies must be allowed an opportunity to address any flaws in existing systems, without exposing the owners of installed systems to additional risk. Moreover, unless this policy is adopted, it will be impossible to obtain the full cooperation of manufacturers in evaluations. Consequently, the evaluation platform should not always make its findings public immediately but should do so with discretion, according to a well-defined procedure.

9. *Be operated according to a formal quality system*
   Ideally, the platform would be independently accredited by a recognized accreditation body.

10. *Respond positively to improvements proposed by users*

European Public-Sector Applications

In the exploratory project of 2009, four applications were considered:

Vessel Monitoring System and e-logbook for maritime applications
The single most important feature for this application is the requirement for free-space QKD for ship-to-shore or ship-to-satellite communications. The exploratory project also pointed out that there might be some contexts on large vessels where fibre optic QKD could be used inside a vessel.

Peer-to-peer network with traffic light protocol
The traffic light protocol (see e.g. https://www.us-cert.gov/tlp) is a set of designations used to ensure that sensitive information is shared with the correct audience. Information to be shared is labelled red (only amongst those party to the specific exchange), amber (only amongst individuals who need to know, within involved organizations), green (only within a defined community) or white (public). For example, information exchange within the JRC-managed European Reference Network for Critical Infrastructure Protection (ERNCIP) uses the TLP. The exploratory project hypothesized the case where there was a central "Trusted Agent Node" through which parties communicated, so that the distance limit on current QKD systems might not be severe restriction, a trusted node being present anyway.

The European Commission's confidential communications
TESTA (Trans European Services for Telematics between Administrations) is a communication platform to exchange electronic data between European and Member States administrations in a secure, reliable and efficient way, based on a private wide area network, originally fully isolated from the public internet. The current implementation, called sTESTA (s for secure) is in the process of being migrated to its successor TESTA ng (new generation), which will have enhanced services and security and will make use of the public internet for exchanging non-sensitive material. The architecture is based on a dedicated backbone called EuroDomain, to which individual administrative networks belonging to the Institutions or Member States are connected. It is designed for communications classified up to Restreint UE. Encryption is based on IPSEC, which supports triple DES and AES symmetric ciphers, but has also been the subject of controversy because of alleged insertion of deliberate security vulnerabilities.
Given the complexity of this network of networks, opportunities for enhancing security by means of QKD could exist of several points. The most obvious is within the EuroDomain backbone, but one could also imagine QKD being used for connections with the backbone and/or within institutional networks.

Reference
pieter.wellens@ec.europa.eu
TESTA NG Testa new generation 2nd International Conference on Cyber Crisis Cooperation and Exercises, 23-24 Sept 2013, Athens, Greece

Digital Tachograph
The EU Digital Tachograph system was introduced by Council Regulation 3821/85 as amended by Council Regulation 2135/98 and Commission Regulation 1360/2002. The last includes in Annex I(B) - Requirements for construction, testing, installation, and inspection - the technical description of the digital tachograph system.
The European Root Certification Authority (ERCA) was designed, implemented and is currently operated by the JRC on the Ispra site. Countries receive the symmetric and asymmetric encryption keys for use by their Member State Authority via trusted couriers, who come to JRC Ispra for an ERCA signing session. These are held, on average, twice a month. The public keys are then published in the ERCA web site. See http://dtc.jrc.ec.europa.eu .
The idea would be to try to replace this manual key distribution with QKD links. It would be possible to implement QKD only for some member states, where it was feasible and the country wanted it.

Two more applications have subsequently emerged which should be considered for evaluation.

Certificate distribution for e-passports

Electronic passports issued by EU member states have the capability of storing an encrypted image of the bearer's fingerprints in an ISO/IEC 14443 radio-frequency identity chip, embedded in the passport cover. Since this data is far more security-sensitive than the name, place and date of birth, place and date of issue, and photograph visible on the passport's main page, it is essential to ensure that it can be read only by authorised persons using certified equipment. This is achieved by encrypting the fingerprint data by elliptic curve cryptography and a suitable public key infrastructure, in which certificates are issued to "inspection systems" (=passport reader devices) by the "document verifier" (=the organisation responsible for the inspections systems) and the document verifier is certified by the "country verifying certification authority" (= the root authority for each member state). There is no European level certification authority for passports.

In many cases, the certification authorities will be physically situated in a major city, within a short enough distance of passport issuers and airports to allow direct fibre optic communication without repeaters, if such links exist or can be installed. Currently, certificates are distributed from the CVCA's to the DV's every three days by human courier. Using a secure electronic communications could reduce cost and eliminate the risk of physical theft of the certificates from the courier.

In the case of a DV responsible for a large number of IS's, for example a large airport, with several different passport check points, each with several different readers, quantum key distribution could be used to avoid the need to physically bring the certificates to each reader or the possible security risk of sending them on an internal network. The threat in this case would consist of a malicious party eavesdropping on the internal network. This is arguable the most immediately feasible opportunity because the environment is controlled and obtaining or installing dedicated fibre lines would be relatively simple. The distances would be short enough e.g. 10's of km, that no trusted nodes would be needed.

References

TechnicalGuideline TR-03110 (parts 1,2,3)
Advanced Security mechanisms for Machine Readable Travel Documents
Version 2.10 20th March 2012
Bundesamt fuer Sicherheit in der Informationstechnik

Technical Guideline TR-03129-2
PKIs for Machine Readable Travel Documents
Protocols for the Management of Certificates and CRLs
National Protocols for ePassport Application
Version 1.1 4th March 2014
Bundesamt fuer Sicherheit in der Informationstechnik

Proposal for an eIDAS Token

Regulation (EU) N°910/2014 on electronic identification and trust services for electronic transactions in the internal market (eIDAS Regulation) was adopted by the co-legislators on 23 July 2014, based on a proposal in Commission Communication COM(2012) 238 of 4 June 2012. It is considered to be a milestone in providing a predictable regulatory environment to enable secure and seamless electronic interactions between businesses, citizens and public authorities and so increase the effectiveness of public and private online services, eBusiness and electronic commerce in the EU.
http://eur-lex.europa.eu/legal-content/EN/TXT/?uri=uriserv:OJ.L_.2014.257.01.0073.01.ENG

BSI and ANSSI, the German and French IT security agencies, together with industry partners, have developed a concept for using the machine-readable travel document (MRTD) specification, as used for the e-passport, as the model for other applications of electronic identity within the eIDAS framework. Details, including a beta-version specification, may be found at
https://www.bsi.bund.de/EN/Publications/TechnicalGuidelines/TR03110/BSITR03110-eIDAS_Token_Specification.html;jsessionid=5BA25305CA0E5DF0954A615751F98627.2_cid359

Demonstration of quantum key distribution for MRTD's, as proposed above, would therefore open up an opportunity for its application for eIDAS tokens as well.

Conclusion

Based on the information gathered during 2014, as well as the experience of the exploratory project of 2009, ten general requirements for a quantum key distribution platform and six possible public sector European applications have been identified.

European Commission
EUR 27039 EN – Joint Research Centre – Institute for the Protection and Security of the Citizen
Title: Requirements of a Quantum Key Distribution Reference Platform

Author(s): Adam M. Lewis, Carlo Ferigato and Lothar Breitenbach

Luxembourg: Publications Office of the European Union

2015 – 10 pp. – 21.0 x 29.7 cm

EUR – Scientific and Technical Research series – ISSN 1831-9424

ISBN 978-92-79-44724-2

doi:10.2788/76797

Abstract

The concept of a quantum key distribution reference platform is defined and the background against which the requirements for such a platform have been identified is explained. Availability of products, forthcoming QKD networks, standards, and the character of the market are explained. The requirements themselves are listed, with a brief explanation of the rationale for each. The main applications of interest are described.

LB-NA-27039-EN-N

JRC Mission

As the Commission's in-house science service, the Joint Research Centre's mission is to provide EU policies with independent, evidence-based scientific and technical support throughout the whole policy cycle.

Working in close cooperation with policy Directorates-General, the JRC addresses key societal challenges while stimulating innovation through developing new methods, tools and standards, and sharing its know-how with the Member States, the scientific community and international partners.

Serving society
Stimulating innovation
Supporting legislation

Publications Office

doi:10.2788/76797

ISBN 978-92-79-44724-2