30 years of Poznan Supercomputing and Networking Center

61-139 Poznań
ul. Jana Pawła II 10
phone: (+48 61) 858-20-01
fax: (+48 61) 852-59-54
office@man.poznan.pl
www.psnc.pl

Piotr Rydlichowski

QKD Technology Standardisation Landscape

QKD Technology Standardization Landscape

Standards Developing Organisations.

- ETSI was the standards developing organisation (SDO) starting QKD standardisation in 2008. The ETSI Industry Specification Group for Quantum Key Distribution (ISG-QKD) was born from the QT community established by the European FP6 project, SECOQC. To date it has produced **14 Group Specifications and Reports** in areas such as protocol security, implementation security, component and module characterisation, key delivery, and use cases. The ISG-QKD has also been an important forum in the QT community, helping to shape recent research and innovation projects, such as OPENQKD.
- The emergence of commercial-grade products for QKD and Quantum Random Number Generation, and their uptake by early adopters in the past few years has produced a surge in interest in QT standards. Membership of the ETSI ISG has swelled to include equipment vendors, telecom operators, end users, national metrology institutes and leading security researchers and the pace of development has increased. In parallel, and to a large extent in competition,
- Several other SDOs have established initiatives in QT, including CEN/CENELEC, ISO/IEC, IEEE and ITU-T.

QKD Technology Standardization Landscape

National Standardisation examples:

- BSI TR 021012, Cryptographic methods: Recommendations and key lengths
- NIST Cryptographic Technology (CT) Group
- Japan, the Cryptographic Research and Evaluation Committee (CRYPTREC)

QKD Technology Standardization Landscape

European Standardisation examples:

- CEN-CENELEC Focus Group on Quantum Technologies (FGQT)
- ETSI ISG-QKD
- ETSI TC CYBER WG QSC9 (Technical Committee Cyber Security Working Group for Quantum-Safe Cryptography)

QKD Technology Standardization Landscape

International Standardisation examples:

- ISO/IEC JTC 1/SC 2712 “IT Security” is the Sub-Committee 27 of the Joint Technical Committee 1 of ISO and IEC. The SC 27 develops standards for IT security, cybersecurity and privacy protection. The QKD work items are part of working group WG3 “Security evaluation, testing and specification”, which also develops and maintains the ISO/IEC 15408 Common Criteria for Information Technology Security Evaluation (CC) standard itself. The two QKD security evaluation standards currently being developed in WG3, ISO/IEC 23837-1 and 2 both are “applications” of the Common Criteria paradigm to QKD.
- ITU-T/SG 1313 “Future Networks” dealing with next-generation networks and their evolution, while focusing on future networks and network aspects of mobile telecommunications and their QKD related work items prefixed with “ITU-T Y.QKDN”. ITU-T/SG 1714 “Security” coordinates security-related work across all ITU-T Study Groups and their QKD related work items prefixed with “ITU-T TR” and “ITU-T X”. ITU-T FG-QIT4N15 (Focus Group on Quantum Information Technology for Networks) was established in September 2019 to tackle pre-standardisation issues of quantum information technology for networks
- Quantum Internet Research Group (QIRG)
- Crypto Forum Research Group (CFRG)
- International group IEEE SA QuantumComm – Software-Defined Quantum Communication (P1913)
- GSMA Internet Group (Groupe Speciale Mobile Association)

QKD Technology Standardization Landscape

Standards in quantum communications module security.

Published standards				
SDO	Document number	Document title	Version	Publ. date
ETSI	GR QKD 003	Quantum Key Distribution (QKD); Components and Internal Interfaces	V2.1.1	2018-03
ETSI	GR QSC 004	Quantum-Safe Cryptography; Quantum-Safe threat assessment	V1.1.1	2017-03
ETSI	GS QKD 005	Quantum Key Distribution (QKD); Security Proofs	V1.1.1	2010-12
ETSI	GS QKD 008	Quantum Key Distribution (QKD); QKD Module Security Specification	V1.1.1	2010-12
ETSI	GS QKD 011	Quantum Key Distribution (QKD); Component characterization: characterizing optical components for QKD systems	V1.1.1	2016-05
ETSI	GS QKD 012	Quantum Key Distribution (QKD); Device and Communication Channel Parameters for QKD Deployment	V1.1.1	2019-02
ETSI	GS QKD 016	Quantum Key Distribution (QKD); Protection Profile (PP)	V.1.1.1	2023-04

QKD Technology Standardization Landscape

Standards in quantum communications module security.

Standards in draft/revision				
SDO	Document number	Document title	Version	Expected publ. date
ETSI	GS QKD 005	Quantum Key Distribution (QKD); Security Proofs	V2.1.1	2023-04
ETSI	GS QKD 010	Quantum Key Distribution (QKD); Implementation security: Protection against trojan horse attacks in one-way QKD systems	V.1.1.1	2023-04
ETSI	GS QKD 013	Quantum Key Distribution (QKD); Characterisation of optical output of QKD transmitter modules	V1.1.1	2023-07
ETSI	GS QKD 016	Quantum Key Distribution (QKD); Protection Profile (PP) (This is intended to be a certified update to the PP.)	V.2.1.1	TBC
ETSI	GR QKD 019	Quantum Key Distribution (QKD); Design of QKD interfaces with Authentication		2023-07
ISO/IEC	23837-1	Information security – Security requirements, test and evaluation methods for quantum key distribution – Part 1: Requirements		Approved- Publication TBC
ISO/IEC	23837-2	Information security – Security requirements, test and evaluation methods for quantum key distribution – Part 2: Test and evaluation methods		Approved- Publication TBC

QKD Technology Standardization Landscape

Interface standards in the area of network interoperability.

Published standards				
SDO	Document number	Document title	Version	Publ. date
ETSI	GS QKD 004	Quantum Key Distribution (QKD); Application Interface	V2.1.1	2020-08
	GS QKD 014	Quantum Key Distribution (QKD); Protocol and data format of REST-based key delivery API	V1.1.1	2019-02
	GS QKD 015	Quantum Key Distribution (QKD); Quantum Key Distribution control interface for software defined Networks	V2.1.1	2022-04
	GS QKD 018	Quantum Key Distribution (QKD); Orchestration Interface of Software Defined Networks	V1.1.1	2022-04
Standards in draft/revision				
SDO	Document number	Document title	Version	Expected publ. date
ETSI	GS QKD 020	Quantum Key Distribution (QKD); Protocol and data format of REST-based Interoperable Key Management System API	V1.1.1	2023-09
ITU-T SG 11	Q.QKDN_profr	Quantum key distribution networks – Protocol framework		Drafting
	Q.QKDN_Ak	Protocols for Ak interface for QKDN		Drafting
	Q.QKDN_Ck	Protocols for Ck interface for QKDN		Drafting
	Q.QKDN_Kx	Protocols for Kx interface for QKDN		Drafting
	Q.QKDN_Kq-1	Protocols for Kq-1 interface for QKDN		Drafting

QKD Technology Standardization Landscape

Other standards in the area of network interoperability.

Published standards				
SDO	Document number	Document title	Version	Publ. date
ITU-T SG 13	Y.3800 (ex Y.QKDN_FR)	Overview on networks supporting quantum key distribution Corrigendum 1		2019-10 2020-04
	Y.3801 (ex Y.QKDN-req)	Functional requirements for quantum key distribution networks		2020-04
	Y.3802 (ex Y.QKDN_Arch)	Quantum key distribution networks – Functional architecture		2020-12
	Y.3803 (ex Y.QKDN_KM)	Quantum key distribution networks – Key management		2020-12
	Y.3804 (ex Y.QKDN_CM)	Quantum key distribution networks – Control and management		2020-09
	Y.3805 (ex Y.QKDN_SDNC)	Quantum key distribution networks – Software-defined networking control		2021-12
	Y.3806 (ex Y.QKDN-qos-req) (ex Y.QKDN-qos-gen)	Quantum key distribution networks – Requirements for quality of service assurance		2021-09
	Y.3807 (ex Y.QKDN-qos-pa)	Quantum key distribution networks – Quality of service parameters		2022-02
	Y.3810 (ex Y.QKDN-iwfr)	Quantum key distribution network interworking – Framework		2022-09
	Y.3811 (ex Y.QKDN-qos-arc)	Quantum key distribution networks – Functional architecture for quality of service assurance		2022-09
	Y.3812 (ex Y.QKDN-qos-ml-req)	Quantum key distribution networks – Requirements for machine learning based quality of service assurance		2022-09

QKD Technology Standardization Landscape

Other standards in the area of network interoperability.

Standards in draft/revision				
SDO	Document number	Document title	Version	Expected publ. date
ETSI	GS QKD 017	Quantum Key Distribution (QKD); Network architectures	V1.1.1	2023-07
ITU-T SG 13	Y.3813 (ex Y.QKDN-iwrq)	Quantum key distribution networks interworking – functional requirements		Drafting (Consented)
	Y.3814 (ex Y.QKDN-ml-fra)	Quantum key distribution networks - functional requirements and architecture for machine learning enablement		Drafting (Consented)
ITU-T SG 13	Y.QKDN-qos-iw-req	Requirements of QoS assurance for QKDN interworking		Drafting
	Y.QKDN-qos-ml-fa	Quantum key distribution networks - Functional architecture enhancement for machine-learning based quality of service assurance		Drafting
	Y.QKDN-qos-mmq	Quantum key distribution Networks - Measurement methodology for QoS parameters		Drafting
	Y.QKDN- iwac	Quantum key distribution networks interworking – architecture		Drafting
	Y.QKDN-amc	Quantum key distribution networks - Requirements and architectural model for autonomic management and control		Drafting
	Y.QKDNf-fr	Framework of Quantum Key Distribution Network Federation		Drafting
	Y.QKDNi-SDNC	Quantum Key Distribution Network Interworking – Software Defined Networking Control		Drafting
	Y.QKDN-rsfr	Framework of quantum key distribution network resilience		Drafting

QKD Technology Standardization Landscape

Standards in the area of roadmaps applications, use cases etc.

Published standards				
SDO	Document number	Document title	Version	Publ. date
CEN/CENELEC FGQT	FGQT Q04 and FGQT Q05	FGQT Quantum Technologies Standardisation Roadmap	V1.0	Drafting (expected 2023-03)
ETSI	GS QKD 002	Quantum Key Distribution (QKD); Use Cases Use cases	V1.1.1	2010-06
ITU-T SG 13	Y.3808 (ex Y.QKDN_frint)	Framework for integration of quantum key distribution network and secure storage network		2022-02
	Y.3809 (ex Y.QKDN_BM)	A role-based model in quantum key distribution networks deployment		2022-02
	Y Suppl. 70	Y.3800-series – Quantum key distribution networks – Applications of machine learning		2021-07
Standards in draft/revision				
SDO	Document number	Document title	Version	Expected publ. date
ITU-T SG 13	Y.QKDN_SSNarch	Functional architecture for integration of quantum key distribution network and secure storage network		Drafting
	Y.QKDN_SSNreq	Functional requirements for integration of quantum key distribution network and secure storage network		Drafting
	Y.supp.QKDN-roadmap	Standardization roadmap on Quantum Key Distribution Networks		Drafting
	Y.Supp.QKDN-UC	Use cases of quantum key distribution networks		Drafting
	TR.QN-UC	Use cases of quantum networks beyond QKDN		Drafting
	Y.TR-QEFN	ITU-T's Views for Quantum-Enabled Future Networks		Drafting

QKD Technology Standardization Landscape

Standards in quantum networks security.

SDO	Document number	Document title	Version	Publ. date
ETSI	GS QSC 003	Quantum Safe Cryptography; Case Studies and Deployment Scenarios	V1.1.1	2017-02
ITU-T SG 17	X.1710 (ex X.sec-QKDN-ov)	Security framework for quantum key distribution networks		2020-10
	X.1712 (ex X.sec-QKDN-km)	Security requirements and measures for quantum key distribution networks – key management Corrigendum 1		2021-10 2022-02
	X.1714 (ex X.cf-QKDN)	Key combination and confidential key supply for quantum key distribution networks		2020-10
	X.1715 (ex X.sec_QKDN_intrq)	Security requirements and measures for integration of quantum key distribution network and secure storage network		2022-07
	XSTR-SEC-QKD	Security considerations for quantum key distribution networks		2020-03
	XSTR-HYB-QKD (ex TR.hyb-qkd) (ex TR.hybsec-qkdn)	Overview of hybrid approaches for key exchange with Quantum Key Distribution		2022-05
Standards in draft/revision				
SDO	Document number	Document title	Version	Expected publ. date
ITU-T SG 17	X.sec_QKDN_AA	Authentication and authorization in QKDN using quantum safe cryptography		Drafting
	X.sec_QKDN_CM	Security requirements and measures for quantum key distribution networks - control and management		Drafting
	X.sec_QKDNi	Security requirements for Quantum Key Distribution Network interworking (QKDNi)		Drafting
	X.sec-QKDN-tn	Security requirements and designs for quantum key distribution networks - trusted node		Drafting

QKD Technology Standardization Landscape

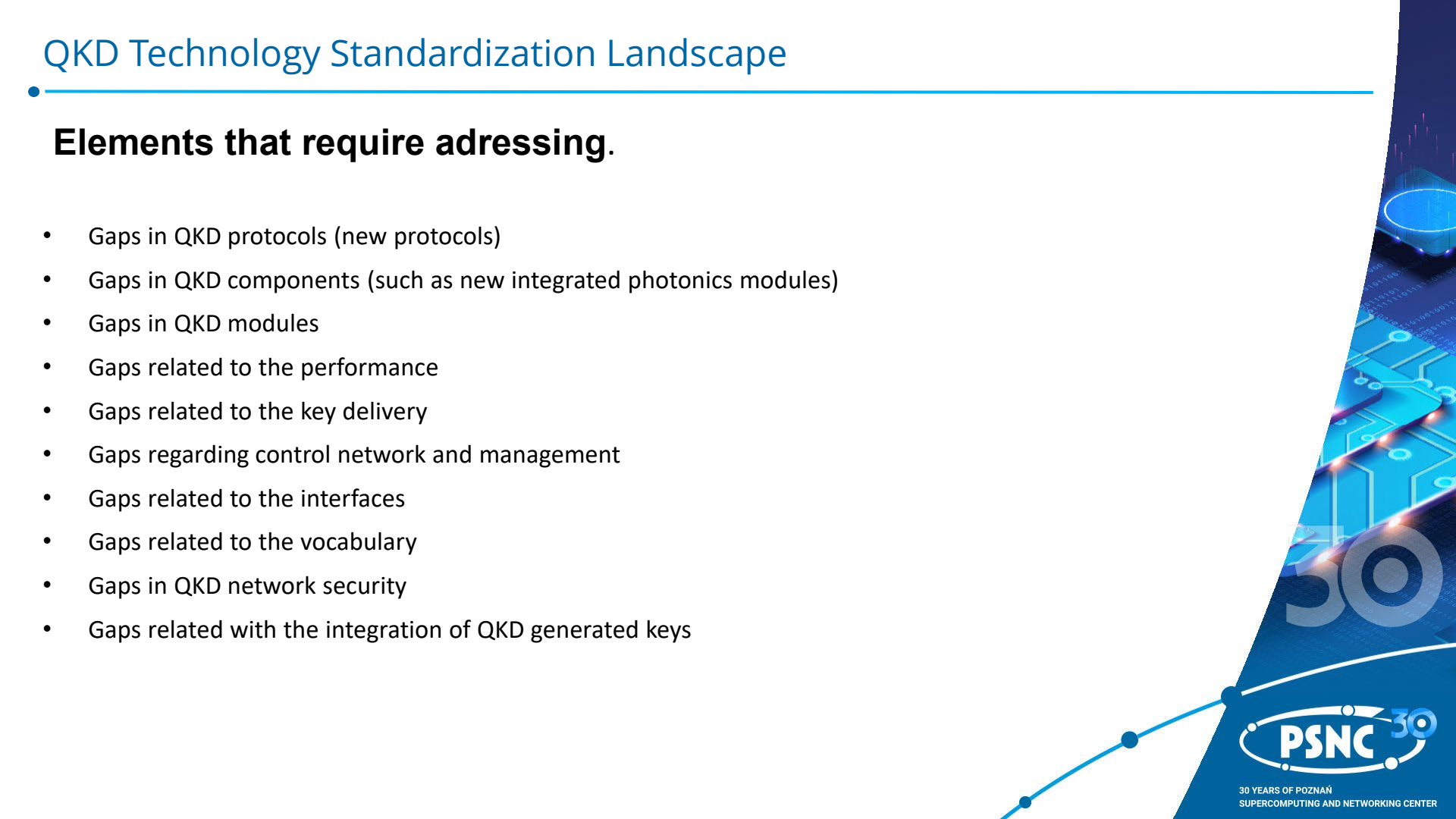
Other standards related to QKD.

Published standards				
SDO	Document number	Document title	Version	Publ. date
ETSI	GR QSC 001	Quantum-Safe Cryptography (QSC); Quan-tum-safe algorithmic framework	V1.1.1	2016-07
	GR QSC 006	Quantum-Safe Cryptography (QSC); Limits to Quantum Computing applied to symmetric key sizes	V1.1.1	2017-02
	TR 103570	CYBER; Quantum-Safe Key Exchanges	V1.1.1	2017-10
	GR QKD 007	Quantum Key Distribution (QKD); Vocabulary	V1.1.1	2018-12
Standards in draft/revision				
SDO	Document number	Document title	Version	Expected publ. date
ETSI	GR QKD 007	Quantum Key Distribution (QKD); Vocabulary	V2.1.1	2023-05
IEEE	P1913	Software-Defined Quantum Communication		Drafting
	P7130	Standard for Quantum Technologies Definitions		Drafting
	P3172	Recommended Practice for Post-Quantum Cryptography Migration		Drafting
	P1943	Standard for Post-Quantum Network Security		Drafting
IRTF	draft-irtf-qirg-principles	Architectural Principles for a Quantum Internet		Under approval
	draft-irtf-qirg-quantum-internet-use-cases	Application Scenarios for the Quantum Internet		Drafting

QKD Technology Standardization Landscape

Elements that require adressing.

- Gaps in QKD protocols (new protocols)
- Gaps in QKD components (such as new integrated photonics modules)
- Gaps in QKD modules
- Gaps related to the performance
- Gaps related to the key delivery
- Gaps regarding control network and management
- Gaps related to the interfaces
- Gaps related to the vocabulary
- Gaps in QKD network security
- Gaps related with the integration of QKD generated keys



QKD Technology Standardization Landscape

Elements related to strategic standardisation roadmap

- Quantum communication module and link security
- Fibre network interoperability
- Quantum network security
- Free-space QKD (terrestrial and satellite)
- QT and QKD are strategic elements for standardisation and need to be coordinated between each other

Poznań Supercomputing and Networking Center

61-139 Poznań
ul. Jana Pawła II 10
phone: (+48 61) 858-20-01
fax: (+48 61) 852-59-54
office@man.poznan.pl
www.psnc.pl