SQuaD

Schirmprojekt Quantenkommunikation Deutschland

Current needs for standardization activities in Quantum Communication

Findings from the SQuaD Standardization Workshops

Dr. Christian Goroncy
DIN e. V.

23.8.2024

GEFÖRDERT VOM

Bundesministerium
für Bildung
und Forschung

1. Introduction

Following intensive research in the field of Quantum Communication, the technological leap from science to industry is now imminent. It is being supported by SQuaD, the BMBF-funded Umbrella Project for Quantum Communication in Germany (Schirmprojekt Quantenkommunikation Deutschland, SQuaD) within the Innovation Hub for Quantum Communication. SQuaD plays a key role in ensuring that basic research and industry are optimally networked and connected in the coming years.

In close exchange within the SQuaD network key players from research and industry, such as the QuNET, QR.X, and DIVQSec initiatives, will learn and benefit from each other. In addition to enhanced cooperation, activities on standardization and certification are planned within the involvement of central organizations such as the Deutsche Institut für Normung (DIN) in order to validate commercial exploitation strategies.

The Goals of SQuaD are:

- Enabling the technology leap from science to industry;
- Creating a sustainable network between basic research and industry in the coming years and establishing an ongoing professional dialog between the sectors;
- Transferring current Quantum Communication Technologies sustainably into industrial applications;
- Establishing a comprehensive research network as an innovation hub for Quantum Communication in Germany;
- Laying the foundation for innovative, internationally competitive products in this key area of technology;
- Actively supporting activities for the certification and standardization of Quantum Technologies; as well as
- Making a significant contribution to Germany's continued leadership among the world's top technology providers.

Standardization is a crucial part for the establishment of quantum communication, as it lays down relevant requirements, ensures interoperability, and guarantees comparability across different quantum technologies. This helps in establishing consistent and reliable practices, facilitating integration and collaboration within the industry. Therefore, SQuaD centrally consolidates substantive contributions and positions (e.g., regarding the standardization of QKD protocols) from key stakeholders in Germany and develops a common position on standardization topics. This consensus will then be strategically and cohesively introduced into relevant standardization committees to achieve strong representation of Germany and relevant issues for the technological landscape in Germany. Conversely, through this coordinating work, SQuaD provides an overview of international quantum communication standardization activities and make this information centrally available and visible for interested stakeholders in Germany. This ensures efficient integration of quantum communication development with current standardization activities, allowing Germany to set standards, SQuaD is acting as a single point of contact. To support these activities effectively, SQuaD partner DIN informs and keeps scientists and industry stakeholders updated on standardization issues through workshops and informational events.

2. Standardization Workshop within SQuaD

DIN within its work in the SQuaD project recently conducted two workshops involving over 25 participants from industry, research, and public bodies in March 2025. The primary objective was to identify obstacles and needs in the field of quantum communication, focusing on potential solutions from both regulatory and normative perspectives. Instead of directly asking for standardization needs, which has proven insufficient in previous projects, the workshops were structured to identify obstacles and hurdles along the value chain. This approach ensures that the entire lifecycle of quantum communication technologies is considered, minimizing the risk of overlooking critical aspects. The participants explored issues across the value chain, which was divided into three main phases:

- Production and Hardware
- Installation and Integration
- Application

The statements and findings presented in this report are based on the opinions of individual experts and do not necessarily represent the views of SQuaD or its project partners. The below transcription and sorting of the workshop discussions aims to provide an accurate reflection and interpretation of the participants' inputs.

The SQuaD-project and especially DIN would like to thank all participants for their participation and contribution to the workshops. Additionally, a survey for evaluating these needs will be conducted, and more information about this survey will be published on the SQuaD webpage (www.squad-germany.de).

3. Results

In the consolidation of the findings from both workshops it became evident that some obstacles were mentioned multiple times, reflecting their occurrence in various phases of the value chain. The identified needs and obstacles were then categorized into four main groups:

- General
- Hardware
- Interoperability
- Security and Certification

Additionally, potential general solutions for the identified needs were developed and documented as thoroughly as possible. Where mentioned ongoing activities have also been added.

General

Need / Obstacle	Potential Solution	Ongoing Activities
Post Quantum Cryptography (PQC) vs. Quantum Key Distribution (QKD)		
- **unclear which technology will provide long time security**	- interoperability between different technologies should be envisaged and considered in all standardization activities	
- **migration from classical cryptography to QKD/PQC**	- defined procedure for migration - definition of interfaces for migration to quantum cryptography - using key hybridization to allow partial migration	
Life-Cycle Management		
- **undefined complete life-cycle management**	- identify all relevant parts of the life-cycle of quantum communication systems regarding security issues - define requirements that need to be fulfilled in the different phase of the full life-cycle management within standardization documents	
Added Value and User Needs		
- **unclear added value for companies and end users** - **no clear defined user and its required needs**	- authorities need to specify their product requirements regarding quantum cryptography and communicate them to relevant stakeholders - market analysis of existing user needs regarding quantum communication - establish exchange between suppliers and end users	
- **applications' requirements far from current quantum technologies capabilities**	- awareness raising for potential of quantum communication in counteracting the quantum computing thread with clearly stating its capabilities	
Development of Knowledge for Quantum Technology Application		
- **more knowledgeable stake-holders along the value chain**	- educate so called Quantum Engineers, e.g., within Quantum Engineering Master course	
- **low availability of national experts**	- standards enhance application of quantum communication without losing security or needing high knowledge quantum experts - align ongoing standardization activities on different levels within SQuaD - need to support standardization activities, not only by providing financial resources but also by emphasize its relevance as quantum technology is a strategic topic for Germany and Europe	
- **missing competence in testing agencies**	- develop competence in testing agencies	

Need / Obstacle	Potential Solution	Ongoing Activities
Policy and Collaboration		
- **collaboration on European level**	- establish CEN/CLC/JTC 22 as strategic hub for standardization issues within Europe	
- **no clear guidance from government or other authorities** - **4 NSAs in EU do not support QKD by now** - **authorities hesitate to use QKD due to lack of knowledge**	- describe the need for a European or national Quantum preparedness Act like in the US - adoption of solutions described in standards (consensus, transparent) increases trust in QKD	

Hardware

Need / Obstacle	Potential Solution	Ongoing Activities
Parameters and hardware requirements in general		
- **unclear, which parameters are relevant for application**	- definition of relevant parameters for application - measurement of defined parameters - defined scenarios for QKD characterization for evaluation of QKD performance - standardization document (e.g., TS) on quantum channel	
- **missing or not sufficient defined technical parameter for components in general**	- identification of relevant technical parameters for QC in general - definition of relevant parameters for components in standardization documents - ensuring that standards are applicable for all quantum technologies whenever possible - general standard on measurement values for quantum technologies as a whole - round ribbon test for performance / benchmarking	- QuNET+BlueCert - constitution of testing facilities
Definition and characterization of Quantum Communication System		
- **definition and characterization of a full quantum communication system and its assemblies**	- definition and characterization of full quantum technology systems and assemblies (e.g. pulse correction and photon number) - evaluate characteristics of systems (terminology, metrics, characteristics, measurement technique) - define characteristics of systems in standardization documents - develop implementation guidelines for suppliers	- DEP4 Nostradamus - test of QKD- and QComm-systems in testbeds

Need / Obstacle	Potential Solution	Ongoing Activities
Electrical and Mechanical Requirements		
- **missing electrical and mechanical requirements in general, as well as for components and systems**	- identification of relevant electrical and mechanical requirements - definition of relevant electrical and mechanical requirements in standardization documents - round ribbon test for performance / benchmarking	
KPIs		
- **missing KPIs for hardware or insufficient comparability of KPI in QKD systems (different assumptions, scenarios, configuration)**	- definition of KPIs - standardized procedure to measure KPIs - characterization of parameters, physical prop., systems, subsystems and benchmarking, evaluation methodology - Benchmarking/ standards for protocols, implementation, key performance indicators (security level, range, key rate, etc.) - definition of an evaluation methodology	- European Qu-Test Initiative - Interfaces in ETSI ISG QKD - ETSI PP for prepare and measure QKD Systems - ongoing activities for security proof of QKD protocols for real devices
Fiber		
- **missing or not sufficient defined technical parameter for fibers**	- development of standardization documents for fiber requirements (range, types, losses OTDR), that are general applicable and not only for QC - definition of classes of range within standardization document - development standardized test procedure for fibers	
- **unclear impact of extraneous light**	- requirements to detect and evaluate the impact of extraneous light on fibers - development standardized test procedure for fibers	
Single Photon Devices		
- **no standardized requirements for single photon devices**	- development of standardization documents for single photon devices	
Trusted Nodes		
- **low range of QKD requires trusted nodes**	- further research to improve range	
- **unclear whether a trusted node is a device or device container**	- definition whether a trusted node is a device or device container - standard for configuration of trusted nodes	

Interoperability

Need / Obstacle	potential solution	ongoing activities
High technological variety of QKD-Sytems		
- **high technological variety of unstandardized QKD-technologies and protocols**	- standardization document (e.g., TR) for description of different techniques and protocols - standardization document (e.g., TS) for quantum channels	
Interfaces		
- **interoperable implementation of QKD interfaces**	- identification of relevant interfaces - define requirements for interfaces within standardization documents	
- **interaction of different devices and components** - **lack of viable standards for QKD networks**	- further development of standards and implementation guidelines for manufacturers - definition of parameters of the full system - characterization of relevant parameters for the full systems - round ribbon test for performance / benchmarking	- WI 022 ETSI ISG QKD Network architecture - JTC 22 /WG4 TR 1(Lessons learned about QKD-Networks)
Integration in Existing Systems		
- **integration in existing management systems**	- defined QKD management systems requirements within standardization documents	
- **unsatisfied integration of QKD keys in application** - **incompatibility of KMS**	- adaption of existing standards to integrate external keys - definition of horizontal compatibility of KMS from different vendors - standardization of KMS systems to overcome proprietary issues - development of a standardized horizontal interface for KMS-KMS	ETSI WI 21 – horizontal interoperability
Hybridization Path		
- **lack of clear hybridization path / mechanism**	- standardization documents for hybridization of various cryptographic primitives - standardization documents for hybridization of QKD with classical cryptography	- ETSI TC Cyber WI 15

Security and Certification

Need / Obstacle	potential solution	ongoing activities
General		
- **gap between measurements and the overall implication on the security**	- defined KPI regarding security and how to measure them - characterization of parameters, physical prop., systems, subsystems and benchmarking within standardization document	
No Clear Requirements for Security		
- **undefined security levels and different difficulty level of testbeds**	- definition of security levels with certain requirements in standardization documents - European wide agreement on security levels, definition in European standards preferred - evaluate and define attack ranking and countermeasure efficiency - standardization document with defined conformity proofs	
- **lack of agreement on potential rating for security evaluations and high variety of QKD-attacks**	- define requirements for risk analysis - standardized description of QKD-attacks and countermeasures	
Protection profile		
- **missing standards for hardware authentication/validation and its implementation**	- develop standardization documents to implement hardware authentication/validation, conformity proofs, protection profile by CC - definition of attacks rankings and countermeasure efficiency - develop standardization document or guideline for the implementation of PP	
- **missing secure QKD protocol or provable security**	- develop standardized QKD protocols	
Security of Trusted Nodes		
- **lack of definition of security need for trusted nodes**	- standardized security requirements for trusted nodes on a European basis - defined requirements by national security agencies - standards/definition for security levels for trusted nodes for various EU security levels - physical requirements for trusted nodes (safe, …)	

Need / Obstacle	potential solution	ongoing activities
Operative Service		
- **missing guidelines for operative service of QKD components in system**	- guidelines for anomaly detection and handling in systems	
Missing Application Interface		
- **missing secure application interface and certification handling**	- development of a standard ETSI 004+ or similar - alternative or update to ETSI 014 or ETSI 004 with reference implementation	
Initial Secrets / PSK		
- **missing requirements for initial secrets / PSK mechanism**	- define requirements for initial secret / PSK mechanism in standardization documents	
Certification		
- **missing certification in general and relevant documents**	- development of requirements for certification - regulative definition of requirements for certification - certified testing agency for quantum cryptography - standardized relevant basic documents for future certification - identification of relevant security parameter for QC (Ypsilon)	QuNET project DEP4 Nostradamus
- **theoretic prove vs. practical application for certification**	- new certification documents (PP2)	
- **no listed QKD products exist**	- list QKD products publicly when security has been proved	