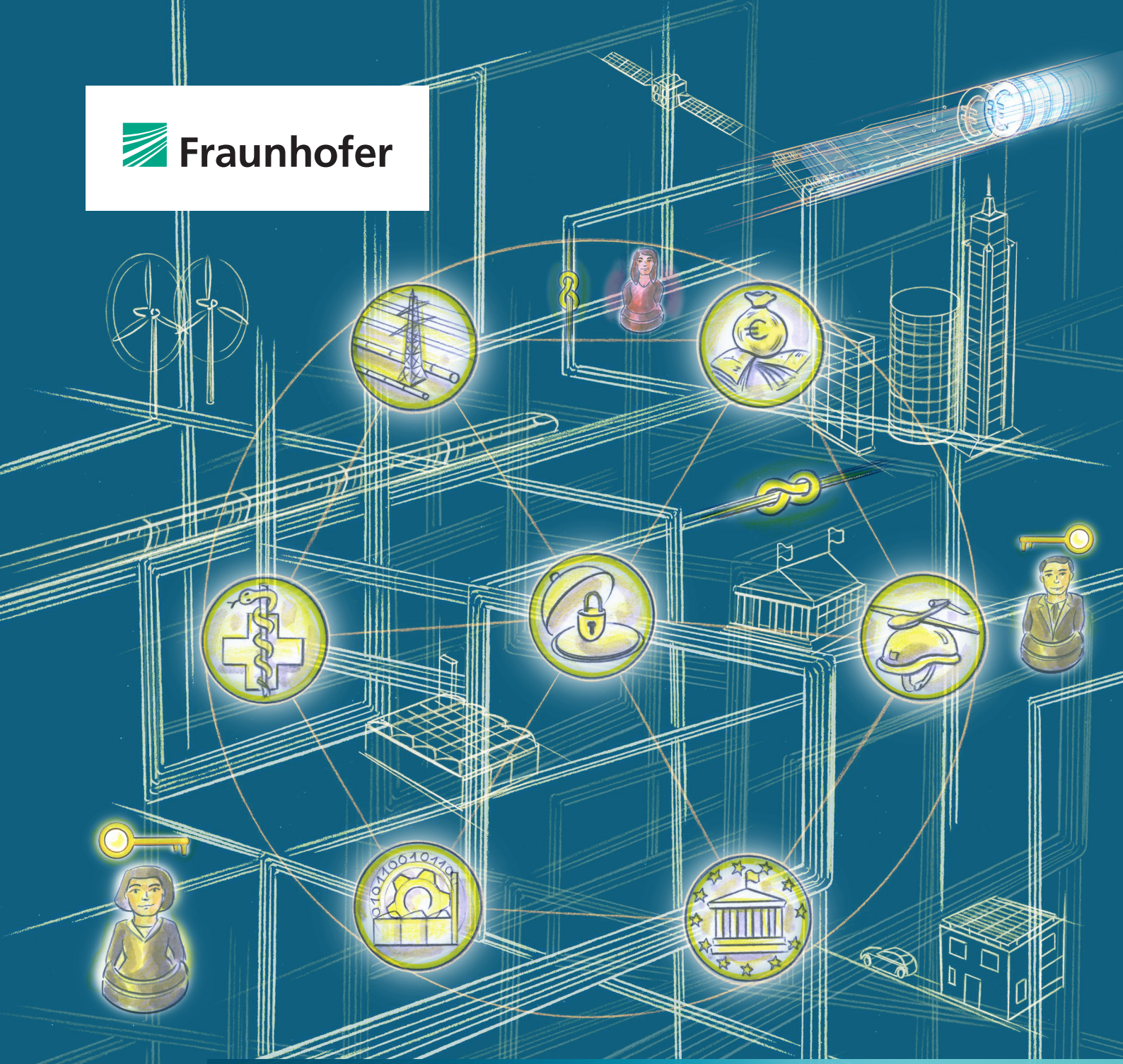
Fraunhofer



June 2025

Application Perspectives in Quantum Communication

Publishing Notes

Application Perspectives in Quantum Communication

Report coordination

Fraunhofer Institute for Systems and Innovation Research ISI

Breslauer Str. 48, 76139 Karlsruhe, Germany
Thomas Schmaltz, thomas.schmaltz@isi.fraunhofer.de

Responsible for content

Thomas Schmaltz, Fraunhofer ISI, thomas.schmaltz@isi.fraunhofer.de
Chie Endo, Fraunhofer ISI, chie.endo@isi.fraunhofer.de
Lukas Weymann, Fraunhofer ISI, lukas.weymann@isi.fraunhofer.de
Tim Wicke, Fraunhofer ISI, tim.wicke@isi.fraunhofer.de
Saeideh Shirinzadeh, Fraunhofer ISI, saeideh.shirinzadeh@isi.fraunhofer.de
Michael Friedewald, Fraunhofer ISI, michael.friedewald@isi.fraunhofer.de
Bernd Beckert, Fraunhofer ISI, bernd.beckert@isi.fraunhofer.de
Christian Goroncy, DIN, Christian.Goroncy@din.de
Henrike Wissing, Fraunhofer HHI, henrike.wissing@hhi.fraunhofer.de
Thorsten A. Goebel, Fraunhofer IOF, thorsten.albert.goebel@iof.fraunhofer.de
Nino Walenta, Fraunhofer HHI, nino.walenta@hhi.fraunhofer.de

Contributing institutes

Fraunhofer Institute for Telecommunications, Heinrich-Hertz-Institut, HHI

Einsteinufer 37,10587 Berlin
Nino Walenta, nino.walenta@hhi.fraunhofer.de
Henrike Wissing, henrike.wissing@hhi.fraunhofer.de

Fraunhofer Institute for Applied Optics and Precision Engineering IOF

Albert-Einstein-Str. 7, 07745 Jena
Thorsten A. Goebel, thorsten.albert.goebel@iof.fraunhofer.de

DIN e. V. (German Institute for Standardization)

Am DIN-Platz, Burggrafenstraße 6, 10787 Berlin
Christian Goroncy, Christian.Goroncy@din.de

Compiled in the context of the

Umbrella Project for Quantum Communication in Germany (Schirmprojekt Quantenkommunikation Deutschland – SQuaD), funded by the Federal Ministry of Research, Technology and Space (Bundesministerium für Forschung, Technologie und Raumfahrt – BMFTR)

With funding from the:

Federal Ministry of Research, Technology and Space

Picture credits

Cover page: Heyko Stöber, Hohenstein

Published

June 2025

DOI

doi: 10.24406/publica-4734

License

Notes

Contents

Zusammenfassung und Kernergebnisse (German)

Kontext

Der zunehmende Bedarf an IT-Sicherheit und die potenziellen Gefahren, die Quantencomputer für klassische Verschlüsselung bringen, haben zu einem wachsenden Interesse an quantensicherer Kryptografie geführt. Bei korrekter Umsetzung verspricht die Quantenschlüsselverteilung (QKD) eine quantensichere Option für die Kryptografie, die zur sicheren Übermittlung streng vertraulicher Informationen genutzt werden kann. Sie hat daher großes Potenzial für Bereiche, die mit kritischen und geheimen Informationen arbeiten, wie zum Beispiel die öffentliche Verwaltung, das Militär und der Medizinsektor. Dieser Bericht erörtert Anwendungsmöglichkeiten für QKD in verschiedenen Sektoren, einschließlich Netzwerkaspekten, Standardisierung und Zertifizierung, die die Einführung von QKD stark beeinflussen. Weitere Anwendungen der Quantenkommunikation, die über QKD hinausgehen, werden ebenfalls diskutiert.

Sichere Kommunikation – Status Quo und Rahmenbedingungen.

Sichere Kommunikation wird immer wichtiger und regulatorische Rahmenbedingungen versuchen Mindeststandards für Cybersicherheit durchzusetzen. Zu den wichtigsten Regelungen in der EU gehören die NIS-Richtlinie (eine Richtlinie zur Sicherheit von Netz- und Informationssystemen), die NIS2-Richtlinie (eine Richtlinie über Maßnahmen zur Erreichung eines hohen Cybersicherheitsniveaus in der Europäischen Union) und die CER-Richtlinie zur Resilienz kritischer Einrichtungen (eine Richtlinie zur Stärkung der Resilienz kritischer Einrichtungen gegenüber physischen Bedrohungen wie Naturkatastrophen, Terrorismus oder Sabotage). Die Anforderungen sind jedoch je nach Sektor unterschiedlich, weshalb es wichtig ist, die Rahmenbedingungen der einzelnen Sektoren zu kennen, wenn QKD als Cybersicherheitslösung implementiert werden soll.

Die aktuelle Cybersicherheitslösung basiert auf Verschlüsselung mit schlüsselbasierten Verfahren, die in symmetrische und asymmetrische Verfahren unterteilt werden können. Symmetrische Schlüssel gelten zwar als sicherer, aber der sichere Schlüsselaustausch ist kompliziert. Deshalb werden derzeit häufig asymmetrische Schlüssel verwendet. Diese beruhen auf mathematischen Problemen, die mit klassischen Computern nicht einfach zu lösen sind. Mit dem Aufkommen von Quantencomputern dürften asymmetrische Schlüssel mittelfristig jedoch unsicher werden. Daher ist ein Übergang zu einer sogenannten quantensicheren Kryptografie unter Verwendung von Algorithmen der Post-Quantum-Cryptography (PQC) und möglicherweise QKD von entscheidender Bedeutung.

Allgemeine Herausforderungen für die QKD-Technologie

Obwohl QKD eine vielversprechende Option für quantensichere Kryptografie ist, gibt es noch verschiedene Herausforderungen, die einer breiteren Einführung im Wege stehen. Zu diesen Herausforderungen gehören:

Entfernungsbeschränkungen: Glasfaserbasierte QKD ist derzeit auf Entfernungen von etwa 100 Kilometern beschränkt, möglicherweise etwas weiter, jedoch auf Kosten einer deutlichen Verringerung der Schlüsselraten. Für die Kommunikation über große Entfernungen sind vertrauenswürdige Knoten oder Quantenrepeater erforderlich. Vertrauenswürdige Knoten stellen zwar eine zusätzliche Sicherheitslücke dar, Quantenrepeater sind jedoch noch nicht kommerziell verfügbar und werden voraussichtlich auch nicht vor 2035 auf den Markt kommen. Satellitengestütztes QKD, das größere Entfernungen überbrücken kann, ist weniger ausgereift, teurer und mit zusätzlichen Herausforderungen verbunden.

Stabilität, Robustheit und Schlüsselraten: Viele QKD-Systeme sind noch nicht ausreichend stabil und robust und erfordern weitere technische Verbesserungen und Optimierungen für eine breite Implementierung. Die Schlüsselraten sind zwar für viele Anwendungen ausreichend, aber noch begrenzt.

Seitenkanalangriffe: Obwohl QKD einen physikalisch sicheren Schlüsselaustausch verspricht, sind externe Angriffe weiterhin möglich. Die Beseitigung dieser sogenannten Seitenkanal-Schwachstellen ist für eine sichere Kommunikation über QKD unerlässlich.

Integration, Infrastrukturbedarf und Kosten: QKD muss in die bestehende IT-Sicherheitsinfrastruktur integriert werden, was beispielsweise Herausforderungen hinsichtlich der Interoperabilität mit sich bringt. Derzeit ist QKD auf nicht parallel zu Telekommunikationszwecken genutzte Glasfaser-Verbindungen (Dark Fiber) angewiesen, was zu hohen Infrastrukturkosten für die Implementierung von QKD führt. Auch die QKD-Geräte selbst sind noch recht teuer.

Standardisierung, Zertifizierung und Zulassung: Zusätzlich zu den oben genannten Herausforderungen behindert das Fehlen standardisierter, zertifizierter und zugelassener QKD-Systeme/-Protokolle die Einführung von QKD in Sektoren, die auf zertifizierte oder zugelassene IT-Sicherheitsprodukte angewiesen sind.

Bewusstsein und Akzeptanz: In vielen Branchen ist das Bewusstsein für die Quantenbedrohung und mögliche quantensichere Lösungen nur begrenzt vorhanden. Andererseits ist die Zurückhaltung gegenüber einer Umstellung der derzeit laufenden Systeme groß.

Risiken in der Lieferkette: Die Lieferkette für QKD sollte diversifiziert werden, um geostrategische Abhängigkeiten zu begrenzen und technologische Souveränität in der Quantenkommunikation zu erreichen.

Sektorspezifische Anwendungsszenarien

Öffentliche Verwaltung: Regierungen gelten aufgrund ihres Bedarfs an sehr hoher Datensicherheit als wichtige potenzielle Kunden für QKD. Der Übergang zu quantensicherer Kryptografie ist auch aufgrund der Notwendigkeit langfristiger Sicherheit dringend erforderlich. Allerdings sind die europäischen Länder derzeit noch zurückhaltend bei der Einführung von QKD, da es noch nicht ausgereift ist und es keine zertifizierten und zugelassenen QKD-Systeme gibt. Folglich hat dieser Sektor ein mittleres bis hohes Marktpotenzial für QKD, aber eine nennenswerte Umsetzung vor 2030 ist unwahrscheinlich.

Militär: Die Anforderungen an die Datensicherheit im Militär- und Verteidigungssektor sind ebenso hoch wie in der öffentlichen Verwaltung, und auch hier ist ein langfristiger Schutz der kommunizierten Informationen erforderlich. Da symmetrische Schlüsselverteilungsprozesse (z. B. per Kurier) in vielen Fällen bereits vorhanden sind, verspricht QKD zusätzliche Vorteile in Bezug auf Sicherheitsprofil, Geschwindigkeit und Flexibilität. Da vertrauenswürdige Knotenpunkte an militärischen Standorten mit weniger Aufwand als in anderen Sektoren realisiert werden könnten, ist die Einführung eines militärspezifischen QKD-Netzwerks für die strategische Kommunikation in mehreren europäischen Ländern potenziell vielversprechend. Dieses wird jedoch nur für die jeweilige Anwendung zugelassene Technologien umfassen.

Versorgungsanbieter: Die Infrastruktur für die Strom-, Gas- und Wasserversorgung ist für Industrie und Gesellschaft lebenswichtig, und QKD könnte zu ihrer Sicherung beitragen. Allerdings machen der geringe Reifegrad, die hohen Kosten und die regulatorischen Rahmenbedingungen eine breite Einführung in diesem Sektor kurzfristig unwahrscheinlich.

Medizinsektor: Dieser Sektor hat einen extrem hohen Bedarf an langfristigem Datenschutz, was Möglichkeiten für den Einsatz von QKD eröffnet. Die begrenzten Ressourcen des Sektors stellen

jedoch einen erheblichen Engpass dar, sodass eine breite Einführung in der nahen Zukunft unwahrscheinlich ist.

Banken und Finanzen: Dieser Sektor hat hohe Anforderungen an die Cybersicherheit und verfügt grundsätzlich über die erforderlichen Mittel. Allerdings ist der Bereich bei der Einführung neuer Technologien zurückhaltend, und das Bewusstsein für Cybersicherheitsrisiken sollte geschärft werden. Demonstrationsprojekte dürften in der nächsten Zeit zu einer langsamen Marktakzeptanz führen, langfristig besteht jedoch ein großes Marktpotenzial. Weniger Vorschriften als im öffentlichen Sektor könnten den Markteintritt beschleunigen.

Industrie: Der Bedarf an sicherer Kommunikation und die langfristige Kritikalität von Daten sind in der Industrie in der Regel geringer als in anderen Sektoren, was das kurz- und mittelfristige Potenzial für QKD begrenzt.

QKD-Dienstleistungssektor: Während Geschäftsmodelle für die Einführung von QKD noch in der Entwicklung sind, könnten Telekommunikationsanbieter, die QKD-gesicherte Dienste anbieten, z. B. QKD-basierte Verschlüsselung, die Einführung beschleunigen und die Anfangsinvestitionskosten senken. Beispiele für erste Anwendungsfälle sind die Sicherung der Kommunikation zwischen Rechenzentren.

Über QKD-Anwendungen hinaus

Die Quantenkommunikation umfasst viele Technologien und (potenzielle) Anwendungen, die über QKD hinausgehen („Beyond QKD"). Obwohl die meisten dieser Technologien und Konzepte derzeit noch einen geringen Reifegrad aufweisen, könnten sie langfristig an Bedeutung gewinnen. Zu den kryptografischen Anwendungen, die über QKD hinausgehen, gehören die Verteilung von Quantengeheimnissen über mehrere Parteien, blindes Quantencomputing, Quantentoken, Quantengeld und der Quantenmünzwurf. Weitere potenzielle zukünftige Anwendungen sind verteiltes Quantencomputing und verteilte Quantensensorik, die jeweils erhebliche Leistungssteigerungen bieten könnten. Viele dieser „Beyond QKD"-Technologien sind zwar vielversprechend, stehen aber derzeit vor großen Herausforderungen, wie z. B. der Realisierung der Verschränkungsverteilung über große Entfernungen. Sie sind daher kurz- bis mittelfristig nicht zu erwarten und erfordern erhebliche FuE-Anstrengungen.

Infrastruktur- und Netzaspekte

Für eine großflächige Einführung von QKD ist eine Netzintegration erforderlich, die weit über Punkt-zu-Punkt-Verbindungen hinausgeht. Folgende Infrastruktur- und Netzaspekte müssen berücksichtigt werden:

Verfügbarkeit von Glasfasern: Derzeit erfordert die glasfaserbasierte QKD nicht parallel zu Telekommunikationszwecken genutzte Glasfaser-Verbindungen (Dark Fiber). In einigen Fällen könnten vorhandene Dark Fibers verwendet werden, allerdings müssten diese von klassischen Verstärkern isoliert werden. Eine strategische Erweiterung der Glasfasernetze um quantentaugliche Dark Fibers, die auch nicht-städtische Gebiete einbezieht, ist sehr wünschenswert.

Multiplexing: Wellenlängenmultiplexing (WDM) verbessert die Glasfasernutzung, indem dieselbe Glasfaser für verschiedene Signale verwendet wird. Weitere Entwicklungen sind nötig, um Quantensignale effizient neben klassischen Signalen in der gleichen Faser zu übertragen.

Verstärkung: Die Dämpfung in Glasfasern begrenzt die Reichweite von Photonen, und klassische Verstärker können für Quantensignale nicht verwendet werden. Vertrauenswürdige Knoten (trusted nodes) sind derzeit die einzige Möglichkeit, die Reichweitenbeschränkung für Quantensignale zu überwinden, während zukünftige Lösungen wie Quantenrepeater und „Heralded-Aplifier" noch in der Forschung sind.

Optisches Routing: Als Teil der Entwicklung hin zu größeren Quantennetzwerken wird das optische Routing von Quantensignalen immer wichtiger, um die Glasfaserressourcen effizient zu nutzen. Bauteile, die diese Aufgabe effektiv erfüllen können, sind jedoch noch in der Entwicklung.

Orchestrierung und Netzwerkmanagement: Die Koordination eines Quantenkommunikationsnetzwerks erfordert ausgefeilte Orchestrierungs- und Netzwerkmanagementtechniken, die sowohl quanten- als auch klassische Ressourcen einbeziehen, die Schlüsselverwaltung automatisieren und die Sicherheit durch Echtzeitüberwachung und adaptives Routing verbessern.

Authentifizierung: Quantenkommunikationsnetzwerke brauchen starke Mechanismen für Authentifizierung, Dienstzugangskontrolle und Rechnungswesen (ASA), um Identitäten zu überprüfen, Berechtigungen zu verwalten und die Nutzung zu verfolgen. Authentifizierung ist auf verschiedenen Ebenen wichtig: erstens bei jedem QKD-Protokollablauf, zweitens für administrative Aufgaben und drittens für die Zugangskontrolle zu Diensten. Post-Quantum-Kryptografie (PQC) könnte in den meisten Fällen eine gute Option für die erste Authentifizierung sein.

Knotensicherheit: An Quantenkommunikationsknoten sind Sicherheitsmaßnahmen wie physische Zugangskontrollen erforderlich, um die Sicherheit zu gewährleisten. Darüber hinaus müssen die QKD-Systeme vor Seitenkanalangriffen geschützt werden.

Standardisierung, Zertifizierung und Zulassung

Die Standardisierung spielt eine wichtige Rolle bei der Gewährleistung von Konsistenz, Interoperabilität, Qualität und Sicherheit von Produkten, Dienstleistungen und Systemen. Standards und Spezifikationen basieren auf einem Konsens zwischen Branchenexperten, Interessengruppen und Regierungsbehörden und sollen die Kompatibilität erleichtern, die Effizienz steigern, Kosten senken und Innovationen fördern, während gleichzeitig die Bedürfnisse aller Beteiligten berücksichtigt werden. Mögliche Bereiche für die Normung in der Quantenkommunikation sind Terminologie, Messungen und deren Rückverfolgbarkeit, Prüfungen, Schnittstellen und Kompatibilität. Konkret besteht beispielsweise Standardisierungsbedarf bei sicheren QKD-Protokollen, Definitionen und Anforderungen für vertrauenswürdige Knoten und Standards für die Hardware-Authentifizierung.

Die Zertifizierung und Zulassung von Quantenkommunikationstechnologien, insbesondere von QKD, ist unerlässlich, um Vertrauen und Zuverlässigkeit zu gewährleisten und den Einsatz im öffentlichen Sektor zu ermöglichen. Die Zertifizierungs- und Zulassungsverfahren folgen klaren Protokollen, um sicherzustellen, dass die erforderlichen Anforderungen erfüllt sind. Obwohl eine erste Reihe von Anforderungen für die Common-Criteria-Zertifizierung von Prepare-and-Measure-QKD-Systemen in Form eines Schutzprofils entwickelt und vom BSI zertifiziert wurde, ist bisher noch kein QKD-Gerät in Europa zertifiziert oder zugelassen worden. Experten gehen davon aus, dass es noch einige Jahre dauern wird, bis die Technologie ausgereift ist und alle notwendigen Standards entwickelt sind, damit eine Zertifizierung erfolgen kann.

Perspektiven bis zur Einführung

Im Jahr 2025 steht eine breitere Einführung von QKD noch vor verschiedenen Herausforderungen. Zu den wichtigsten zählen die begrenzte technische Reife, hohe Kosten (für QKD-Systeme und Infrastruktur), fehlende Standards und zertifizierte/zugelassene QKD-Systeme, geringe Bekanntheit bei potenziellen Nutzern, unklare Geschäftsmodelle, die Sicherheit der Lieferkette und der Bedarf an qualifizierten Arbeitskräften. Die Bewältigung all dieser Herausforderungen wird für eine breitere Einführung der QKD-Technologie von entscheidender Bedeutung sein.

Um den Entwicklungsstand der QKD-Technologie mit Anwendungsfällen zu verknüpfen, wurden beispielhafte Entwicklungsstände definiert, die von der heutigen Situation (Entwicklungsstand 1) über ein technologisch ausgereifteres und zertifiziertes Stadium (Entwicklungsstand 2) bis hin zu

einer hochentwickelten, miniaturisierten und deutlich kostengünstigeren Technologie (Entwicklungsstand 3) reichen. Viele potenzielle Anwendungsfälle werden erst zwischen den Entwicklungsständen 2 und 3 eine breitere Einführung der QKD-Technologie erfahren, wenn die Technologie ausgereifter, zertifiziert/zugelassen und kostengünstiger ist. Einige Anwendungsfälle von QKD, darunter die sichere Kommunikation von Daten zwischen Rechenzentren oder sichere Transaktionen innerhalb und zwischen Banken, könnten bereits in den kommenden Jahren langsam eingeführt werden. Der öffentliche Sektor, einschließlich der öffentlichen Verwaltung, des Verteidigungssektors und des Militärs, wird aufgrund des Bedarfs an sehr hoher und langfristiger Datensicherheit wahrscheinlich eine wichtige Rolle bei der Einführung von QKD spielen, jedoch nicht vor Entwicklungsstand 2, wenn QKD-Geräte zertifiziert/zugelassen sind.

Schlussfolgerungen

Die Quantenkommunikation ist ein strategisch wichtiges Technologiefeld für Europa. Sie hat das Potenzial, ein hohes Maß an langfristiger Sicherheit zu gewährleisten, selbst wenn Quantencomputer in der Lage sind, klassische Verschlüsselungsmethoden zu knacken. Obwohl verschiedene Herausforderungen bestehen, sollten die Politik und die gesamte Gemeinschaft auf die Schaffung eines dynamischen Ökosystems für die Quantenkommunikation hinarbeiten, das in der Lage ist, die technologische Souveränität Europas im Bereich der Quantenkommunikation zu gewährleisten. In mehreren Sektoren wird eine Hybridisierung mit PQC als wahrscheinlich angesehen, um die immer strengeren Sicherheitsstandards zu erfüllen.

Executive Summary

Context

The increasing need for IT security and potential threats posed by quantum computers for classical encryption have led to a growing interest in quantum-safe cryptography. When implemented correctly, quantum key distribution (QKD) promises a quantum-safe option for cryptography that can be used to communicate highly confidential information in a secure way. It therefore has great potential for sectors dealing with critical and secret information, such as the government, the military, and the medical sector. This report discusses application perspectives for QKD in various sectors, including network aspects, standardization and certification, which heavily influence QKD adoption. Further applications of quantum communication that go beyond QKD are also discussed.

Secure communication – status quo and framework conditions.

Secure communication is becoming increasingly important, and regulatory framework conditions are trying to enforce minimum standards for cybersecurity. Key regulations in the EU include the NIS directive (a directive on the security of network and information systems), the NIS2 directive (a directive on measures to establish a high level of cybersecurity across the European Union) and the Critical Entities Resilience (CER) directive (a directive to strengthen the resilience of critical facilities to physical threats such as natural disasters, terrorism or sabotage). However, the requirements differ for different sectors, which is why it is important to understand the framework conditions for each sector when implementing QKD as a cybersecurity solution.

The current cybersecurity solution is based on encryption using key-based procedures, which can be divided into symmetric and asymmetric procedures. While symmetric keys are considered to be more secure, safe key exchange is complicated. Therefore, asymmetric keys are currently widely used. These rely on mathematical problems that cannot be easily solved with classical computers. However, with the emergence of quantum computers, asymmetric keys are likely to become unsafe in the medium term. Therefore, a transition to so-called quantum-safe cryptography using post-quantum cryptography (PQC) algorithms and potentially QKD is crucial.

General challenges facing QKD technology

Although QKD is a promising option for quantum-safe cryptography, it still faces various challenges that are hindering its broader adoption. These challenges include:

Distance limitations: Fiber-based QKD is currently limited to distances of approximately 100 kilometers, possibly a bit farther but at the cost of significantly decreasing key rates. For long-distance communication, trusted nodes or quantum repeaters are required. While trusted nodes represent an additional security vulnerability, quantum repeaters are not yet commercially available and not expected to be so before 2035. Satellite-based QKD, which can achieve longer ranges, is less mature, more expensive and comes with additional challenges.

Stability, robustness and key rates: Many QKD systems are not yet sufficiently stable and robust and require additional technical improvements and optimizations for broad implementation. Although sufficient for many applications, the key rates are still limited.

Side-channel attacks: Although QKD promises a physically secure key exchange, external attacks are still possible. Removing these so-called side-channel vulnerabilities is vital for secure communication via QKD.

Integration, infrastructure needs, and costs: QKD has to be integrated into existing IT security infrastructure, which creates challenges with respect to interoperability, for example. Currently, QKD

relies on dark fibers, which leads to high infrastructure costs for implementing QKD. The QKD devices themselves are still quite expensive as well.

Standardization, certification and approval: In addition to the above challenges, the lack of standardized, certified and approved QKD systems/protocols is hindering the adoption of QKD in sectors that rely on certified or approved IT security products.

Awareness and acceptance: In many sectors, there is only a limited awareness of the quantum threat and possible quantum-secure solutions. On the other hand, reluctance to change currently running systems is high.

Supply chain risks: The supply chain for QKD should be diversified to limit geo-strategic dependencies and move toward technological sovereignty in quantum communication.

Sector-specific application scenarios

Public administration: Governments are seen as key potential customers for QKD based on their need for very high data security. Transitioning to quantum-safe cryptography is also urgent due to the need for long-term security. However, European countries are currently cautious about adopting QKD because of its lack of maturity and certified and approved QKD systems. Consequently, this sector has medium to high market potential for QKD, but significant implementation is unlikely before 2030.

Military and defense: The data security requirements of the military and defense sector are as high as in the public administration and long-term protection of the communicated information is also needed. As symmetric key distribution processes (e.g., via a courier) are already in place in many cases, QKD promises complementary benefits in terms of security profile, speed and flexibility. As trusted nodes could be realized within military facilities with less effort than in other sectors, the implementation of a military-specific QKD network for strategic communication is potentially promising in several European countries. However, this will only involve technologies approved for the corresponding application.

Utility provider: The infrastructure supplying electricity, gas and water is vital for industry and society and QKD could help to safeguard it. However, the QKD's low maturity, high costs and regulatory framework conditions make significant adoption in this sector unlikely in the short term.

Medical sector: This sector has an extremely high demand for long-term data privacy, which opens opportunities for the use of QKD. However, the sector's limited resources represent a very significant bottleneck, so that widespread adoption is unlikely in the short term.

Banking and finance: This sector has high cybersecurity requirements and the necessary funds, in principle. However, the sector is cautious when implementing new technologies and its awareness of cybersecurity threats needs to be heightened. Demonstration projects are likely to lead to slow market adoption in the short term, with large market potential in the long term. Fewer regulations compared to the public sector could speed up market entry.

Industry: The need for secure communication and the long-term criticality of data are typically lower in industry than in the other sectors, limiting the short- and medium-term potential for QKD.

QKD service sector: While business models for the adoption of QKD are still under development, telecom providers offering QKD-secured services, e.g., QKD-based encryption, could speed up adoption and reduce initial investment costs. Examples of first use cases include securing the communication between data centers.

Beyond QKD applications

Quantum communication encompasses many technologies and (potential) applications "beyond QKD". Although most of these technologies and concepts are currently at a low maturity level, they have the potential to become important in the longer term. Cryptographic applications beyond QKD include quantum secret sharing, blind quantum computing, quantum tokens, quantum money, and quantum coin flipping. Other potential future applications include distributed quantum computing and distributed quantum sensing, each of which could offer significant performance enhancements. While many of these "beyond QKD" technologies are promising, they currently face major challenges, such as realizing entanglement distribution over long distances. They are therefore not to be expected in the short or medium term and will require significant R&D efforts.

Infrastructure and Network Aspects

For larger-scale adoption of QKD, network integration is required that goes far beyond point-to-point links. The following infrastructure and network aspects need to be considered:

Fiber availability: Currently, fiber-based QKD requires dark fibers. Existing dark fibers could be used in some cases, although this requires efforts to isolate these fibers from classical amplifiers. A strategic extension of fiber networks with quantum-ready dark fibers to include non-urban areas as well is highly desirable.

Multiplexing: Wavelength-Division Multiplexing (WDM) enhances fiber utilization by using the same fiber for different signals. Further developments are needed to efficiently co-propagate quantum signals with classical signals.

Amplification: Attenuation in glass fibers limits the distance of photons, and classical amplifiers cannot be used for quantum signals. Trusted nodes represent the only currently available option to overcome the distance limitation for quantum signals, while future solutions such as quantum repeaters and heralded amplifiers are still in the research stage.

Optical routing: As part of the progress toward larger quantum networks, the optical routing of quantum signals will become increasingly important to ensure efficient use of the fiber resources. However, components able to carry out this task effectively are still under development.

Orchestration and network management: Coordinating a quantum communication network calls for sophisticated orchestration and network management techniques that incorporate both quantum and classical resources, automating key management and enhancing security through real-time monitoring and adaptive routing.

Authentication: Quantum communication networks require solid authentication, service access control, and accounting (ASA) mechanisms to verify identities, manage permissions, and track usage. Authentication is crucial at different levels: firstly, during each QKD protocol run; secondly, for administrative tasks; and thirdly, for service access control. Post-Quantum-Cryptography (PQC) could be a plausible option for initial authentication in most cases.

Node security: Security measures, such as physical access control, are necessary at quantum communication nodes to ensure security. Additionally, the QKD systems need to be impervious to side-channel attacks.

Standardization, certification and approval

Standardization plays an important role in ensuring consistency, interoperability, quality, and safety across products, services, and systems. Standards and specifications are based on consensus among industry experts, stakeholders, and governing bodies and aim to facilitate compatibility, enhance efficiency, reduce costs, and promote innovation while meeting the needs of all relevant parties.

Potential areas for standardization in quantum communication include terminology, measurements and their traceability, testing, interfaces, and compatibility. More specifically, a need for standardization is seen, for example, in secure QKD protocols, definitions and requirements for trusted nodes and hardware authentication standards.

Certification and approval of quantum communication technologies and especially QKD are essential to ensure trust and reliability and enable them to be used in the public sector. The certification and approval processes follow clear protocols to ensure that the necessary requirements are fulfilled. Although a first set of requirements for certifying prepare-and-measure QKD systems in the form of a common criteria protection profile has been developed by ETSI and certified by the BSI, no QKD device has been certified or approved in Europe to date. Experts expect that it will still take a few years until sufficient technological maturity has been achieved and all necessary standards have been developed so that certification can be realized.

Perspectives towards adoption

In 2025, broader QKD adoption is still facing various challenges. The most relevant include limited technical maturity, high costs (for QKD systems and infrastructure), a lack of standards and certified/approved QKD systems, low awareness on the part of potential users, unclear business models, supply chain security and the need for skilled workers. Addressing all of these challenges will be key for broader adoption of QKD technology.

To correlate the development stage of QKD technology with use cases, we defined exemplary development statuses that range from the situation today (development stage 1), a technologically more mature and certified stage (development stage 2) to a highly developed, miniaturized and significantly less expensive technology (development stage 3). Many potential use cases will only experience broader adoption of QKD technology between development stage 2 and 3, when the technology is more mature, certified and less expensive. Several use cases of QKD, including the secure communication of data between data centers, or secure intra- and inter-bank transfers could already start to be slowly adopted in the coming years. The public sector, including public administration, defense and the military, is likely to play a major role in QKD adoption due to the need for very high and long-term data security, but not before development stage 2 when QKD devices are certified/approved.

Conclusions

Quantum communication represents a strategically important field of technology for Europe. It has the potential to ensure a high level of long-term security, even when quantum computers are in a position to break classical encryption methods. Although various challenges exist, policymakers and the whole community should work toward establishing a vibrant quantum communication ecosystem capable of achieving technology sovereignty in quantum communication in Europe. Hybridization with PQC is considered likely in several sectors to meet the increasingly stringent security standards.

1 Introduction

Quantum communication (QCom) refers to quantum technologies dealing with the transmission, distribution and communication of quantum states as well as the resulting technologies and applications. QCom is based on quantum mechanical principles, such as entanglement or the superposition of quantum states such as photons, to enhance security or functionality. One of the currently most mature QCom technologies is quantum key distribution (QKD), which can enable highly secure communication by exchanging quantum-safe keys.

In recent years, we have witnessed an increasing focus on secure communication in industry and society, as digitalization progresses, and cybersecurity threats grow. The developments in quantum computing present a particularly relevant threat. As the capabilities of quantum computers continue to improve, we are rapidly approaching "Q-day", i.e., the day when quantum computers will be powerful enough to decrypt classical encryption methods based on Shor's algorithm, for example. Although no-one knows when quantum computers will be ready to do so, experts assume that this is likely to happen before 2040. [1] Therefore, a transition is necessary to cryptographic methods that cannot be easily decrypted by classical or quantum computers. Quantum-safe cryptography can be implemented using new algorithms summarized as Post-Quantum Cryptography (PQC). While first PQC algorithms have already been standardized by NIST [2] and could be quickly adopted, the long-term security of PQC is based on mathematical assumptions. Quantum key distribution (QKD) is one quantum-safe cryptography option and its hybridization, i.e. QKD with PQC greatly increases long-term security. The implementation of QKD, however, requires additional equipment and infrastructure and is currently expensive. For this and other reasons, there is currently no mass market for QKD. This study tries to assess the perspectives for a more widespread adoption of QKD and other QCom applications. To do so, it analyzes various application sectors for QKD, including their needs, requirements, and framework conditions. The sectors analyzed comprise the public administration, the military and defense sector, utility provider, the medical sector, banking and finance, industry and the QKD service sector. Network aspects, standardization, certification and general challenges facing QKD technology are also discussed, as these have a significant impact on QKD adoption. The report also discusses applications beyond QKD, albeit in less detail due to their generally lower level of maturity.

2 Methods

Desk Research

Desk research was conducted to gain a fundamental understanding of the landscape surrounding IT security legislation and requirements for critical infrastructures. Sources of IT security legislation, company requirements and announcements by the BSI and the European Commission were analyzed. The pertinent literature, research articles, and industry white papers were also used as sources to identify relevant use cases and their specific requirements, which are cited accordingly. The desk research served as a basis for the subsequent methodological components, enhancing the understanding of QKD technology and its implications across various sectors.

Interviews

We conducted more than 35 interviews with stakeholders across various sectors, including finance (banks and insurance companies), telecommunications and data centers, energy infrastructure (electricity and gas), manufacturing, healthcare, government, public administration, military and defense. Each interviewee offered unique insights specific to their sector, focusing on topics such as network applications, quantum-safe financial solutions, and critical infrastructure requirements. The interviews provided information about the potential of QKD technology across the different sectors and highlighted the varying degrees of security required and the urgency for adoption. Experts identified challenges such as high initial infrastructure costs, regulatory hurdles, and the importance of executive-level awareness as critical factors influencing the implementation and adoption of QKD across applications and sectors.

Workshop

We also conducted an expert workshop to validate the initial findings and enhance the understanding of QKD applications through further in-depth analyses. The workshop participants explored specific use cases, identified challenges to implementation, and collaboratively developed a roadmap for the future of quantum communication technologies. They comprised a diverse mix of stakeholders from various sectors. This diversity enriched the discussions and ensured that a broad spectrum of perspectives on the utilization of QKD and quantum communication was represented.

The workshop focused on assessing QKD applications across various sectors, for which participants identified use cases and challenges related to the adoption of QKD technologies. Strategies for overcoming these challenges were developed, resulting in a roadmap that outlines the actions required to advance quantum communication applications.

3 Quantum Communication Technologies

Quantum communication represents a revolutionary approach to secure information exchange, leveraging the principles of quantum mechanics to achieve levels of security that are unattainable with classical methods. One of the most significant advancements in this field is Quantum Key Distribution (QKD), which aims to enable two parties to share a secret key in a manner that is highly secure against eavesdropping. Theoretical frameworks such as BB84 [3] and BBM92 [4] have laid the groundwork for various QKD protocols, each with its own unique advantages and challenges.

QKD technologies

QKD can be implemented using different encoding methods that are primarily categorized into prepare-and-measure and entanglement-based approaches. Prepare-and-measure QKD has two prominent encoding schemes:

1) Discrete variable (DV) protocols typically use single photons to encode information, utilizing discrete properties like polarization or time-phase. More sophisticated strategies have emerged beyond basic two-dimensional encoding to higher-dimensional schemes for denser information transfer.
2) In contrast, continuous variable (CV) QKD encodes information in continuous states of light, such as amplitude and phase. The uncertainty principle imposes limitations on measuring both properties with high precision simultaneously, presenting unique properties for protocol design.

In entanglement-based QKD, photons are created that are entangled in one or more properties, e.g., polarization or time-energy. Notably, entanglement-based QKD allows source-independent arrangements, where the properties of entangled photon pairs are determined only upon measurement, enabling multi-user connections with a single source in the center and a star-like configuration. As the source does not reveal any information, and any manipulation will be revealed upon detection at the receiver's side, this means the source can be placed in an unsecured environment.

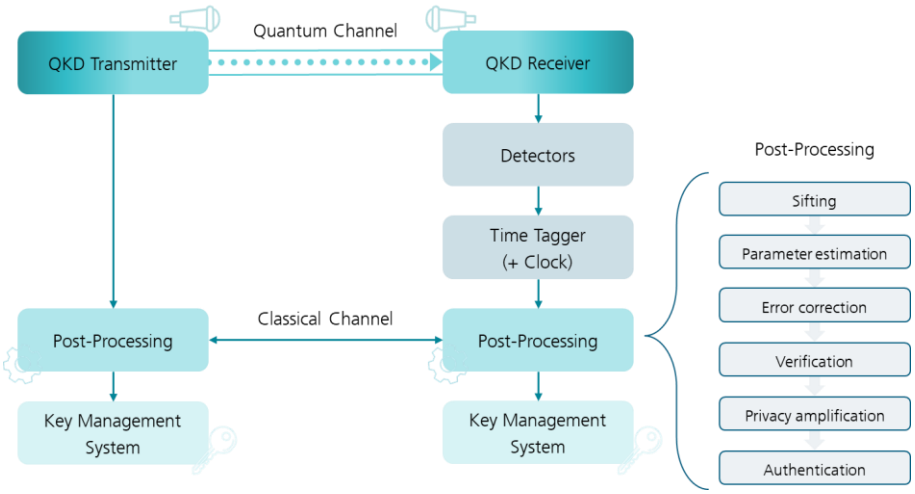
Measurement-Device-Independent (MDI) QKD turns this scheme around and uses two sources and a central detection point. This advanced method based on the interaction between signals from different sources enables secure communication by employing a central node that measures signals without revealing the original states of the senders. This eliminates side-channel attacks on the receiver side. For example, in polarization encoding, the two incoming signals interfere in a Hong–Ou–Mandel manner at a beam splitter and afterwards polarizing beam splitter separate the photons into horizontal and vertical polarization. Publishing the measurement results does not reveal any information, while the senders can extract the original states since they know their prepared states.

Longer transmission distances can be achieved with Twinfield (TF) QKD, which can be seen as a variant of MDI QKD. Unlike other schemes, TF-QKD relies on first-order interference at a central node. This provides beneficial scaling of transmission rate with loss, effectively doubling the transmission distance. Encoding can be done via prepare-and-measure, e.g., by phase encoding single photons. However, stabilizing long-distance interferometric links and maintaining phase locking between remote individual laser systems remains a significant technical challenge.

A QKD system comprises several different components. Figure 1 illustrates the abstract components for a single link with a prepare-and-measure configuration. The QKD sender module prepares random quantum states and the QKD receiver module analyzes them. Additional hardware and software are required, as well as the necessary infrastructure for transmission (QKD link). For transmis-

sion, an optical channel is needed for quantum information as well as a separate channel for classical data. Both channels can be implemented using the same transmission medium. The exchanged qubit information is post-processed, and the secret keys received are stored in Key Management Systems (KMS). Applications can then retrieve the keys from the KMS through a suitable interface. Not depicted in this sketch is the network organization, which requires an additional controller and orchestrator for one domain.

Figure 1: Abstract sketch of a QKD system for a single transmitter and receiver used in prepare-and-measure protocols with an overview of the most important post-processing steps.



Challenges for QKD deployment

Generally, the maturity of commercially available QKD systems has increased strongly over the last few years, especially for prepare-and-measure schemes. Nevertheless, several technological challenges remain, system security must be considered, and technological sovereignty is becoming more and more important.

The hardware and software systems supporting QKD are diverse and complex, and each face their own challenges. Security constraints arise from the fact that implementing a certain protocol includes imperfections that may open the door to a potential eavesdropper. Therefore, protocols and systems are further developed, for instance, by adding decoy states to the BB84 implementation or adding isolators to the transceiver for prepare-and-measure QKD systems. Additional spectral filtering and power monitoring at the receiver side are intended to decrease the likelihood of eavesdropping. Finally, deploying QKD for classified data requires system hardening and certification.

In general, it is crucial for the stability of the QKD system that it can be operated under typical server room ambient conditions or even in the field without changing its performance, in particular, not opening side channels, e.g., due to temperature changes. Single photon detectors, such as superconducting nanowire single-photon detectors, used in DV and entanglement-based QKD provide high performance but require cryogenic cooling. In contrast, near-infrared single-photon avalanche detectors required for fiber-based systems come with fewer restrictions but also perform worse in terms of high dead times and dark counts. New developments, including up-conversion schemes, aim to enhance detection efficiency and reduce environmental constraints. On the other hand, CV-QKD necessitates highly stable lasers and precise detection methods, such as homodyne or heterodyne detection.

Besides the technical challenges, the standardization and certification of QKD systems is still pending and remains an open task for the community, metrology institutes, and national security agencies (see section 6).

Network integration

Integration into existing terrestrial communication networks presents both opportunities and challenges. Quantum communication can utilize dark fibers alongside classical channels, although the combination of both in a single fiber remains limited. Dark fibers are unused optical fibers that can be repurposed for quantum communication, providing a dedicated pathway for quantum signals without interference from classical data traffic. This is advantageous for maintaining the fidelity of the quantum states being transmitted, as quantum communication is particularly sensitive to noise and disturbances.

The challenge lies in the attenuation of quantum signals over long distances, which can lead to significant loss of information. To mitigate this, quantum repeaters are being developed to extend the range of QKD systems by enabling the entanglement swapping of quantum states over longer distances. Until quantum repeaters are available, trusted nodes are required to expand the distances in a network. In a trusted node, the quantum signal is detected and stored in a classical way, requiring a trusted site. A new connection is then established to the next node. The quantum key can then be forwarded in such a network via direct forward encryption, for example.

Free-space optical communication involves the transmission of quantum signals through the air or space using direct line-of-sight paths. This method is particularly useful for areas where laying optical fibers is impractical, such as across geographical barriers. Free-space links can also be directly connected to fiber networks by low-loss in- and out coupling from the fiber to the free-space part, resulting in hybrid links.

Satellite technology is crucial for long-distance quantum communication, as this enables QKD over vast distances that exceed the limitations of terrestrial networks and can achieve global coverage. Specialized optical ground stations are required to receive or transmit the quantum signals due to the high losses. However, atmospheric conditions such as rain, fog, or turbulence can affect the reliability and quality of the transmitted quantum states.

While the integration of QKD systems into terrestrial networks is already taking place, the harsh conditions during launch and in space remain a challenge for a space-based quantum communication infrastructure. Additionally, optical ground stations are expensive and have special building requirements due to weight and stability. For a more comprehensive overview, section 5.1 describes the infrastructure requirements and networks for QKD.

Beyond QKD technologies and outlook

While the above-described technologies focus on QKD, most of the quantum technologies for applications beyond QKD are similar. For future applications such as distributed quantum computing, quantum repeaters are crucial to enable entanglement distribution from endpoint to endpoint. Entanglement-based networks are also referred to as the Quantum Internet, where entanglement is a resource that can be used for many different applications (including QKD with end-to-end security) (see section 4.3).

As quantum communication technology continues to evolve, establishing standards, e.g., for interfaces, will be essential to enhance interoperability among systems. The future holds promise not only for QKD but also for broader quantum networks and applications that go beyond secure key distribution.

4 Application Scenarios and Sectors

4.1 Secure Communication – Status Quo and Regulatory Framework Conditions

The use of quantum communication offers key distribution schemes that promise higher levels of protocol security compared to classical cryptography, as it is based on provable physical principles with minimal assumptions on the eavesdropper's capabilities instead of mathematical hard problems. If this promise can be realized in practical implementations, companies and organizations with high IT security requirements in particular could benefit. In order to determine the general application possibilities of quantum communication, it is necessary to know the current IT security requirements and IT security approaches in the various sectors. Companies and organizations in the different sectors have different IT security issues and challenges. In the financial sector, for example, the focus is on protecting against cyber-attacks, in the energy sector it is on preventing sabotage, and in production it is on securing international supply chains and preventing data espionage. However, the technologies and methods used to achieve cyber security in the various sectors are very similar. They range from the systematic risk identification and the use of firewalls and encryption technologies to robustness tests and the implementation of company-wide information security management systems (ISMS) in accordance with ISO/IEC 27001 [5] or the BSI "IT-Grundschutz" which is a concept developed by the Federal Office for Information Security (BSI) in Germany that includes various modules, guidelines, and standards based on best practices. [6]

Depending on the sector, different legal requirements and standards must be observed and different practices for the implementation of IT security measures have become established. The legislative basis for the cybersecurity activities of companies and organizations in Germany are the German and European IT security legislations, which are most relevant for critical infrastructures (KRITIS). There are also sector-specific regulations, such as DORA for the financial sector, which are important as well.

In the following, the focus is on information regarding the technological aspects and purely organizational precautions (such as the rules for reporting incidents, monitoring and forensics) are dealt with to a lesser extent.

4.1.1 The Regulatory Context

IT security has been regulated by law in Germany since the BSI Act of 1990 (last amended in 2009). Following the first serious IT security incidents, the German government established voluntary cooperation with the operators of so-called 'critical infrastructures' (KRITIS)[1] in 2007. As the threat situation became more serious, it was recognized that a binding regulatory framework was necessary. Attempts to harmonize such measures were launched at EU level in order to "achieve a high common level of security of network and information systems within the EU". The result of these endeavors was the European *NIS Directive* (Directive on security of network and information systems), which was implemented in Germany with the IT Security Act (IT-SiG 1.0), [7] the NIS Directive Implementation Act and the KRITIS Ordinance (BSI-KritisV). [8]

IT-SiG 1.0 and BSI-KritisV provided extensive definitions of relevant critical services for various sectors and their industries. Regulated sectors included energy supply, information technology and telecommunications, transport and traffic, health, water, food, finance and insurance (§§ 2-9 BSI-

[1] According to the BSI "*Critical infrastructures (*KRITIS*) are organizations and facilities of major importance for society whose failure or impairment would cause a sustained shortage of supplies, significant disruptions to public order, safety and security or other dramatic consequences.*" https://www.bsi.bund.de/dok/kritis-allgemein

KritisV). Threshold values were used to define which organizations were considered critical for public supply and therefore had to meet certain requirements. As a guideline, organizations were considered 'critical' if they served 500,000 citizens or more, i.e., predominantly large institutions (BSI-KritisV, Appendix 1, Part 2). They had to fulfil a number of security requirements and reporting obligations. They were expected to implement appropriate state-of-the-art measures to secure data processing and communication to prevent or minimize the likelihood and impact of security incidents (§1 (7) IT-SiG1.0). However, violations could only result in moderate fines (§1 (9) IT-SiG 1.0). [9]

An expansion of those affected by IT security regulation took place with the adoption of the European *General Data Protection Regulation* (GDPR) in 2016, which stipulates in article 32 that state-of-the-art measures shall be implemented to ensure a level of security appropriate to the risk when processing personal data. [10] These regulations are not limited to organizations of a certain size or to certain types of processing but to everyone processing personal data.

However, it soon became apparent that the NIS Directive was not sufficient in view of the dynamic technological development and the further increase of the security threats (keywords: war of Russia against Ukraine and disinformation campaigns). For this reason, the IT Security Act 2.0 (IT-SiG2.0) [11] was adopted in Germany in 2021 and the *NIS2 Directive* (Directive on measures for a high common level of cybersecurity across the Union) [12] at European level at the end of 2022. These primarily entailed a significant expansion of the scope of application, but also stricter enforcement mechanisms. After IT-SiG2.0 had already declared the waste sector and companies in the special public interest (UBI) to be critical infrastructures, the NIS 2 extended the regulations to cover even more organizations and sectors.

The implementation of the NIS2 Directive, which has been applicable since 18 October 2024, is planned by the NIS2UmsuCG. [13] Its adoption, however, has been delayed due to the previous government coalition collapsing but is now expected during the course of 2025. [14]

The NIS2 directive is supplemented by the *Critical Entities Resilience (CER) directive*, [15] which aims to strengthen the resilience of critical facilities toward physical threats such as natural disasters, terrorist threats or sabotage. It applies to operators of critical facilities in eleven sectors, some of which are the same as those in the NIS2 Directive. [16] In Germany the CER directive is implemented under the KRITIS framework law (KRITIS Dachgesetz). [17]

With the incorporation of NIS2 and CER into national law, IT security will be regulated in a large number of sectors, especially in "sectors of high criticality" (Annex I, NIS2) including energy, transport, banking, financial market infrastructures, healthcare, drinking water, wastewater, digital infrastructure, business-to-business (ICT) services management, public administration, space and "other critical sectors" (Annex II, NIS2), including postal and courier services, waste management, production, manufacture and trade of chemical substances, production, processing and distribution of food, manufacturing/production of goods, digital service provider and research amongst others. Initial estimates assume that the number of affected organizations and companies will increase from 12,000 to 30,000. [18]

After the incorporation of the NIS2 Directive into German law in the course of 2025, companies and organizations in these sectors will have to comply with its (higher) requirements. These include, among others:

- Risk analysis concepts, measures to maintain operations, backup management and concepts for the use of encryption,
- a three-stage reporting system for cyber security incidents,
- fines for breaches of IT security requirements, based on a company's global annual turnover, and

- appointment of a Chief Information Security Officer for the federal government and statutory anchoring of essential requirements for information security management. [19]

While NIS2 and CER regulate providers of infrastructures and services, the *Cyber Resilience Act* (CRA), [20] which came into force on 10 December 2024, is aimed at manufacturers of any products with digital elements, i.e. hardware or software that are directly or indirectly connected to a network. [21]

4.1.2 The Classical Approach to Cryptography[2]

The mission of information security is defined by three so-called protection goals: [24, 25] (1) confidentiality means that only authorized persons can access data, (2) integrity means that data is protected against unauthorized changes and deletion, i.e., that its accuracy and completeness is guaranteed, (3) finally, availability means that systems and data must be available to authorized persons at all times, e.g., by preventing system failures.

Protection goals 1 can be achieved in particular by suitable encryption of the data, in which the information is converted in such a way that it can ideally only be decrypted and read again by authorized parties.

Firstly, a distinction is made between *point-to-point encryption* (P2PE) and *end-to-end encryption* (E2EE). P2PE means that data is encrypted during transmission between two devices or nodes in a network so that the data line is tap-proof. However, the data is decrypted again in each device or network node and, if necessary, re-encrypted for further transmission. To prevent messages that are transmitted over several nodes (as is usual on the Internet) from being intercepted in an intermediate node (so called man-in-the middle attack), E2EE encrypts the messages across all transmission stations. Only the communication partners (the end points of the communication) can decrypt the message.

Today, encryption itself is carried out almost exclusively using key-based procedures, which can be divided into symmetric and asymmetric procedures. The key is usually a sequence of characters that are used by a cryptographic algorithm to convert the plaintext of a message into the ciphertext.

Symmetric cryptography uses the same key for both encryption and decryption. Because only *one* key is used in symmetric cryptography, it is important to keep this key secret to prevent compromise, i.e., the unintentional disclosure of the message. However, keys are changed regularly to limit damage when a past key is compromised. This leads to the key exchange problem, which arises because the communicating parties must exchange the key before a secure, encrypted communication channel is established. They must therefore have some other secure mechanism for transferring the keys. On the other hand, symmetric encryption is more efficient and faster than asymmetric encryption (see below).

Today, the Advanced Encryption Standard (AES), a block cipher which was specified by the National Institute of Standards and Technology (NIST) in 2000, is considered state-of the art and is the most commonly used symmetric encryption algorithm. The method is considered secure in the practical sense, i.e., there is no known practically feasible attack that significantly reduces the time for breaking the encryption.

Asymmetric cryptography or public-key cryptography was developed as early as the late 1970s to address the key exchange problem as it uses pairs of keys, a public key used for encryption and a corresponding private key for decryption. These are generated using so-called one-way functions, which are easy to calculate in one direction but practically impossible in the other. Apart from the

[2] For more technicalities of cryptographic algorithms see for instance Paar et al. [22] or Buell [23].

quality or 'hardness' of the one-way function used, the security of asymmetric encryption methods is based only on the secrecy of the private key; the public key can be distributed openly without risking a compromise to the security of the system. The security level of the best asymmetric methods comes close to that of the best symmetric ones, but a sufficiently powerful attacker could solve the underlying mathematical problem. Moreover, asymmetric algorithms tend to be relatively slow compared to symmetric ones.

Examples of widely used methods of asymmetric cryptography are the RSA algorithm (Rivest, Shamir and Adleman)[3], elliptic curves cryptography using discrete logarithms, or Diffie-Hellman (DH) key exchange. RSA is used, for example, in e-mail encryption with Pretty Good Privacy (PGP) or S/MIME, in the IPSec transmission protocol or in electronic banking with a HBCI (Home Banking Computer Interface).

The security of asymmetric cryptosystems is based on the fact that there are still no efficient, practical methods of factoring a number into its prime factor or computing discrete logarithms with conventional computers. However, more than 30 years ago Peter Shor (1994) presented a quantum algorithm that is capable of efficiently solving the factorization and discrete logarithm problem. He showed that given sufficiently advanced quantum hardware it is possible to crack the classical asymmetric cryptographic methods. Leading experts believe that in the 2030s, quantum computers will be able to crack the public key cryptography currently in use. [1, 26]

Fortunately, researchers have found new, hard-to-solve mathematical problems that can be used to develop new cryptosystems. Since neither efficient classical nor quantum algorithms are known to solve these mathematical problems, such systems can better withstand attacks by quantum computers, as things stand today. There are currently a number of approaches to this so-called *Post-Quantum Cryptography* (PQC), none of which are as well researched as conventional methods, but which are so advanced that the National Institute of Science and Technology (NIST) has taken steps to standardize them (Dam u. a. 2023). The methods include lattice-based, hash-based, code-based, isogeny-based and multivariate cryptography, from which NIST has approved two lattice-based and one hash-based algorithm as Federal Information Processing Standards in August 2024 (FIPS 203, 204, 205). [2]

4.2 Application Scenarios for QKD

QKD can be used in various applications and sectors. This section discusses general considerations, opportunities and challenges for QKD adoption and takes a closer look at several sectors that could potentially adopt QKD, along with their sector-specific requirements and framework conditions.

4.2.1 General Considerations for the Use of QKD

This subsection provides general considerations about why QKD should be used, what challenges currently exist, and how sectors can be evaluated for the introduction of QKD.

4.2.1.1 General Challenges facing QKD Technology

In 2025, QKD is still facing several technical and non-technical challenges on its way to becoming more widely adopted. Some challenges are sector-specific and will be discussed in the following sections, others are cross-sectoral and will be discussed in this section.

Technical challenges

- **Distance limitation**: Currently, commercially available fiber-based QKD systems can enable communication over distances of typically 100 km, some up to about 150 km [27] (see also section 5.1.1). The attenuation in the glass fiber limits the range of communication, because the key rate drops exponentially with increasing distance. [28] This applies to various different approaches of QKD including prepare-and-measure QKD, entanglement-based, and MDI-QKD. Although experiments have shown for example that distances of up to 400 km are possible with entanglement-based QKD and MDI-QKD [29, 30], this typically comes at the cost of significantly decreased key rates and requires the use of costly high-end equipment. Using twin-field QKD (see section 3), this distance could be doubled for point-to-point connections. Research has demonstrated distances of up to 1000 km using such setups, [31] although this is at the cost of low key rates, meaning that communication distances of 1000 km are currently not practically feasible. This means that quantum communication over longer distances currently requires the use of trusted nodes (see also section 5.1.3). Trusted nodes are locations in the communication channel, where the quantum signal is converted into a classical signal and a new quantum signal is sent to the next node or the receiver. By converting it into a classical signal, they create an additional attack surface for eavesdroppers. Communication via such trusted nodes is therefore based on the trust in these nodes and their operators. The secure key is then transmitted, for instance, by forward encryption through the chain of trusted nodes to its final destination. In the future, long-distance QKD could be performed based on quantum repeaters or heralded qubit amplifiers (see also section 5.1.3). Using quantum repeaters, the quantum signal can be directly forwarded without the need to convert it into a classical signal, which in turn increases security. Networks based on quantum repeaters could therefore more easily fulfill regulatory requirements. However, they are not yet technologically very mature and commercial solutions are not expected before 2035.
  Another option to increase the communication distance is satellite-based QKD. However, this comes with additional complexity and its own limitations [32] and is currently not feasible for many use cases. We therefore focus on fiber-based QKD in this report.

- **Stability and robustness:** Many of the current QKD systems are the product of recent work from R&D labs. Consequently, their technological maturity is still limited, and manufacturers are still working on improving their stability and robustness, e.g., with regard to external influences such as temperature changes, vibrations, humidity, etc. Further improvements to optimize these devices will most likely solve these issues, however currently this can still be a limiting factor for their adoption.

- **Key rates**: Many factors in QKS systems influence the key rate, including the single photon source, the detector, and the attenuation in the fiber. For all fiber-based QKD systems the attenuation in the fiber limits the distance and for longer distances this is certainly the most limiting factor. For most DV-QKD systems the single-photon detectors are the limiting factors for the key rate, while the light sources are not.
  When using quantum keys for symmetric encryption of data, a gigabyte of data can be encrypted with one 256 bit key. Keys are regularly exchanged, e.g., every few minutes. Depending on the amount of data that is to be encrypted, a greater or lesser number of keys are necessary. For many applications the current key rates of a few kbits/s are sufficient. For larger amounts of data they might need to be increased. In the medium term, it will therefore always be necessary to prioritize which data is to be additionally secured by QKD and which can be sent using other encryption methods.

- **Side-channel attacks**: Although QKD promises a high level of security in theory, in reality, the device imperfection can provide various vulnerabilities to external attacks. [33] Examples include Trojan-horse attacks against QKD transmitters or photon-number-splitting attacks exploiting multi-photon signals in DV-QKD systems. To overcome this issue, QKD manufacturers are trying to close loopholes and entrance points for attackers. Furthermore, advanced protocols are being developed and used:
  - **Entanglement-based QKD** mitigates the vulnerabilities associated with the light source (source-independent).
  - **MDI-QKD and TF-QKD** mitigates the vulnerabilities associated with the measurement device (measurement-device-independent).
  - **DI-QKD** is a concept that aims to guarantee security independent of how the devices are implemented (both on the measurement and emitter side).

- **Cost reduction**: QKD devices are currently produced in low quantities and mostly by companies that still have high R&D expenses. Accordingly, the device prices are currently still rather high with prices often around 200 000 Euros. Currently, the costliest component in DV-QKD systems are often the single-photon detectors. The scaling up of production quantities, triggered by increasing market demand, as well as further technical developments will likely lead to cost and price reductions in the future. Eventually, the miniaturization of QKD devices, i.e. integrating the components on photonic integrated circuits (PIC) could lead to further significant cost reductions.

- **Integration into existing systems and interoperability:** QKD systems are not useful as stand-alone devices, they have to be integrated into existing cryptographic and communication infrastructure. This leads to challenges, as interfaces between different components, (e.g., key management systems, network management systems, encryptors) need to be adjusted and ideally standardized (see also section 6.1). Companies also typically do not want to rely only on one manufacturer or product, as this leads to strong dependencies. However, the interoperability between different QKD devices is typically not guaranteed.

- **Infrastructure:** As of today, QKD requires dark fibers for transmission of the quantum signal. This means that on top of the costly QKD devices, a very expensive separate fiber infrastructure is necessary to operate QKD systems. Therefore, many use cases might rely on service models, in which the user does not own the fiber infrastructure. R&D efforts are in progress to determine how the existing fibers in use can be utilized to co-propagate the quantum signal. However, this is not possible, for the time being.

Non-technical challenges

- **Standardization and certification:** With increasing technological progress in an emerging field, standardization becomes more and more important. It allows for fair comparison of technologies and performance indicators and potentially also for interoperability between technologies. Although various standardization efforts are underway in quantum technologies and quantum communication (see section 6.1), many standards are still lacking.
  Certification relates to specific QKD products and includes a detailed evaluation of the function and security of the system according to the requirements defined in a protection profile. To date, no QKD product in Europe has received a certification and it is expected that this will not be possible for several years to do so, as still various aspects (incl. standards) are still lacking (see section 6.2). Although a certification is not required in all sectors (see Section 5.5.2), it would certainly help to build trust in this technology. For QKD usage in the public sector, the

system would need to be approved by the responsible national (cyber-)security agency. This approval covers similar aspects to certification but also includes aspects such as the supply chain security. Similar to certification, no QKD devices have been approved in Europe yet, and it will be some time before they are (see section 6.2).

- **Awareness and acceptance:** At present, the knowledge and awareness of quantum technologies is still low in the industry. [34] As a result, awareness of the quantum threat, i.e. the possibility of fast decryption of classical encryption algorithms using quantum computers is low. Consequently, awareness of solutions to this threat, such as PQC and QKD, is low as well. While first PQC algorithms have been standardized by NIST [2] and are currently being implemented by many applications, a wider adoption and fast roll-out of QKD is still hindered by limited market interest. One of the challenges is therefore to increase awareness of QKD technologies among potential users. This can be achieved through community outreach activities and demonstration projects including end users. The latter can also lead to increasing market acceptance and growing markets.

- **Different levels of security in different parts of the network:** QKD offers the potential for highly secure communication. However, due to the technical complexity, size and costs of the systems, QKD will not be implemented in all parts of the network. Especially end user devices will not be equipped with QKD systems and therefore not all communication in the network will have the same level of security.

- **Supply chain aspects:** QKD systems contain various components and sub-systems that typically are bought by the QKD system manufacturers. However, some of the necessary components (such as field programmable gate arrays - FPGAs) are only available from certain vendors or countries, which leads potentially to geo-political dependencies. In view of recent political developments in the world, a diversified supply chain without unilateral dependencies is, however, highly desirable and might be even required for approval and subsequent adoption in the public sector.

4.2.1.2 How to assess a sector for QKD adoption

QKD can be used in various sectors and use cases. There are various dimensions by which these sectors can be evaluated in terms of their potential for QKD adoption. These dimensions include:

1) Market and economic aspects

How large is the potential market in the short, medium and long term? How many QKD devices will potentially be needed?

2) Financial capability of the sector

What is the overall financial capability of the sector? And how high is the willingness to pay for QKD?

3) Need/required level of security

How sensitive is the data that is being communicated? How much protection and what level of security is required?

4) Urgency (long-term security)

The "store-now decrypt-later" approach introduces a time criticality into the transition to quantum-safe communication. Depending on how long a piece of information should be kept secret, the transition requires a greater or lesser degree of urgency. Therefore, the questions are: How long does the information in this sector need to be secure? This can range from only a few years to hundreds of years for top-secret information in the public sector. There is some debate about when quantum computers will be able to perform relevant cryptanalytic tasks, but it is expected to be between 2030 and 2040. [1] So, counting back from the year in which the quantum computers could be operational, you get the time frame in which your information could remain secret without quantum-safe methods. Therefore, a maximum time frame of 15 years is still possible. If the information is to remain secret for 15 years, the transition needs to take place now. If the information is to remain secret for more than 15 years, a transition to quantum-safe cryptography would have had to take place in the past.

5) Transition speed

Some sectors are faster than others in implementing changes and carrying out transitions. Assessing the transition speed of a sector is important in order to be able to plan on how fast an adoption of QKD could be performed.

6) Technological feasibility

Today, there are still several technical challenges for QKD. Some of which apply to all sectors, others are more critical only in certain sectors. Looking at the specific technical challenges in the sectors helps to develop the systems in line with the needs of the sector.

7) Framework conditions

Framework conditions, such as regulatory requirements, can be quite diverse in different sectors. Whereas the public administration or the military, for example, are quite strictly regulated, private companies typically face less stringent regulatory requirements.

These and more aspects will be considered in the following sections, in which QKD adoptions will be analyzed in various sectors.

4.2.2 Sector-Specific Application Scenarios for QKD

In this section, we will discuss promising sectors for QKD applications, i.e. the public administration, the military and defense sector, utility provider, the medical sector, banking and finance, industry, and the QKD service sector. In the following subsections, examples of sector-specific use cases, framework conditions and challenges will be discussed.

4.2.2.1 Public Administration

Public administration

- Governments are seen as potential key customers for QKD due to their very high data security needs
- European countries are cautious about adopting QKD, due to low maturity and lack of certification and approval amongst other concerns
- Various projects are ongoing to test QKD and start to implement infrastructure
- High urgency for transitioning to quantum-safe method
- Medium to high market potential for QKD, but significant implementation is unlikely before 2030.

Overview of the sector

Governments and public bodies are often considered promising customers of QKD technologies, due to their long-lasting data security requirements (see section 4.1). At the same time, it is generally challenging to implement new technological solutions in this sector, as they are often subject to strict rules and regulations. The communication networks in the governmental sector include, for example, the connections between different locations of an institution or the connection between different ministries.

Framework conditions of the sector

Under current law, government bodies, i.e., ministries, public administrations, and local authorities (as well as operators of "critical infrastructure" and companies of special public interest such as defense companies or companies of high economic importance) must implement certain IT security measures. These include cybersecurity risk analyses and preventive security measures for their IT systems in order to assess and minimize security risks.

The NIS2UmsuCG is primarily aimed at operators of critical infrastructures (KRITIS). In principle, government and public administration are also considered critical infrastructures, but they have already been exempt from many KRITIS obligations in the past, and this will continue with the implementation of NIS2. OpenKritis [35] lists which ministries and authorities at federal, state, and local levels are affected by the implementation law and which are not, and where there are activities to voluntarily comply with the requirements of NIS2. In general, it can be said that the NIS2 requirements and the additions made by the KRITIS framework law (KRITIS-Dachgesetz) apply to all federal ministries, the Federal Chancellery, and the federal administrative institutions as well as public corporations, institutions and foundations, but that many parts of the administration at the state level (Bundesländer) and local level (Kommunen) are excluded. [35]

The minimum requirements formulated in the NIS2UmsuCG are supplemented by the standards that the BSI has already developed based on the IT Security Act 2.0. These include the requirement that administrations use state-of-the-art IT security technologies in the following areas:

- Attack detection systems, (e.g., intrusion detection systems [36]),
- logging systems for processing internal authority data for the detection of faults and attacks,
- state-of-the-art security software and hardware,
- encryption technologies for sensitive data and communication, and
- authentication systems for secure access control. [11, 35]

Another measure is to ensure that IT security is certified according to Common Criteria Protection Profiles. Protection profiles are a set of security requirements for a specific type of IT product. These profiles compile security requirements for particular types of IT products and are used as part of the security certification of IT products according to "Common Criteria" (ISO/IEC 15408 2020). [37] Vendors can use a protection profile to describe the security features of their products and use it as a guide for implementation. Test centers can test and validate the level of security based on the protection profile. [38] For more details see section 6.2.

Status Quo

To date, national security authorities in various countries have made recommendations to address the threats of quantum computing and have also provided statements on the use of QKD for security. While the USA and the UK have shown hesitation towards the use of QKD in the public administration, the European Commission mentions the possibility of using QKD as a hybrid solution with PQC. The national security agencies of Germany, France, the Netherlands and Sweden assess the maturity for practical applications as currently too low for applications beyond niche use cases (Table 1). Multiple European countries' agencies provided supporting letters or similar statements afterwards. Nonetheless, various implementation projects are in progress, testing the implementation of QKD into governmental communication networks (see below).

On the other hand, China and South Korea have already set up QKD networks with the goal to ensure secure communication. For example, the Beijing-Shanghai Backbone Network is a 2000km long QKD link with 32 trusted nodes that connects the cities of Beijing, Jinan, Hefei and Shanghai. [39, 40] To connect various sites within these cities, metropolitan QKD networks have been developed and attached to this backbone. One example is the Jinan Municipal Party and Government Quantum Communication Network. [41] This network is restricted to Party and government users. [42]

SK Telecom in South Korea, together with ID Quantique, is trying to construct one single convergence network connecting government organizations across countries, with QKD systems being installed. The first phase of the project was completed in 2022, building a backbone network with a total length of 800 km, which connects 48 organizations. [43] The final goal of the project is to develop a network of up to 2,000 km. [44] Also, the regulatory requirements have been met recently, when the QKD-system used for this network received the national security certification and thus meets the national security standards of South Korea. [45]

Table 1: Relevant countries and their current position on QKD.

Country (Authority)	Position on QKD
US (NSA)	"***NSA does not support the usage of QKD or QC to protect communications in National Security Systems*** *and does not anticipate certifying or approving any QKD or QC security products for usage by NSS customers unless these limitations are overcome.*" [46]
UK (NSCS)	"***the NCSC does not endorse the use of QKD for any government or military applications*** *and cautions against sole reliance on QKD for business-critical networks, especially in Critical National Infrastructure sectors.*" [47]
DE (BSI), FR (ANSSI), NL (NLNCSA), SE (Swedish Armed Forces)	"*Due to current and inherent limitations,* ***QKD can however currently only be used in practice in some niche use cases.*** *For the vast majority of use cases where classical key agreement schemes are currently used it is not possible to use QKD in practice.*" [48]
EU (The European Commission)	"*This Commission Recommendation encourages Member States to develop a comprehensive strategy for the adoption of PQC, … This should lead to the deployment across the Union of PQC technologies into existing public administration systems and critical infrastructures* ***via hybrid schemes that may combine PQC with existing cryptographic approaches or with Quantum Key Distribution***." [49]

Possible scenarios and added values of QKD use in the sector

Use case: Secure communication between governmental institutions (e.g., ministries)

There are different kinds of information that are being communicated between governmental institutions. They are typically classified into different security levels that can vary from country to country. However, classifications from official to top secret are typical. In Germany the security levels for classified information are *for official use only*, *confidential*, *secret*, to *top secret*.[4] [50] QKD will not be useful for all communication between governmental institutions due to its current high costs and its technological limitations but could represent an option for secret and top-secret information.

Ministries are already using encryptors to enable secure communication of classified information. They traditionally work with asymmetric keys that potentially can be decrypted by quantum computers. Therefore, a transition to PQC algorithms is currently taking place. For an additional layer of security, QKD keys could be used in combination with PQC in those encryptors. The security in this scenario will hence be house-to-house (ministry to ministry) rather than end-to-end in terms of communication devices.

Considering Germany with its 16 federal ministries and various subordinate agencies (e.g., Foreign Intelligence Service - BND, Federal Criminal Police Office - BKA, etc.), as well as the different locations of these ministries (Berlin and Bonn) and agencies, a considerable number of sites would need to be connected (>100 sites). Furthermore, depending on the amount of classified data that needs

[4] German: "VS - nur für den Dienstgebrauch", "VS - vertraulich", "geheim", "streng geheim"

to be transmitted, several QKD systems would need to be installed at each site. Additionally, the state ministries and agencies also deal with classified information and connecting them would significantly increase the market.

But secure communication is not only necessary within one country. The EU member states, for example, have to work closely together and thus also communicate classified information. Hence, secure cross-border communication is very important as well. This poses additional demands on the interoperability of the systems and regulatory requirements of both countries.

Assessment of the public administration for QKD adoption

The assessment of the public administration for the implementation of QKD depends on various aspects that are discussed in this section and summarized in Table 2.

1) Market and economic aspects

The number of ministries and government agencies within Germany and the EU is large enough to create a significant market for QKD systems, if they were to be installed at all sites. Due to regulatory requirement, this market is not expected to develop in the near future, as approval from national security agencies is required in Germany and other EU member states. In the medium and long term, however, significant market developments in this sector are conceivable. Several funding programs in the EU and its member states have been launched to set up the initial infrastructure required for QKD. The EU's EuroQCI program is the most promising initiative in this area. This program also simultaneously creates an early market opportunity for QKD vendors to sell their systems.

2) Financial capability of the sector

The financial capability of public administration can be considered medium to high. On the one hand, the government has the power to decide on how taxes are spent and has considerable resources at its disposal. On the other hand, most countries are struggling to realize all the planned projects and initiatives with the budget available to them. Hence, it always depends on the priority that governments give to a certain project or initiative. Therefore, the money for a transition towards QKD-secured communication in public administration would be available. The question is rather whether the priority for this transition is considered high enough to drive it forward.

3) Need/required level of security

The information that is being communicated between governmental institutions can have different classification level and can be up to top secret. Such communication data can contain information on national security, thus the required level of security in this sector is very high.

4) Urgency (long-term security)

In public administration, classified information should be kept secret for more than 10 years, in the case of top-secret information, e.g., information on national security, this can be extended to 100 years. Hence the transition to quantum-safe cryptography is urgent, especially considering that data is already being intercepted and stored.

5) Transition speed

The transition speed in the public administration is typically rather low, as various regulations and standard procedures exist that make a transition to quantum-safe cryptography slow.

6) Technological feasibility

In 2025, QKD is still facing various technological challenges that complicate its broad usage. As discussed, the distance limitation is one of the biggest challenges. This limitation makes it necessary to use trusted nodes if communication is to be carried out over a distance of 100 km. This on the other hand raises the question of who operates the trusted nodes and how can one make sure that

these nodes are secure. In particular, when communicating top-secret information, trust in the technology has to be very high, and it is not certain whether trusted nodes will be approved for this use.

Additionally, the stability and robustness of the QKD systems has to be improved so that trained IT experts can operate the devices and little maintenance is needed. The key rate should be enhanced and the interface to the network management systems needs to be improved. And finally, the prices for QKD systems and the infrastructure (which currently need dark fiber) should be reduced.

7) Framework conditions

The public administration is a highly regulated environment, and strict rules exist for the implementation of security solutions. In order to deploy new communication technologies, the product needs to be approved by the national security agency. To date, no QKD system has been certified by the BSI or any other European national security agency. It is expected to take at least two to five years for the first QKD system to be certified in Europe. Recently the European Commission initiated a project called Nostradamus, which is led by Deutsche Telecom, and aims to build test infrastructures to enable the evaluation and certification of QKD devices for EU players. Nevertheless, the certification process will be conducted by each country's individual security agency.

On the other hand, there are government institutions that do not fully depend on the certification and approval of the national security agencies, such as state authorities in Germany. However, it is not likely that government institutions will take the risk to broadly implement a technology that has not been certified by the national security agency.

At the same time, many people and government institutions have little knowledge about the threat on data security by quantum computers and rely on recommendations by the national security agencies. As mentioned above, most European national security authorities do not currently recommend QKD technology and some even recommend that it should not be used for national security, emphasizing its low technical maturity.

Table 2: Summary of expert's assessment of the public administration:

Market potential (medium-term)	**Medium to high**
Financial capability of the sector (willingness to pay for security)	**Medium to high**
Need/required level of security	**High**
Urgency (long-term criticality of data)	**High**
Transition speed in the sector	**Low**

Source: Workshop

Examples of demonstration projects

Many demonstration projects have been carried out for QKD in the public administration. The biggest project in the EU is EuroQCI that aims to create a secure quantum communication infrastructure spanning the entire EU. [51] It is divided into notional projects, for example:

Table 3: Examples of QKD demonstration projects in the public administration:

Country	Description
Austria	Austria will work on a QKD demonstration network installed via inner-city connections in Vienna. The network connects the Federal Chancellery (BKA) as a central node with the three ministries (Ministry of Defense, the Ministry of the Interior and the Ministry of European and International Affairs). [52]
Denmark	Denmark's national project will establish a metropolitan network between five public authorities and two associated data centers in the Copenhagen area. [53]
Netherlands	The Netherlands' EuroQCI project will establish a governmental QKD testbed, which connects multiple ministries for exchanging data in the Amsterdam – The Hague region. [54]

Many other examples of demonstration projects have been summarized elsewhere. [55]

Conclusions

The public administration represents one of the most promising application sectors for QKD, in the long term. Due to the high security standards and regulatory requirements, especially in European countries, QKD is likely to play a significant role in this sector only after significant standardization results have been accomplished and QKD systems have been certified. Therefore, a market implementation in this sector beyond prototyping and testing is not likely to happen before 2030.

Beyond these regulatory framework conditions, the technical limitations, such as the distance limitation of approx. 100km, limits the use in this sector. Possible solutions such as trusted nodes might not be approved to be secure enough by authorities, which would significantly limit the application cases. In the long term, when quantum repeaters are available, a broader implementation in this sector is likely, due to its high security requirements.

4.2.2.3 Military and Defense

Military and defense sector

- Extremely high communication security standards are necessary
- Financial capabilities tied to political decisions, but high in general
- Trusted nodes could be comparatively easily implemented on military sites. Additional trusted nodes, however, raise critical questions about how to maintain the network's security
- While strategic use cases are anticipated in the next years, it remains unclear to what degree QKD will become relevant for tactical use cases

Overview of the sector

Ensuring a high level of information and communication security is critical for the military. Eavesdropping on the communication of adversaries can be used to gain relevant information on military capabilities or mission details, which provides a powerful strategic advantage. For this reason, approaches to secure communication channels are highly relevant for this sector and as such the development of QKD is being followed with interest. On the other hand, as already mentioned in the public administration section, the relevant authorities of various countries have formulated clear positions to public actors on the use of QKD technology in national security (Table 1). While the use of PQC is strongly recommended in many cases, the development of QKD is being monitored to assess the future potential of the technology. Due to the high strategic relevance, the military sector has stricter requirements on the data and communication security than public sectors. In this chapter, the unique perspectives and use cases of the military sector will be discussed.

Framework conditions of the sector

Companies in the security and defense industry have been classified as "companies of special public interest" (UBI) since the IT-SiG2.0 came into force in 2021 and have been subject to increased cybersecurity requirements ever since. With the implementation of NIS2, the UBIs will cease to exist as an independent group and the defense sector will be integrated into the NIS2 manufacturing sector as they will fall into the important and very important institutions categories. Under NIS2, companies in the defense industry may be affected if they exceed certain thresholds for company size and produce specific goods according to NACE codes[5]. This could include manufacturers of optical equipment, communication devices, electronics, radars, GPS, antennas, electrical components, aerospace and aircraft parts, military combat vehicles, and other related products. [35] According to §29(3) NIS2UmsuCG [13] the Federal Ministry of Defense and its subordinate agencies, on the other hand, are not covered by the critical infrastructure regulations, thus maintaining a distinction between private sector defense companies and government defense entities. [35]

Government defense institutions in Germany, i.e., the "Bundeswehr" have defined their own stringent security requirements, including in the area of information and cyber security. Cybersecurity in the Bundeswehr is organized through the Cyber and Information Domain Service (Kommando Cyber- und Informationsraum, KdoCIR), which was established in 2024 as a full military service branch. [56] The KdoCIR is responsible for managing cybersecurity, IT, military intelligence, geo-

[5] The economic sectors in the European Union are classified by NACE codes

information, and operative communication units within the Bundeswehr. KdoCIR and BSI work closely together not only in the area of operational IT security (especially in the National Cyber Defense Centre), but also in the definition of security standards, ensuring that civilian and military standards are aligned. However, the boundary between civilian and military requirements is fuzzy. While certain KRITIS sectors already have high technical cybersecurity requirements, military cybersecurity standards are generally more stringent and comprehensive. [57] This is due to the sensitive nature of military operations and the potential impact of data breaches on national security.

Status Quo

It should be noted that it is difficult to obtain detailed information about the implementation of communication technologies in the global military environments because this information is extremely relevant to national security and therefore highly confidential. Nevertheless, taking into account the recommendations of national security agencies, many national security actors are currently focusing on the transition to PQC. The development of QKD in this sector is seen by experts as a complementary solution to that proposed as a hybrid scenario.

Some initial global activities involving the use of QKD technology in a military context can already be assumed based on the following examples:

- The Indian Army has initiated the process of procuring the QKD systems developed by QNu Labs, after the success of a trial project. [58]
- One researcher points out that the People's Liberation Army in China is one of the major clients of the country's quantum communication networks, indicating the nature of the technology as part of the civil-military cooperation activities. [59]

NATO formulated its Quantum Technologies Strategy and published its summary in January 2024. The document states, *"In the future, further improvements could allow QKD to also contribute to secure communications"* and highlights the possibility of the cooperation among Allies in the development and implementation of QKD as well as PQC. [60] NATO is also promoting R&D activities under the framework of Science for Peace and Security (see demonstration projects below). The military sector in Germany will follow the recommendations of the BSI and is therefore currently only observing and testing QKD (see demonstration projects below). The military is aware of the potential value that quantum networks offer for applications beyond QKD. [61]

Possible scenarios and added value provided by the use of QKD in this sector

Use case 1: Strategic communication between domestic military sites

Similar to the communication between government sites, the strategic communication between domestic military sites could be carried out via QKD-secured channels. Communication between military sites naturally contains highly confidential information. Nowadays, this is either encrypted using asymmetric key generation algorithms (e. g. RSA) or by encryption based on the symmetric distribution of initial keys, often transported as a physical object by a courier. Compared to the latter, QKD offers advantages in terms of speed and, presuming that a QKD network is in place, flexibility, albeit with a different security profile: QKD-keys promise long-term security in the face of continuous interceptions by eavesdroppers if an implementation with protection from side-channel attacks could be achieved. Nevertheless, the implementation of QKD links between the military sites requires a suitable infrastructure that can cover the distances between the locations. In the absence of a convincingly scalable satellite-based QKD infrastructure, this can only be achieved by rolling out an suitable fiber infrastructure, which is limited by the current range of the systems. Significantly greater distances between military sites can only be covered with the implementation of trusted nodes or yet to be developed technologies like quantum repeaters.

Trusted nodes are a controversial topic, as it widens the attack surface of the QKD link. In what form trusted nodes will be accepted in a QKD network for strategic military purposes cannot be conclusively clarified at this stage. However, the part of the network actual on the military site can use secured nodes with comparatively low effort, as a certain level of protection will be present. In densely populated countries, military sites usually lie closer to each other, which could enable a QKD network, where all nodes are located at these sites. Setting up such an infrastructure comes at a high cost for the additional fibers and the QKD systems. If additional trusted nodes are required to close the gaps in the network, questions on how these nodes will be secured so as not to reduce the security of the complete communication network have to be addressed.

We modelled a simplified network for Germany based on the towns and villages in which the Bundeswehr is located according to their careers homepage. [62] The number of locations in Germany according to this homepage is 269 – the number of individual sites however will be much larger, as the Bundeswehr refers to nearly 1500 sites all over the world. [63] However, as this rough estimation only aims to provide an impression of the complexity of the required QKD network in Germany, the approximate locations as given on the careers homepage suffices.

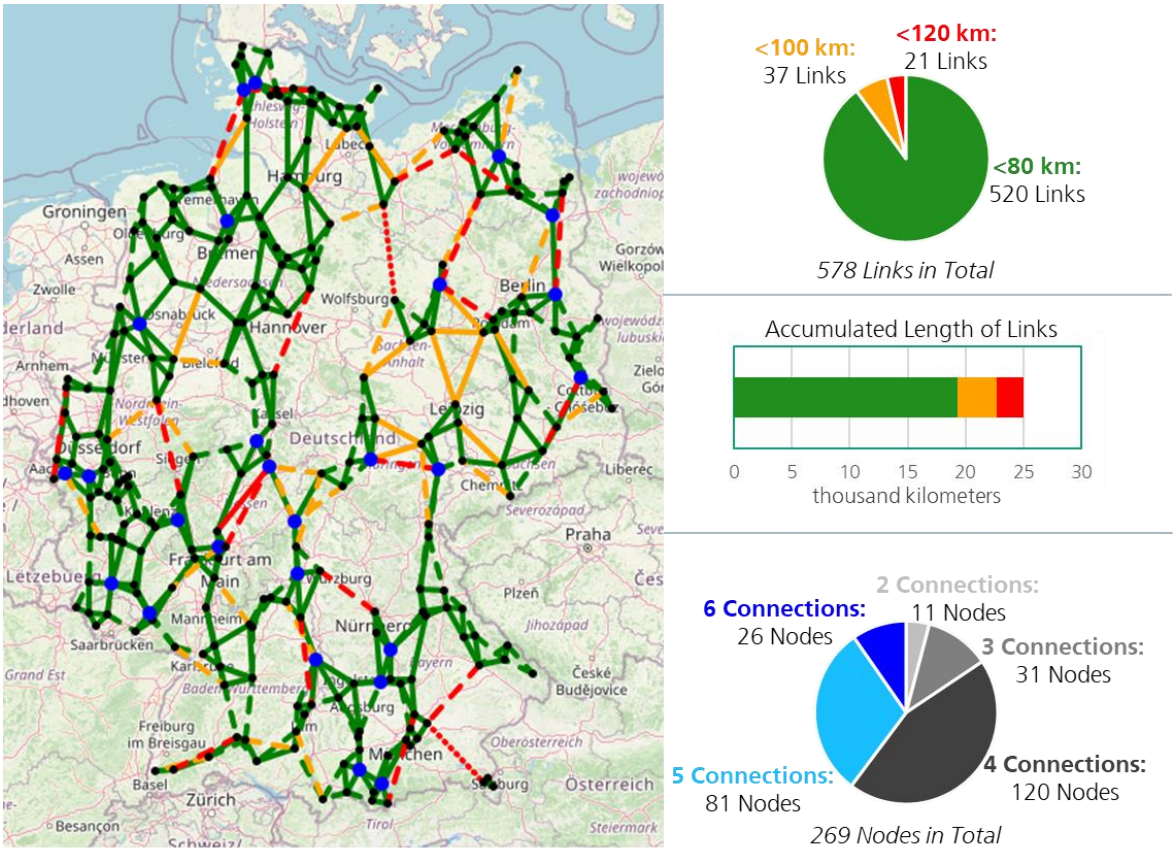
Figure 2: Hypothetical QKD network between villages/towns with Bundeswehr sites

This analysis is based on strongly simplified assumptions (taking only into account the villages/towns in which Bundeswehr sites are located according to the careers page of the Bundeswehr. Not taking into account any existing fiber infrastructure.

Green: Links shorter than 80km; Yellow: 80-100km; Red: 100-120km

Full lines: Two or more redundant paths with 5 or less intermediate nodes; Dashed: One redundant path (<5 nodes); Dotted: No redundant path (<5 nodes).

Black Nodes: connected with 1-5 links to the network; Blue: connected over 6 links to the network



In Figure 2, an example for a hypothetical QKD-network is modelled6, solely based on the data of towns and villages with existing Bundeswehr sites. Even though this is not sufficient to create a realistic representation of a Bundeswehr-QKD-network due to several reasons (not taking into account exact locations, additional sites, existing infrastructure), it should be sufficient to illustrate the fact that with the sites in Germany being so densely located, an implementation without the need for additional trusted nodes (in the sense of locations outside of existing Bundeswehr buildings) would be possible in theory for 266 of the 269 locations, when a maximum inter-node distance of 100 kilometers is assumed. However, the assumption that all sites are connected end-to-end with sufficient fibers and are used as nodes in the network is too ambitious in the short-term.

For countries with a less dense distribution of military sites, or international alliances, similar QKD fiber networks are not possible without trusted nodes or technology as yet to be developed.

Use case 2: Communication with a deployable communication center in the field

A separate use case is the communication from the headquarters in the home country to a deployable headquarters in countries in which the military is active (e.g., missions, combats, etc.). Deployable headquarters must be flexible to a certain extent and, in most scenarios, are located far from their home country, making a fiber connection impossible in most cases. Therefore, the only viable option would be a connection via one or more QKD-satellites.

The need for secure communication with the home country is very high. Even though key material can be pre-shared for symmetric encryptions, the continuous establishment of new keys as provided by QKD offers security advantages: e.g., if the pre-shared key material is compromised, the exchange of new material requires time and effort.

However, PQC-encryptions offer already a high level of security. The long-term security plays a role as the potential USP of QKD compared to PQC, if the information being exchanged needs to be protected over very long periods of time. To what extent this applies to the data that is commonly exchanged over this channel, is not clear.

Use case 3: Tactical communication via free-space QKD for use in the field

Another interesting use case is the use of QKD between mobile units (or with headquarters) in the field. This applies equally to soldiers in vehicles, airplanes, ships and submarines, as well as to remotely controlled vehicles, such as drones. As fibers are impractical in most of these scenarios, promising approaches can be found in free-space QKD via direct optical links (in the case of submarines even under water) or satellites.

The quicker and the less predictably the unit is moving, the harder it will be to establish a QKD link. However, as keys can be stored, a continuous connection of the quantum channel is not required, as long as the key rate is sufficient to generate enough key material for the time spans in which the (quantum) connection is lost. Furthermore, the requirements for mobile QKD systems are very high, especially as robustness in the face of harsh environmental conditions in the field is absolutely essential.

However, the advantages of QKD over non-quantum approaches to key distribution are limited: Most missions only last a limited amount of time, which makes it possible to change pre-shared key material between missions. The information exchanged in the field (e.g., commands) is mostly

[6] The model is based on two simple rules: 1) Connect the two locations with the shortest inter-node distance, as long as they are not already connected over two redundant paths with maximum 5 intermediate nodes. 2) Stop when the inter-node distances are larger than 80km (green), 100km (orange), 120km (red).

only critical for a short period of time, which reduces the disadvantages of PQC (relying on cryptoagility). In view of this and given the low maturity of free-space technology, the effort and cost of implementation, this use case is not expected to be realized in the medium term.

Assessment of the military sector on the adoption of QKD

1) Market and economic aspects

The military usually uses separate fiber networks (such as those provided by the BWI for the Bundeswehr) and have implemented security measures at its sites that can be theoretically used as trusted nodes. Therefore, integrating QKD systems into their fiber-based infrastructure could be less challenging than in some of the other sectors discussed in this study. Therefore, the military sector has a relevant market potential for QKD technologies in the future.

The Bundeswehr alone operates several hundred military sites in Germany. If all their sites become part of a QKD-secured communication network in the future, this number gives an impression of the potential market potential in this sector.

2) Financial capability of the sector

Some experts estimate the military sector's financial capabilities to be higher than other sectors, as their purpose is often beyond economic considerations: it deals with highly confidential information, and it is about protecting the lives of citizens. On the other hand, in most countries, QKD technology providers have to go to considerable lengths to obtain the approval required to implement the solution, which could pose a barrier to the market for foreign-based enterprises. This situation could pose both a risk and an opportunity – on the one hand, such an approval and certification practice will deter the proliferation of more mature systems developed outside of the country, while on the other hand it could ensure technological sovereignty by providing an incentive to domestic developers.

3) Need/required level of security

Since the purpose of the military is to ensure the nation's security, the need for a highly secure communication channel is crucial. Failures of the communication systems would lead to critical security risks.

4) Urgency (long-term security)

In many cases, the confidentiality of the information being communicated between military actors must be guaranteed over long periods of several decades. Any leak of information about the strategic plans for the military's protection of the nation could have devastating consequences. Long-term protection of the most confidential data is therefore undoubtedly of great importance.

5) Transition speed

The transition speed of the military sector depends greatly on the framework in which it takes place. Some countries provide their military with extensive powers and financial capabilities, which enables the quick implementation of new technology, if it offers a strategic advantage. However, usually the equipment and infrastructure of the military sector have to be tested extensively to ensure that they are suitable and meet their exacting requirements (including certification and approval). In many European countries like Germany, the processes to buy and implement new technology is closely connected with public authorities, which can slow down the procurement. Furthermore, the complex communication infrastructures and the great number of military sites in many countries lead to concerns about whether a quick transition to a QKD communication network is possible. The experts in the workshop therefore assumed that only a low transition speed can be expected in the military sector.

6) Technological feasibility

To cover the whole military network, trusted nodes will be required in most scenarios. However, until there is an official definition of trusted nodes (how do we define "trusted"?), the implementation of such nodes in a military environment poses a challenge.

In some cases, communication security solutions must meet specific performance indicators in order to be approved for military applications. In the case of Germany, for example, the solution should offer a certain level of key rate to guarantee that the key is not reused so often that the security level becomes a hindrance. However, the required key rates for realistic scenarios are still expected to be relatively low (kbit/s). [64]

If QKD systems can achieve suitable key distribution over longer distances, it will reduce the number of necessary nodes and systems to cover the entire network, resulting in a reduction in the infrastructure cost.

In real operational environments, robustness of the system, temperature stability, monitoring systems and system redundancy are required. A simplification of the key management systems is also favorable from an operational point of view. Furthermore, standardized solutions or interfaces are required to enable communication with different forces, e.g., from other countries.

7) Framework conditions

Developing technological solutions that are mature enough to gain the approval from the relevant authorities is critical in order to deploy QKD in the military sector. However, the exact regulations are country specific.

Another challenge is to implement QKD across borders. Currently, EuroQCI is addressing this challenge by pushing for a connection of terrestrial QKD networks in different member states. The transfer of confidential information across the border itself is subject to further regulations of the participating member states.

Table 4: Summary of the expert's assessment of the military sector:

Market potential (medium-term)	**Medium to high**
Financial capability of the sector (willingness to pay for security)	**High**
Need/required level of security	**High**
Urgency (long-term criticality of data)	**High**
Transition speed in the sector	**Low**

Source: Workshop

Examples of demonstration projects

Even though the detailed activities within the military sector are often classified, important demonstration projects testing QKD have been publicly communicated. There are various projects in Europe and internationally in which QKD is being tested in the military field. A list of relevant activities is given in the following Table.

Table 5: Examples of QKD demonstration projects in the Military and Defense sector:

Country/ Actor	Description
NATO	NATO's framework of Science for Peace and Security is supporting a number of projects to explore the use QKD in the military sector, for example: [65] • "Quantum Cybersecurity in 5G Networks (QUANTUM5)" aims to demonstrate the practical applications of QKD in 5G networks • The objective of the "Implementation Vulnerabilities in QKD Components for Fiber and Drone Applications" is to use next-generation components to identify loopholes in QKD technology and propose protocols and/or algorithms to minimize the risk of eavesdropping. • "Secure Communication via Classical and Quantum Technologies" pursues a security model allowing the design of cryptographic protocols for secure group communication on a PQC/QKD hybrid network.
EDA	The European Defence Agency also promoted quantum secure communication projects, including QKD, under the framework of the Preparatory Action on Defence Research. [66]
Germany	The Federal Ministry of Defence (BMVg) supports the Munich Quantum Network (MuQuaNet) project, the goals of which are to develop and build a quantum-secure communication network and to enable the network for research organizations, authorities and military actors. Part of the MuQuaNet is the BWI GmbH, which is responsible for the fiber network used by the Bundeswehr. One example of an application simulated in this project is the remote maintenance of a military platform. [67]
Italy	Research and demonstration projects on underwater QKD have been conducted to ensure secure communication between a submarine and another party (submarine, ship, unmanned underwater vehicle). In this approach the underwater equivalent to free-space QKD was used. [68]

Conclusions

The military sector is one of the most interesting potential markets for QKD technologies, due to their exacting security requirements, including long-term protection of communication. In most countries, the military has access to substantial financial capabilities and is therefore in general able to implement new cost-intensive technologies.

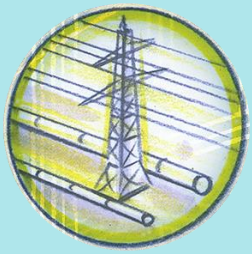
In countries like Germany, the military sector has to obtain approval from public authorities for the technological solutions to be implemented. An implementation of QKD solutions that are not approved for their communication networks is not possible or foreseen in the majority of countries. The most promising use case is implementing QKD links between domestic military sites, due to the possibility of using existing militarily-secured locations as trusted nodes to extend the distance limitations of QKD systems. Compared to the use cases for tactical communication, the technological requirements are easier to meet.

Due to its complementary profile, QKD could therefore play a significant role in the military sector alongside existing symmetric (pre-shared keys) and asymmetric (e.g., RSA, Diffie-Hellman, …) key exchange solutions. However, the remaining technological challenges to achieve an approval for relevant applications by the relevant public authorities have to be resolved first.

4.2.2.4 Utility Provider

Utility Provider

- This sector offers great market potential due to the important role in maintaining public order.
- Above all, the power grid could become an interesting area for the application of QKD.
- Challenges include high implementation costs, technical immaturity (e.g., robustness of systems) and the complexity of integration
- Providers often only do the bare minimum – regulatory requirements would significantly accelerate expansion but are unlikely in the short to medium term.



Overview of the sector

The basic supply of electricity, gas and water to households, as well as to industry and public institutions, is part of the critical infrastructure. Critical infrastructures refer to the assets, systems, and networks that are essential for the functioning of a society and economy. These infrastructures are crucial for maintaining national security, public health and safety, and the overall well-being of the population. The failure or disruption of these infrastructures can lead to significant economic and social consequences. In addition to the providers of electricity, gas and water, further areas are summarized under the heading critical infrastructure, e.g., food production and distribution, healthcare, transportation, telecommunications, and financial services. Areas that are not considered in the following are financial services and healthcare which are discussed separately.

Framework conditions of the sector

The energy sector (electricity and gas supply, fuels, domestic heating oil and district heating) was one of the first economic sectors to be considered as part of the critical infrastructure. Companies in the sector are therefore obliged to fulfil the requirements of the IT-SiG 2.0 and the BSI-KritisV, and in future the NIS2 directive (for the requirements companies must meet according to these laws, see section "The regulatory context" above). The forthcoming implementation of NIS2 will increase the security requirements for companies in the energy sector (for details see [69]). The exact requirements again depend on the size and type of services provided, with a distinction being made between operators of energy supply networks, operators of energy installations, operators of energy services and operators of KRITIS energy supply networks or installations (for detailed thresholds and criteria, see [35]).

Energy companies are also regulated by the German Energy Industry Act (EnWG, "Energiewirtschaftsgesetz") which sets out IT security requirements for energy infrastructure providers. According to the EnWG, energy companies classified as KRITIS have been obliged to implement the IT security catalogue ("IT-Sicherheitskatalog") of the German Federal Network Agency ("Bundesnetzagentur") since 2024. This requires the establishment and certification of an information security management system (ISMS) in accordance with DIN EN ISO/IEC 27001. With the transition to the European NIS2 regulation, this IT security catalogue is currently being revised. [35]

The IT security catalogue classifies the energy company system into six zones, each of which is subject to different levels of IT security regulation. The zoning is a classification of applications, systems, and components of an energy plant in terms of their importance for a secure operation. [70] Under the new Energy Industry Act, which will come into force in 2025, the Federal Network

Agency will draw up a new catalogue of security requirements for energy system operators, although it remains unclear whether the zoning approach will be continued. The current draft of the law ("Referentenentwurf" [71]) does not envisage any changes to zoning.

Status Quo

In many countries, including Germany, the electricity, gas and water infrastructures are subject to specific regulations and protection to ensure their resilience and security. This involves measures like risk assessments, emergency preparedness, and the implementation of robust security protocols to safeguard against threats such as cyber-attacks, natural disasters and other potential hazards. Ensuring the reliability and security of critical infrastructures is a key priority for governments and organizations worldwide.

QKD could be an approach to secure the grid and prevent blackouts as well as protecting national pipelines from hackers. To achieve this, QKD has to be implemented as an additional layer of security for power line communications, safeguarding the smart grid. [72] So far, the emergency communication level is satellite-based, but QKD could be used to create redundancies.

Several institutions, including the State Grid Corp of China and the Oak Ridge and Los Alamos National Labs, are investigating the application of QKD networks to protect the energy grid, with the objective of ensuring safe and stable operations. [55] Also, the application of QKD for multi-source data security protection of the smart grid is under research. [55]

The need for secure communication is regarded as important especially in the power grid. Among other things because this grid is becoming increasingly important due to the energy transition and the regulation and maintenance of grid stability are most complicated here. In addition, fiber optic cables are often laid alongside power lines (and copper cables are often laid alongside gas or water underground cables), and the distances are even greater at water and gas nodes that can be connected by QKD. The number of network operators and the network is large. Only in Germany, there are about 800 distribution network operators in the power grid alone with at least 2 control rooms that have to be secured also by back-up lines.

Possible scenarios and added value of QKD use in this sector

Use Case 1: Connection between substations of a grid network

As cyber threats grow, QKD can provide robust protection for the central nodes of the network (e.g., power and transformer stations, pumping stations). Especially in smart grids, QKD could play a crucial role in protecting command control data related to energy or water infrastructure. This can prevent cyber attacks from controlling or disrupting infrastructure and the corresponding control commands from being implemented, protecting against unauthorized access and potential sabotage. In Germany alone, there are around 3000 transformer stations, resulting in a network with typical distances of around 50 km between two adjacent nodes. The key rates required for the secure information transmission are low, but weather conditions, for example, could play a role. In some cases, fiber-optic cables are already in place alongside the power lines which can be used for QKD.

Use Case 2: Securing communication between control rooms or grid operators

QKD can be integrated into communication networks to secure data transmission between critical nodes like control rooms or different grid operators, ensuring that communication remains confidential and tamper-proof. As the amount of data is larger than in use case 1, the required key rates are expected to be larger as well. The control rooms are located at various distances from each other, depending on the network or, for example, the number of inhabitants, but can be more than

100 km apart. While the range of QKD fiber-based systems will be sufficient for some connections, others would require the implementation of trusted nodes or eventually quantum repeaters.

Assessment of the utility sector for QKD adoption

1) Market and economic aspects

The market for QKD in the critical infrastructure is emerging. Organizations are beginning to explore QKD solutions as the awareness of quantum threats grows. QKD experts assume a high market potential in the medium term. However, economic constraints and the need for clear regulatory frameworks may slow the pace of adoption. Thousands of devices would be needed in Germany alone for a comprehensive roll-out at the most important network junctions.

2) Financial capability of the sector

Security is an extremely important topic in this sector, which is regulated by various authorities. Depending on the technology, the IT equipment used has a limited lifespan of between five and ten years. Devices are replaced accordingly, and technological innovations can quickly come onto the market. However, network operators strictly adhere to the basic requirements and only spend the bare minimum. Grid operations must be as cost-efficient as possible – otherwise they will be too expensive for customers. In the industry, CapEx is a particularly critical factor, which currently makes investments in QKD unattractive. Since it is always possible to spend more money if this is required by regulations, the potential is considered to be medium.

3) Need/required level of security

Since critical infrastructure is essential for maintaining public order, experts rate the need for security as medium to high. However, some experts who work in the critical infrastructure sector also say that the control commands and information sent for controlling networks are only of low criticality. It is more problematic if, for example, knowledge is gathered by monitoring the control channels in order to manipulate the network afterwards. Also, the risk of actual physical attacks is greater.

4) Urgency (long-term security)

Experts in the workshop estimate that the urgency in this sector is high. At the same time, business-relevant data is stored for approximately 10 years in this sector. The data on grid control are very dynamic and not very valuable after a few years. There are therefore arguments for downgrading the urgency.

5) Transition speed

Due to the large number of operators right down to the regional or municipal level, the transition speed is rather slow. Many things are bureaucratic and take time to change. Typically, years are needed for the implementation of new technology. If the urgency is such that a real attack could conceivably have taken place under the circumstances, the transition speed can accelerate within a few months. However, if action is taken when a situation has become critical, it is likely that problems will arise in the supply chain.

6) Technological feasibility

While QKD technology has made significant advancements, there are still challenges to its practical deployment. Even though the distances between two control rooms or substations in the power grid, for example, are often less than 100 km, there are still some individual routes, particularly in less-populated areas (or redundant connection lines that are longer than the direct connections), where distances over 100 km have to be covered. With the devices currently available on the market, this is not always possible. Almost more important, however, is the system robustness. The infrastructure is exposed to all weather conditions and must be durable.

7) Framework conditions

Since critical infrastructure is subject to regulatory requirements it also makes sense to create a regulatory environment in the area of QKD.

Table 6: Summary of the expert's assessment of the electricity, gas and water infrastructure sector:

Market potential (medium-term)	**High**
Financial capability of the sector (willingness to pay for security)	**Medium**
Need/required level of security	**Medium to High**
Urgency (long-term criticality of data)	**High**
Transition speed in the sector	**Low**

Source: Workshop

Examples of demonstration projects

There are a few demonstration projects in which QKD has been used in particular for power grid applications. These have taken place primarily in publicly funded projects, (e.g., the OpenQKD project). We are not aware of any privately funded projects.

Table 7: Examples of QKD demonstration projects in the utility sector: [73]

Country	Description
Switzerland	Smart Grid project to connect power stations in Geneva (SIG) with QKD testbed, assessing available QKD technologies and services. ID Quantique offers the systems.
Poland	Connection of PSNC datacenter in Poznań with a local police datacenter to secure operational data using QKD network layer equipment together with Toshiba; it involves various aspects like speed, key exchange rate and integration with operational software tools.
Spain	QKD implementation for SCADA networks in Madrid to secure critical infrastructure like water supply and electrical grids; it involves three locations within Telefonica Spain's production network to demonstrate an additional physical security layer. The project partners are IDQ, Toshiba, Huawei
Germany	Demonstration project to connect a power substation in Schleswig-Holstein (SH Netze and ID Quantique are involved). The standard fiber optics installed on electricity pylons were used, which was exposed to various weather conditions.

Conclusions

The integration of QKD into critical infrastructures like electricity, gas or water represents an opportunity for enhancing security in those infrastructure networks. As the sector increasingly relies on digital technologies and information exchange, the need for robust security measures becomes critical. QKD can provide an advanced level of security that is essential for protecting sensitive data.

As organizations in the utility sector begin to recognize the potential vulnerabilities associated with traditional encryption methods, there is a growing interest in exploring QKD solutions. Demonstration projects and pilot initiatives are essential to showcase the practicality and effectiveness of QKD in real-world applications.

However, there are several challenges. These include, like in other sectors, high implementation costs, technical limitations such as distance constraints and the complexity of integrating QKD with existing infrastructure. Additionally, a supportive regulatory environment is necessary to push the sector towards QKD. Even if the financial capability in the sector is high, most companies only do what is required by regulations.

4.2.2.6 Medical Sector

Medical sector

- High potential due to the very critical nature of patient data
- Public medical institutions such as hospitals do not have the resources (either financially or through expertise) for a wide-spread roll-out of QKD at the moment. Cost reductions and a greater technical maturity are necessary
- High-security laboratories could be an interesting candidate for a medium-term implementation of QKD
- Lack of awareness among hospitals and patients

Overview of the sector

The sector is characterized by its critical need for secure communication and storage of files due to the sensitive nature of health data. This includes patient records, medical imaging, and research data. As healthcare systems increasingly digitize and share vast amounts of information, ensuring data confidentiality, integrity and compliance with stringent regulations becomes more and more important. On the one hand, medical facilities such as hospitals or medical practices are being considered for the use of QKD in the medical sector, but medical laboratories are also a promising area.

Framework conditions of the sector

The medical sector was only classified as a critical infrastructure relatively recently and in several stages, although the functioning of the healthcare sector is particularly important for the health and lives of the population and the data it processes is particularly sensitive.

With the adoption of the IT-SiG 2.0 and the BSI-KritisV, hospitals with more than 30,000 full inpatient treatment cases per year were classified as critical infrastructure, which corresponded to only 110, or 10% of all hospitals. [74] At the beginning of 2021, the BSI-KritisV was extended to all hospitals, regardless of their size. From this date on all hospitals had to take appropriate precautions in accordance with the latest technology and implement security objectives. The KRITIS Umbrella Act extends the protection of critical infrastructure in the healthcare sector and now covers various areas such as inpatient medical care, pharmaceuticals and vaccines, laboratories and the supply of life-supporting medical devices. [75]

For hospitals, the industry-specific security standard (B3S) for healthcare in hospitals, developed and regularly updated by the German Hospital Federation (Deutsche Krankenhausgesellschaft, DKG) in coordination with the BSI, is the benchmark for appropriate measures. It calls for organizational and technical measures to secure the "critical service" of hospitals. The primary goal is to maintain the level of care provided by hospitals. [76]

Although physicians in private practice are not considered critical infrastructure, the cybersecurity requirements for this sub-sector have also been significantly tightened in recent years. With the enactment of the Digital Healthcare Act (Gesetz für die digitale Versorgung, DVG), [77] the basic requirements of the IT security guideline in accordance with §75b SGB V (KBV 2020), [78] which was developed by the national associations of statutory health insurance physicians in consultation with the BSI, have applied since 2021. [78] With the implementation of the NIS2 directive, the increased cybersecurity requirements will also be extended to smaller healthcare facilities.

Overall, the cybersecurity standard in hospitals has improved significantly in recent years, but according to the BSI, the healthcare sector still has a comparatively large backlog among the KRITIS

sectors. [79] The situation in medical practices has also improved since the introduction of the IT security guideline, but there are still considerable differences and a need for improvement depending on the size of the practice. [80, 81]

Since March 2024, the Digitalisation Act (DigiG) has also applied to the entire healthcare sector in Germany. [82] The DigiG is part of the national digitalization strategy for health and care. The DigiG is intended to systematically develop and accelerate the digital transformation of the healthcare and social care sector. The aim of the law is to promote electronic patient records (ePA), electronic prescriptions, video consultations and teleconsultations.

Increasing cybersecurity is also one of the goals of the DigiG. To this end, the DigiG incorporates the previous §§75b and 75c SGB V into the new §§390 and 391 SGB V, which now also incorporate mandatory measures to increase the security awareness of practice and hospital staff. The newly introduced §392 SGB V requires health insurances to take appropriate organizational and technical precautions in accordance with the latest technology to avoid disruptions to the availability, integrity and confidentiality of their information technology systems, components or processes that are essential for the smooth running of health insurance processes and for the security of the processed data of the insured persons. In addition, the new §393 SGB V allows the processing of social and healthcare data in the context of cloud computing services if they comply with the BSI's Cloud Computing Compliance Criteria Catalogue (C5). [83]

Status Quo

Medical records include highly confidential information about individuals. Organizations managing such data are legally obliged to protect it in the long term. Simultaneously, this data is a prime target for attackers due to its high value. [84]

Due to the covid pandemic, telemedicine and e-healthcare services have significantly expanded within the healthcare sector. Additionally, various biosensors are now integrated into smartwatches and other wearable devices, collecting and transmitting personal health data and daily activity information. [72] Healthcare organizations must rely on highly secure networks to transmit sensitive information, including patient records with personal details such as names, addresses, dates of birth, social security numbers, and clinical histories. [55]

Apart from the fact that medical data is extremely sensitive, some affected patients are still unaware of the potential consequences of data breaches for them personally.

The relevance of data security in the healthcare sector becomes clear when looking at costs of data breaches. The healthcare industry continues to incur the highest costs of data breaches of any sector. [85] High levels of security and confidentiality of such intimate healthcare data in the era of quantum computing could be ensured by employing QKD-based encryption schemes. QKD may become crucial for securing the storage, transmission and processing of sensitive patient data. [72] The first pilot projects have already been launched for this purpose. However, due to the poor financial resources of the healthcare sector, facilities are currently showing little interest in investing in QKD themselves. The question arising from the poor IT infrastructure in some parts of the healthcare sector, whether QKD is a surplus to requirements and whether other links in the communication chain then represent vulnerability.

Possible scenarios and added values of QKD use in the sector

Use Case 1: Protecting patient files and lab data

Healthcare systems manage vast amounts of sensitive patient information, such as medical records, treatment plans and personal identification data. In addition, there is information from laboratories with high levels of confidentiality, (e.g., genomic data or information about pathogens). Data is sent

back and forth between institutions, e.g., to obtain diagnoses from relevant experts worldwide. Making this data exchange secure is vital for maintaining patient privacy and confidentiality. Quantum cryptography could offer a robust solution for protecting the transmission of health data from unauthorized access and cyber threats. This use case is interesting for hospitals and other medical institutions, but also for laboratories. While the connection between nearby hospitals could be achieved with fiber-based QKD systems, the implementation of a global network would require satellite-based solutions. The effort required to implement such a global QKD network system solely for medical purposes makes it rather unlikely in the short-term.

Use Case 2: Secure telemedicine services

Another use of quantum cryptography is securing communication channels between healthcare providers and patients. For instance, encrypting telemedicine sessions ensures that communication between patients and doctors remains private and confidential. The possible connections between patients and their healthcare providers are very different, however, because patients in particular are in different situations, (e.g., outdoors, at home) and have different distances between each other. For connections to individual patients, the use of conventional telecommunication/internet network will be the only feasible option, which would therefore require a vast number of QKD devices, which is highly unlikely, at least in the next years.

Use Case 3: Security on the wireless body sensor networks in healthcare applications

Quantum cryptography also secures medical devices and sensors that collect sensitive health data, such as vital signs and physiological measurements. Encrypting the data transmitted by these devices ensures its integrity and confidentiality. [86] Here, too, the use of QKD is debatable, since some of the devices are mobile (requiring free-space or satellite solutions), distances vary, and a large number of miniaturized QKD systems would be required.

Assessment of the medical sector for the adoption of QKD

1) Market and economic aspects

The market for QKD in the medical sector is hard to predict. While there is interest from some healthcare organizations, the economic feasibility of QKD will depend on advancements in technology and cost reductions. In particular, awareness for patient data is still not widespread. In addition to hospitals, QKD seems to be of genuine interest for laboratories, but there are only about 60 laboratories with highest security and a few thousand with a high security level worldwide, so the demand here is low for a direct connection between two laboratories. If individual hospitals are also connected, the number increases. If there were a roll-out in hospitals, for example, the number would increase to many thousands of systems. Due to the uncertainties, the potential is estimated as medium.

2) Financial capability of the sector

Generally, the financial capabilities in the medical sector are notoriously tight. Whether or not money is spent on security depends very much on the use case. If the data to be protected is considered very important, then money is available in the healthcare sector (required by legislation/regulations). However, there is still little awareness of critical patient data in particular, so there is not yet a willingness to spend money on the security of health data.

3) Need/required level of security

The data itself are very sensitive, (e.g., genetic information). Therefore, there is a very great need, also for long term security.

4) Urgency (long-term security)

Data cannot be allowed to be lost or fall into the wrong hands. Accordingly, health data must be kept under lock and key for at least the duration of a person's lifetime, and in some cases even beyond that. It is therefore not possible to quantify the storage period in general terms, but in some cases, it is more than 100 years.

5) Transition speed

Change management must be integrated into the existing concept, then it must be certified and accredited. Therefore, the transition process is long and the transition speed generally low. However, situations like the coronavirus pandemic have shown that the healthcare system is capable of responding to acute crises. Although it is still sluggish due to the many different institutions, the lead time is shortening.

6) Technological feasibility

Integrating QKD with existing healthcare IT infrastructures and ensuring interoperability poses significant challenges. The staff who use the IT infrastructure is often not very well qualified in the area of cyber security. A system must therefore be easy to use. For QKD to be widely adopted in healthcare, solutions must be scalable and cost-effective, requiring further advancements in technology. The networking of the many healthcare locations is complex and at the same time the bridging of very long distances, (e.g., expert consultations at the other end of the world) is necessary, which represents a technical challenge that has not yet been solved.

7) Framework conditions

The medical sector requires a regulatory environment and (QKD) devices need to be certified.

Table 8: Summary of expert's assessment of medical sector:

Market potential (medium-term)	**Medium**
Financial capability of the sector (willingness to pay for security)	**Low to Medium**
Need/required level of security	**High**
Urgency (long-term criticality of data)	**High**
Transition speed in the sector	**Low**

Source: Workshop

Examples of demonstration projects

There are a number of publicly funded projects in which QKD has been used in the healthcare sector.

Table 9: Examples of QKD demonstration projects in the medical sector:

Country	Description
Poland	QKD protection of confidential data transfer between hospitals in Poznań, where the PSNC datacenter is connected to a hospital for secure exchange of digital medical data and test results through remote services together with ID Quantique. [73]

Switzerland	In Geneva, the UNIGE-HUG network of hospitals uses QKD from ID Quantique to ensure secure communication between its central data centers over 6 km for sensitive data transfer and long-term storage of patients' medical records, complying with electronic patient record laws requiring document encryption. [73]
United Kingdom	Quantum metropolitan network in Cambridge aims to connect healthcare clusters and universities using Toshibas' QKD technology for secure transfer of private medical data, featuring a fully meshed topology with 10 QKD links and multiple user connections across a 100 sq. km area. [73]
Japan	Securing the high-speed transfer of large-scale sensitive genome data between Toshiba Life Science Analysis Center and Tohoku Medical Megabank Organization over 7 km using a Toshiba QKD system; further trials demonstrated quantum cryptography communication with speeds exceeding 10 Mbps and real-time transmission of whole-genome sequence data with a one-time pad method. [73]
Spain	QKD-security for patient data, remote assistance and surgery in hospitals in Madrid, emphasizing secure transfer of large health databases and the integration of emerging technologies, enabled by 5G networks, for remote medical assistance and surgery (ID Qquantique and Toshiba involved). [73]
Austria	Securing sensitive medical data at rest and in transit in Graz, where Toshiba deployed QKD for medical backup between the Medical University of Graz and the Institute of Pathology, achieving secure bit rates exceeding 2 Mbit/s over fiber links spanning 20 km (also fragmentiX and AIT is involved). [73]
South Korea	Quantum-safe security solution applied at Korea University's K-Bio Center for the first cloud-based medical system in South Korea, with QKD installed at Keimyung University Dongsan Hospital to protect personal information used by autonomous robots. [87]

Conclusions

The potential for QKD in the medical sector is substantial, particularly for high security laboratories that analyze genome data or handle information about pathogens. However, successful implementation will require overcoming significant technical challenges, addressing market readiness, and a corresponding regulatory framework. As healthcare organizations become more aware of the vulnerabilities associated with traditional encryption methods, the strategic adoption of QKD could lead to improved data security and enhanced patient care.

4.2.2.7 Banking and Finance

Banking and finance sector

- Cybersecurity requirements are high in this sector due to the handling of sensitive financial and customer data, but adequate measures are often lacking.
- Regulations like NIS2 and the DORA mandate have improved IT security for financial institutions.
- Market potential for QKD is medium in the short term, with high long-term security needs.
- Demonstration projects show growing interest in QKD, but the sector is generally cautious about implementation.

Overview of the sector

The banking industry deals with sensitive data such as transactions, customer data and proprietary information [55] that must be protected with highly secure solutions. The level of digitalization in the banking and financial sector is high and the awareness of cybersecurity risks is increasing, while sufficient security systems are not always implemented. According to KPMG's survey of bankers in 2023, 81% of respondents expect an increase in cybersecurity threats, supported by rising tensions due to the Russia-Ukraine war and its economic sanctions, while 43% recognize that their banks may not be adequately equipped to protect customers. [88] IBM security estimated that the financial sector incurred the second-highest cost for a data breach (5.9 million USD) in 2023, after the healthcare sector. [85] For these reasons, some literature reviews identify banking and finance as one of the potentially important application areas for QKD implementation. [55]

Framework conditions of the sector

According to IT-SiG 2.0 and the NIS2 Directive, banks and insurance companies are also classified as critical infrastructure (KRITIS) and must ensure comprehensive security measures to protect their IT infrastructure. [89] In addition to these two laws, the EU *Digital Operational Resilience Act* (DORA), which specifically addresses the financial sector, has been in force since January 2025. Its aim is to create a standardized basis for ICT security in the financial sector to prevent cyber-attacks and ensure the availability of financial services.

Both instruments aim to regulate IT security in the financial sector in a uniform manner and to increase IT security in general against the background of new cyber risks, e.g., through increased digitalization and the use of AI. The planned measures overlap to some extent and there is a lack of clarity in the sector as to when the requirements of NIS2 and DORA should be implemented. [90] Additionally, DORA applies not only to banks and insurance companies but also to IT service providers working for these companies, creating a new oversight regime for critical third-party providers and expanding the regulatory framework. [91]

The central requirements of DORA can be divided into five subject areas:

- Information security management and ICT risk management,
- handling, classifying and reporting ICT-related incidents,
- testing of digital operational resilience,
- management of ICT third party risk, and
- exchange of information and findings. [92]

The DORA requirements are not new to financial institutions. Before DORA, there was no directly comparable law, but there were BAIT (Bankaufsichtliche Anforderungen an die IT), the banking supervisory requirements for IT, issued by the German Federal Financial Supervisory Authority (BaFin). These were only administrative letters ("Verwaltungsschreiben"), but compliance was mandatory for financial institutions. Companies that have implemented BAIT have already fulfilled a large part of the DORA requirements. [93]

IT service providers classified as "critical" are also directly supervised by one of the European supervisory authorities, thus ensuring centralized EU supervision of these critical service providers. By transferring supervision to the European authorities, DORA adds an extra level of supervision in this sector, while NIS2 supervision remains at the national level. [90]

Status Quo

To address the emerging threats of quantum computing, a growing number of sector-specific white papers/position papers are being issued by various organizations, such as the World Economic Forum, [94] the German Banking Industry Committee [95] and UK Finance [96]. However, the focus of such recommendations is usually on migrating to PQC. In some cases, QKD is mentioned as a possible solution, (e.g., Monetary Authority of Singapore), [97] but there is no clear statement on where the technology should be applied.

Sectoral experts consider the use of QKD to be optional but not mandatory, even though they believe that QKD technology should be further developed in case PQC, and other classical solutions fail. As a prominent example, JP Morgan Chase declares that they will pursue a "dual remediation strategy", incorporating both PQC and QKD for its quantum-secure network. [98] Several other banks are exploring QKD in demonstration projects as well (examples see below).

Possible scenarios and added values of QKD use in the sector

Use case 1: Inter- and Intra-bank transfers

Financial transactions within banks and also in between different banks are critically important tasks of banks and require a high level of security. For banks, the secure storage and handling of this data is their business capital, for which they can be held partially liable. Therefore, classical cryptographic methods will eventually not be sufficiently secure anymore. QKD could offer to encrypt this critical information.

Use case 2: General intra-bank communication

Beyond financial transactions, all communication between branches and sites of a bank should ideally be kept confidential, as they might contain information on customers, financial records or other confidential financial data. Securing all communication between banking sites would however mean to equip hundreds to thousands of sites per bank and country with QKD devices and infrastructure. This is currently much too expensive to be even considered by banks. With decreasing costs of QKD devices and infrastructure, however, this could become a use case in the long-term future.

Use case 3: QKD and Cryptocurrencies/Blockchain

Cryptocurrencies are blockchain technologies that currently rely on mathematical algorithms for security. With the development of quantum computers, the security of this technology could be thus at risk. While certain information on the blockchain can finally be read by others in the network, during the process the data must stay confidential. To keep this data secure even when quantum computers become powerful enough to decrypt classical encryption algorithms, QKD could be used, as discussed in a white paper from Toshiba. [99]

Assessment of the banking and finance sector for QKD adoption

The assessment of the banking and finance sector for the implementation of QKD depends on various aspects that are discussed in this paragraph and is summarized in Table 2.

1) Market and economic aspects

The market demand in the banking sector depends on how much importance is placed on security in the sector, how high the costs are, and what QKD has to offer. In the medium term, banks are likely to implement QKD only for highly confidential data and according to experts rather as a service and not investing in the systems themselves. Some banks could soon become frontrunners by starting to implement QKD.

In the long term, when cost-effectiveness and miniaturization are achieved, the banking sector has the potential to become a heavy user of QKD. Considering the number of bank sites, this could generate a significant market. Therefore, in the medium term the market size is assessed to be medium, in the long term as high.

2) Financial capability of the sector

The financial capability of the banking and finance sector can be considered high. On the other hand, banks tend to use their money to invest and make more money. Thus, although money is not the limiting factor in the banking sector, the willingness to spend it for QKD might be – at least as long as the requirement for security do not justify it.

3) Need/required level of security

Although the data is not as sensitive as government or military data, financial data is very sensitive information and thus requires a high level of security. Additionally, banks are built on trust, i.e. if customers do not trust the banks to handle their money securely, they will change bank.

4) Urgency (long-term security)

The urgency for a transition to quantum-safe cryptography is medium to high. Depending on the jurisdiction, the required data retention times are typically five to ten years. However, customer data in particular should be kept confidential for much longer than that.

5) Transition speed

The transition speed in the banking sector was rated as medium by experts. This view combines two aspects. First, the sector is typically hesitant to change currently implemented and working systems and some currently implemented systems are, according to experts, already rather outdated. Second, the transition speed could be high (at least compared to the public sector), if there is great urgency to implement a novel technology, due to regulatory requirements or considerable cybersecurity threats.

6) Technological feasibility

Stability and robustness are key requirements for banks and the finance sectors, as the services they provide need to be extremely reliable. As yet, not all QKD systems show a high level of maturity and robustness. For larger scale adoption of QKD in the financial sector, the costs for the system and infrastructure need to be reduced. Scaling and miniaturization (ideally towards Small Form-factor Pluggable SFP transceivers) are two aspects that are likely to lead to cost and price reductions. In addition, high-frequency trading needs to have not only a high level of security but also low latency. When considering worldwide trading, also the distance limitations have to be considered and satellite QKD possibly need to be involved.

7) Framework conditions

Regulatory requirements in the financial sector are defined by NIS2 [12] and DORA [100]. Currently, neither of these regulations define any specific requirement on the use of quantum-secure cryptography. Since, according to experts' opinions, many banks will only do what the regulations require them to, the implementation of QKD can be expected to be slow in the near future. Additionally, as long as QKD devices are not certified and their security is not proven by third parties, their added security is based on trust. A certification and increased awareness of the quantum computer threat could increase the market opportunities for QKD in the financial sector.

Table 10: Summary of the expert's assessment of the banking and finance sector:

Market potential (medium-term)	**Medium to high**
Financial capability of the sector (willingness to pay for security)	**High**
Need/required level of security	**High**
Urgency (long-term criticality of data)	**Medium to high**
Transition speed in the sector	**Medium**

Source: Workshop

Examples of demonstration projects

The table below summarizes examples of demonstration projects all over the world. Most of them tried to demonstrate point-to-point QKD connection between two separate sites, (e.g., data centers) located at a relatively short distance apart (up to 100 km). Several projects also mention block chain applications as part of the missions of the project.

Table 11: Examples of QKD demonstration projects in the banking/finance sector:

Country	Description
Austria	The first-QKD secured bank-transfer between the headquarters of an Austrian bank and the Vienna City Hall, using entanglement-based QKD. [101]
China	People's Bank of China Urumqi Central Sub-branch Star-Ground integrated Quantum Communication Application Project [102]
U.S.	QuantumXChange demonstrated Toshiba's QKD multiplexing system, connecting the data center in the front office and that in the back office via a 32 km dark fiber [103]
Netherlands	The Dutch bank (ABN AMRO) announced a partnership, which is actively developing MDI-QKD (Project SeQure with QuTech) [104]
Switzerland	ID Quantique and Mt Pelerin start testing its solution to secure crypto assets on block chains, which combines QKD, one-time pad and secret sharing schemes. [105]
USA	JP Morgan Chase, Toshiba and Ciena demonstrated QKD securing a mission-critical blockchain application. The optical channel with 800 Gbps was established at distances up to 100km. [106]
Denmark	The research team successfully transferred data between two of Danske Bank's computers that simulate data centers, via CV-QKD. [107]

Japan	Nomura Holdings Inc. and project partners jointly tested low latency data transmission with QKD for large-volume financial transaction data [108]
United Kingdom	HSBC joined the UK's Quantum Secure Metro Network. The bank will trial the test data transmission between the global headquarters and a data center, 62 km away. [109]
Singapore	The Monetary Authority of Singapore (MAS), several banks (HSBC, DBS, OCBC, UOB), the network provider SPTel and the technology provider SpeQtral have signed a memorandum of understanding to test QKD in the financial sector and carry out experiments. [110]

Conclusions

The banking and financial sector represents a promising sector for the adoption of QKD. While banks are often rather conservative in implementing new technologies and tend to use their financial means rather to increase money than to invest in security infrastructure, their business is based on customer trust. With increasing cybersecurity threats, they will need to move towards quantum secure cryptography and QKD could represent added value within this assurance of trust.

4.2.2.9 Industry

Industry sector

- Since the need for secure communication and the criticality of the data are rather low, the rapid market penetration is hindered.
- So far only slow advances by individual industry players.
- Especially high initial costs for QKD technology serve as a barrier.
- But the industry could benefit from the fact that not everything has to be regulated and certified.

Overview of the sector

The industry sector encompasses various domains, including manufacturing, automotive and pharmaceuticals. These fields are increasingly reliant on secure communication to protect sensitive data and maintain operational integrity. As industries become more digitized and interconnected, the need for robust security solutions has become paramount.

Framework conditions of the sector

Manufacturing has not previously been a critical infrastructure, but due to the current geopolitical situation, the security of supply chains and the security of the supply of critical components is now an important issue in parts of the manufacturing industry, too.

According to a recent Bitkom study, [111] the greatest cyber risks in industry are digital theft of business data, including customer data, digital sabotage of information and production systems or operational processes and spying on e-mail, messenger, video calls or similar forms of communication.

The importance of cybersecurity is underlined by the fact that two-thirds of companies surveyed said that cyberattacks threatened their very existence. As a result, the willingness to invest in cybersecurity has increased, with the proportion of IT budgets allocated to security rising from 9% to 17% over the past three years, but it is still at a comparatively low level. [111]

Depending on what is being produced and the size of the business, companies must also comply with various legal requirements relating to IT security, mainly in accordance with three key EU directives:

- The EU Machinery Directive (EU) 2023/1230 requires the design and construction of machinery to comply with current standards, including considerations for digitalization and cybersecurity. The requirements for machine connections to external devices or the Internet do not pose security risks. [112]
- The Cyber Resilience Act (CRA) sets requirements for products with digital elements to ensure cybersecurity throughout their lifecycle, including software updates. It aims to protect end users and businesses from products with inadequate IT security features. Most obligations will apply from 11 December 2027.
- The NIS-2 directive categorizes manufacturing companies as “important facilities” based on their size and specific industry sectors. NIS2 specifically mentions medical device manufacturing, IT equipment and electronics, mechanical engineering, motor vehicle manufacturing (including parts), food manufacturing and chemical production and trade. [35]

The exact provisions as to when a company counts as a critical infrastructure company are listed at "Openkritis.de". [35]

Failure to comply with these regulations can result in fines from the EU, with the CRA imposing penalties of up to 15 million EUR or 2.5% of annual turnover. Therefore, implementing a comprehensive cybersecurity strategy is essential, encompassing technical measures, securing business processes, and raising employee awareness.

Standards play an important role in the industrial sector. According to TÜV Nord, [113] IEC 62443 is the primary standard for IT security in this area and is internationally recognized for compliance in process and automation industries. It serves as a central certification standard for Industry 4.0 and as a possible benchmark for compliance with the Industrial Safety Ordinance ("Betriebssicherheitsverordnung") and the Product Safety Act ("Produktsicherheitsgesetz"). [114]

Status Quo

Currently, QKD is emerging within the industry sector, with several internal projects and research initiatives underway. While there is growing interest in QKD among organizations, widespread adoption is unlikely in the short-term future due to technical, financial and regulatory challenges. Industries typically rely on traditional encryption methods, potentially transitioning slowly to PQC, which in the short and medium term could represent the preferred quantum-secure cryptography method in this sector.

Possible scenarios and added value of QKD use in the sector

Use Case 1: Plant-to-plant communication

Communication between different production plants can be particularly important for manufacturers with different production plants, but also to be able to communicate with other companies along the supply chain. This also protects data transfer between manufacturers and suppliers from unauthorized access, securing corporate IP, research results or process data. Manufacturing industry, but also other industries, such as the pharmaceutical industry can benefit from this use case. Distance between these locations varies strongly and will be in many cases more than 100 km. So far, there is no suitable infrastructure. It is also difficult to integrate everything into existing networks and their corporate communication systems and flows.

Use Case 2: Intra-plant communication

QKD could be used to secure communication channels for IoT devices used in smart manufacturing, protecting sensitive operational data within a plant. Due to digitalization factories becoming more and more networked, they can no longer be operated as isolated systems. Up until now, in most of the factories worldwide no dark fiber is available for QKD implementation, on the other hand the distances are very short. Free-space QKD could be an approach to connect mobile devices. However, a combined implementation of PCQ (mobile devices) and hybrid PQC/QKD solutions seems to be more likely.

Use Case 3: Vehicle-to-vehicle communication

QKD could provide secure channels for communication between autonomous vehicles, enhancing safety, data integrity and ensuring their safe operation. This use case is for the distant future, as no clear concept is yet apparent for how the key transfer to the vehicles should be carried out and no timeline for the market approval and the roll-out of autonomous cars is known. One approach could be so-called "key refueling stations", where a vehicle receives a new security key when refueling or charging, which the vehicle can then use again for a certain period of time. An on-road key

exchange seems technologically challenging and could only be solved over free-space or satellite QKD links. As the added value seems limited, PQC or QKD-key-refueling-stations are expected to be more promising.

Assessment of the industry sector for QKD adoption

1) Market and economic aspects

The market for QKD in the industry sector is still in its infancy and currently shows only a small potential for growth. Key players, including major automotive OEM, are beginning to explore QKD solutions as they recognize the importance of securing their data and business-critical IP. Early adoption of QKD can position companies as leaders in cybersecurity. As regulations tighten, QKD can help organizations meet compliance standards effectively. The economic feasibility of QKD will depend on further advancements in technology and especially on cost reductions. Today, the costs associated with QKD technology and infrastructure represent a barrier for their adoption. As long as the security of PQC is sufficient, cost-driven industrial actors see no increased need for QKD solutions. All in all, the market potential seems to be low to medium.

2) Financial capability of the sector

In many cases, the aspect of secure communication in the industry sector cannot be sold directly to customers. Therefore, most of the larger industry companies are not willing to pay money for QKD systems right now. Security is often seen as an add-on. However, experience shows that money is available in the event of an imminent threat.

3) Need/required level of security

Stored data, e.g., from cars or company staff are critical. Some of the production data and company IP are also critical, but a lot of the stored data is only of interest to direct competitors. However, there are also increasing requirements for the industry to invest in cybersecurity, (e.g., EU Cyber Resilience Act). Overall, the need can be assessed as moderate.

4) Urgency (long-term security)

The urgency varies greatly. Often, company data has to be stored and secured for around 10 years. Some personal data remains relevant for longer than that. In addition, there is company-specific IP, which is important for a company's competitiveness and future viability. Here, too, longer storage periods are important.

5) Transition speed

The transition speed in the industry sector varies because of the different branches and different use cases of the communication technology. Even if there are fewer regulatory hurdles and requirements compared to public sector, things tend to move rather slowly in industry. The reasons for this include costs, processes and manpower. Overall, the transition speed can be classified as medium.

6) Technological feasibility

So far, technical hurdles have prevented the roll-out of QKD systems. Limitations such as distance restrictions and the complexity of integrating QKD with existing systems can hinder deployment. To be widely adopted, QKD solutions must be scalable and more cost-effective in the industry sector, requiring advancements in miniaturization and production processes.

7) Framework conditions

The industry sector requires a limited supportive regulatory environment to facilitate the adoption of QKD. Nevertheless, certification would increase trust in the technology and thus might help to speed up adoption.

Table 12: Summary of the expert's assessment of the industry sector:

Market potential (medium-term)	**Low to Medium**
Financial capability of the sector (willingness to pay for security)	**Low to Medium**
Need/required level of security	**Medium**
Urgency (long-term criticality of data)	**Medium**
Transition speed in the sector	**Medium**

Source: Workshop

Examples of demonstration projects

So far, only a relatively small number of projects has been publicly announced in the industrial sector. However, some automotive manufacturers and other large corporate groups have cyber security departments that are looking into the subject of QKD and, in particular, if PQC is sufficient for their use cases or if PQC and QKD can be combined.

Conclusions

QKD presents opportunities for enhancing security in the industry sector. However, successful implementation hinges on overcoming technical challenges and addressing market readiness. As awareness of quantum threats grows and organizations seek to protect sensitive data, the adoption of QKD could become increasingly feasible, paving the way for innovation and leadership in cybersecurity.

4.2.2.10 QKD Services

QKD service sector

- QKD can enhance security in data centers and telecommunication but faces high infrastructure costs.
- Global (publicly funded) pilot projects show different opportunities for QKD services to improve data security amid rising cyber threats.
- Business models have not yet clearly emerged.
- It would make a big difference if existing infrastructure could be used for QKD instead of a separate (dark) fiber infrastructure.

In 2025, the adoption of QKD is still at an early development stage. QKD represents an option for greater security in communication and is not independent of the current solutions, but rather has to be integrated into existing procedures and systems. Consequently, there are various players involved and various options for services and business models conceivable. This section discusses the players and services of telecommunications providers that take care of the expansion of the (fiber) infrastructure and might offer encryption with their communication services (encryption as a service), to operators of the systems and service providers such as data centers or IT security system providers, which in turn offer various services such as data storage or secure data connections in the form of various business models to corporate and private customers, (e.g., key as a service, encryption as a service). We clustered all these players in this section under the term QKD Services. QKD service providers are active in all sectors, as they enable fundamental (technical) capabilities for the various use cases.

Overview of the sector

The expansion of the telecommunication infrastructure is relevant for the establishment of QKD. The global telecommunications market itself is in a state of growth. In addition to the expansion of mobile networks, (e.g., 5G), the expansion of fiber optics for both internet and television applications has accelerated in recent years.

The largest providers of telecommunications are often private companies, such as AT&T in the USA. In some countries, however, state-owned or partially state-owned companies operate the infrastructure, such as China Telecom. In addition, some regions have hybrid models in which state-owned and private providers cooperate. In addition to telecommunications operators, there are also companies that specialize in secure IT networks (e.g., Adva or Rohde & Schwarz). These can also be responsible for operating the networks in addition to the telecommunications operators.

The hardware for the systems is developed by technology companies (such as Toshiba) or by small and medium-sized enterprises and startups (e.g., ID Quantique, KEEQuant or Quantum Optics Jena). These companies currently sell a small number of devices, specifically for R&D and testing purposes.

The provision of infrastructure can be used by other sectors as a basis for their own applications and business models. A prominent example of the use of public fiber networks are data centers. Traditionally, data centers supported IT functions such as data storage, processing, and management. They also host applications, websites and cloud computing services. In the modern context, data centers provide the necessary infrastructure for big data analytics, machine learning and artificial intelligence. They can be either self-operated by organization that owns them or managed by

third-party providers. These providers have to ensure a secure and reliable environment for their own and customer data. [115]

Framework conditions for QKD service providers

Telecommunications companies, for example data center operators, provide critical infrastructure themselves or provide services to other companies and organizations covered by NIS2 and IT-SiG 2.0. As these laws aim to ensure the availability, integrity and confidentiality of critical infrastructures and to counteract any disruption or failure, companies in the IT and telecommunications sector must take appropriate protective measures, which include identifying vulnerabilities, implementing security measures and regularly reviewing systems. [116]

For companies in the telecommunications sector – as for companies and organizations of the other sectors analyzed here - it is crucial to know whether they are classified as critical infrastructure. The IT-SiG 2.0 specifies thresholds at which companies are classified as critical infrastructure providers. To illustrate the level of detail the law provides here, the criteria for telecommunications and data center providers are presented. The following thresholds apply to telecommunication providers:

- For access and transmission networks: from 100,000 subscribers.
- For IXP providers offering Internet Exchange Points (IXPs), peering, cloud and interconnection services, the threshold is explained by the economic and regional relevance of the IXP: Relevance is based on having approximately 100 connected autonomous systems (AS).
- The threshold value for DNS resolvers is based on the access network they serve. For DNS servers and TLD registries the threshold value is 100,000 subscribers in the connected access network and approx. 250,000 authoritative, delegated, managed domains.
- The threshold for data centers refers to the contractually agreed capacity and is a contractually agreed capacity of 3.5 MW.
- The thresholds for server farms and content delivery networks are 10,000 running physical instances on average per year and approximately 75,000 TB per year of delivered data volume.
- The thresholds for trust services are 500,000 qualified certificates (QeS) issued (OpenKritis, „IT und TK“). [35]

In addition to the IT-SiG 2.0 legislation, the European NIS2 regulation will also apply to IT and telecommunications companies. For telecommunications providers, NIS2 applies if they have more than 50 employees and a turnover of more than EUR 10 million. For qualified trust services, TLDs, and DNS providers, NIS2 applies regardless of size.

In the area of digital infrastructures, companies are often subject to double and multiple regulations. For example, telecommunications providers may also be subject to the DORA regulations if they have financial customers and/or are classified as a critical ICT third-party service provider under the DORA regulation.[7]

Telecommunications companies may also be subject to the German Telecommunications Act of 2021, which sets out its own IT security requirements in the “Catalog of Security Requirements 2.0.” (OpenKritis, "TK-Sicherheitskatalog"). [35] These overlap significantly with IT-SiG 2.0 and NIS2.

Various practices have been established in the telecommunications and IT industry to improve cybersecurity. One such practice is the implementation of information security management systems (ISMS) in accordance with ISO 27001 or the BSI “IT-Grundschutz”. [117] The BSI lists the companies certified to these standards on a dedicated website, [118] including for example Vodafone Cloud & Security Germany.

[7] In which fields the regulations overlap and where they complement each other is described in detail on the website www.openkritis.de.

Status Quo

Unlike in other areas of the telecommunication market, further network expansion for QKD cannot be financed with initial investments from first movers and early adopters. This is due to the very high investment costs (especially of dark fibers) and slow cycles of development. A current obstacle to QKD is that the first users would have to bear the high costs themselves.

Currently, QKD still requires dark fibers. Research is being conducted into using normal optical fibers as well or sharing existing fiber-optic cables for the use of QKD. The multiple use of fiber optics has some disadvantages and is not yet technically possible but is being investigated. For this reason, a new separate infrastructure is still unavoidable. The alternative of communication via satellite requires even greater investment (especially for potential private operators). [119] Furthermore, the development status of satellite-based systems lags behind that of fiber-based systems. For this reason, the expansion of a QKD infrastructure is currently mostly taking place within the framework of public research projects (e.g., EuroQCI or OpenQKD) and is supported by telecommunications providers. In addition, telecommunication providers have their own rather small networks. These are, among other things, used for validation of first QKD hardware solutions and for marketing purposes. The EU is planning to further promote the expansion of QKD infrastructure.

In Germany and also in other European countries, (e.g., Italy, the Czech Republic and Poland) dark fiber infrastructure has been installed, particularly as a QKD testbed infrastructure. In Germany, there are various testbed infrastructures in place adding up to several hundred kilometers. [120] Other countries are already way ahead having already installed large implementation networks, such as South Korea and China, (e.g., the Beijing Shanghai communication network with a length of over 2000 km [39]).

Telecommunications operators and service providers such as Telefónica, China Telecom and British Telecom are currently exploring how QKD systems could be integrated with existing fiber infrastructures to secure data transfer across their networks. [55]

Hardware manufacturers are often also part of the research projects and can thus sell their hardware to the testbeds for testing purposes. There are several commercially available systems, but the quantities are still low. Although systems have also been sold outside the publicly funded testbeds, these are often orders for early adopters in order to test the technology within the company. IT service providers are also looking at QKD technology and testing the extent to which they can integrate the systems into their services.

Since QKD is still in its infancy, there are no established QKD services available in Europe, yet. However, data center operations are seen as one of the great opportunities for a concrete application of QKD services. Data centers play a crucial role in storing and processing vast amounts of data, including private sensitive information, government data, and critical office information. As organizations increasingly rely on cloud and data centers for data backup, storage, and recovery, ensuring data privacy and security has become paramount. [55] Currently, there are around 7,500 data centers worldwide, highlighting the importance of database interconnection. [119] Today, the supply chain is lacking the ability to equip these data centers with QKD across the board. However large private data center providers are currently working on their backbone QKD network. [121] In cloud networks, databases are often physically distant from data generation points and may adopt distributed architectures to enhance efficiency and security. [119] Data centers not only store and process large volumes of data but also transmit data between servers, making them vulnerable to hackers. [72]

Possible scenarios and added value of QKD for service providers

Use Case 1: QKD communication network as a service

In addition to providing established communication channels from the point of view of telecommunications providers, a business model is to provide and operate QKD infrastructure in order to offer other industries, (e.g., data centers, but also other industries such as finance, etc.) a network as a service. [122] Even though it has currently still only been implemented within a few pilot projects due to the high infrastructure costs, its importance could increase in the coming years as prices are expected to fall. Another problem here is that the infrastructure provider must be trustworthy.

In addition to the provision of QKD infrastructure, QKD can also be offered as a service. [123] Various companies are currently establishing themselves in the emerging QKD market. They offer different services. In addition to the hardware producers themselves, data encryption (key as a service/encryption as a service) can also be offered as a service. Additionally, complete transmission (QKD as a service) could be offered. Then a company takes care of the hardware provision and encryption of the data to be transmitted on behalf of their customer. In most cases, a data center operator must be involved in the services (in-house or external). Either this is simultaneously the operator of the QKD service, or this service is taken over by a second operator.

Use Case 2: Secure communication and data exchange between data centers

The publicly accessible fiber infrastructure developed by telecommunication providers making data centers a prime candidate of QKD technology. [119] Even with further advancements in fiber-optics based QKD, secret keys can be generated using standard telecommunication infrastructure (multiplexing). QKD can be a promising solution for enhancing the security of data center interconnection. [55]

Common distances between data centers are typically tens of kilometers, well within the range for DV-QKD or CV-QKD fiber communication. [119] The installation and commissioning of such a geographically close data pair, (e.g., for back-ups) is currently still very expensive and would typically cost a few hundred thousand euros.

By leveraging QKD, data centers can significantly enhance their security infrastructure, ensuring data remains protected from emerging quantum threats while maintaining high standards of privacy and reliability.

Use Case 3: Secure communication and data exchange between data center and customer

In addition to internal data security, another QKD application could be to make communication with the end customer secure. Offering secure data storage, for example in the form of a cloud service, is an important business model for large tech companies such as AWS. The different forms of customer access to the cloud pose a challenge that has not yet been fully resolved from a technical point of view, (e.g., access from a smartphone). [119] Initially, there will be restrictions on the access options for QKD-based connection to data centers or cloud solutions. Services must be able to provide the data reliably at any time and transmit it securely back to the customer.

Assessment of QKD service adoption

1) Market and economic aspects

The telecommunications market is experiencing rapid growth, driven by the expansion of mobile and fiber-optic networks, also in many developing countries worldwide. This presents a significant opportunity for QKD, as the increased focus on security will most likely lead to greater demand for

innovative solutions. The demand for advanced security solutions is expected to rise, particularly in response to growing concerns surrounding cybersecurity.

As it is still in its infancy however, potential users typically do not want to invest so much in advance. This is mainly because it has not yet been decided, for example, how quickly QKD will spread and become established. There are no clear business models as yet. At the same time this leaves opportunities to offer services with QKD. Even if experts see great potential, the specific opportunities are still unclear.

2) Financial capability of the sector

There are various players that can invest in infrastructure or data centers. These include telecommunications providers, but also large tech companies such as Alphabet, Meta or AWS. While tech companies can benefit from the investments directly themselves and are therefore more willing to finance them to advance their own strategic goals, the business model for telecommunications providers must be profitable. Overall, the financial capability of the sector is medium.

3) Need/required level of security

Based on the business case, data centers and telecommunications providers must guarantee a high level of security. At the same time, the actual criticality of the data which is saved with an external service is often rather moderate. If a company or institution has highly critical data, it usually manages and stores it itself.

4) Urgency (long-term security)

Since the data is often stored for others, the guarantee of long-term security is important. This is particularly evident in Europe and Asia.

5) Transition speed

Due to a lack of public regulation and flexible deployment and implementation options, the transition speed is generally high. Nevertheless, it often takes years for new technologies to be integrated into established networks. However, individual projects can be implemented in just a few weeks or months. Therefore, the transition speed is medium

6) Technological feasibility

The feasibility of implementing QKD is influenced by several factors. Many telecommunications providers will need to upgrade their infrastructure to facilitate the integration of QKD. Moreover, ensuring compatibility between QKD and existing encryption standards is crucial for its effective implementation. The ability to scale QKD solutions across multiple data centers and cloud environments will be essential for widespread adoption. Especially interconnectivity is of great importance. At the moment, the range and the costs are still major challenges. Many providers for data centers are currently relying on PQC solutions. This is partly because PQC will be needed for practical applications in the near future anyway , for example to establish a connection to a smartphone.

7) Framework conditions

As long as business models have not been established and the cost for QKD is still high, targeted political support is necessary to advance the adoption of QKD technology. Providing funding and incentives for research and development in QKD, as well as the corresponding infrastructure, would be beneficial for a fast network expansion. Establishing clear industry standards for QKD would facilitate implementation and ensure interoperability among systems. Furthermore, increasing awareness of the advantages of QKD will promote broader acceptance and integration into existing infrastructures. The expansion of the infrastructure can then lead to falling prices and thus to more attractive services on offer at data centers. On the other hand, demand is not as high as in strictly state-regulated areas.

Table 13: Summary of expert's assessment for QKD services:

Market potential (medium-term)	**High**
Financial capability of the sector (willingness to pay for security)	**Medium**
Need/required level of security	**High**
Urgency (long-term criticality of data)	**High**
Transition speed in the sector	**Medium**

Source: Workshop

Examples of demonstration projects

Various pilot projects are currently underway, particularly in Europe but also worldwide, involving infrastructure rollouts and the simultaneous testing of data center use cases.

Table 14: Examples of QKD demonstration for QKD services:

Country	Description
Germany	A network is being set up under the leadership of Deutsche Telekom to see how it can integrate different QKD systems and how this can be integrated into the network. The project can be seen as a blueprint for possible business models. [122]
Spain	QKD as a cloud service in Madrid to link cloud data centers, providing secret keys as a service for client applications (ID Qquantique, Toshiba involved). [73]
China	The Beijing-Shanghai QKD network secures data backups between data centers in Beijing and Shanghai. [39]
Netherlands	A QKD link secures data transfer between Siemens data centers in The Hague and Zoetermeer, with KPN implementing end-to-end QKD between its data centers. [124]
Greece	QKD-interconnected cloud data centers in Athens enhance data security, employing encryption and new crypto acceleration devices for better performance (ID Qquantique, Toshiba involved). [73]
South Korea	SK Telecom and Equinix build a QKD environment in Equinix's SL1 data center in Seoul, providing quantum cryptography protection for private enterprise networks on subscription. [125]

Conclusions

Even if no clear business models have yet been established and there is no supply chain for a QKD service offering, QKD service providers will play a crucial role there. In the long term, it can be assumed that QKD can play a crucial role in individual sectors as an additional security layer. Therefore, the integration of Quantum Key Distribution (QKD) into telecommunications and data center infrastructures presents a significant opportunity to enhance data security and privacy through various QKD service providers, to counter the increasing threats from cyber-attacks while supporting the growth of innovative service models across various sectors. It is important that interfaces or hardware requirements, for example, are defined promptly to enable QKD to spread quickly.

4.3 Beyond QKD Applications

Most of the activities in quantum communication research and development are currently focused on QKD with the goal to optimize technologies, develop new technology variants or test their implementation. This is not surprising, as QKD is a technology that is already being commercialized and expected to be adopted in the next few years. However, quantum communication technologies are certainly not limited to QKD. Further technologies "beyond QKD" are being researched and developed, even though these are generally not yet as mature as QKD. Moreover, in many cases the path towards commercialization or the added value is intangible at the current state of research. Nevertheless, in this section we want to give insights into quantum communication technologies beyond QKD. We will provide an overview of some of the most important trends and applications, without claiming to be exhaustive. For systematic overviews, please refer to recent review papers on this topic, such as from Bozzio et al. [126] First, we will introduce the characteristics that most of the quantum communication technologies beyond QKD share. This will be followed by a discussion of selected technologies.

Many quantum communication technologies, also those beyond QKD, focus on applications in cryptography or promise the realization of the quantum equivalents of cryptographic primitives. [126] Only a few technologies that are based on the transport of quantum states are motivated instead by the enhancement of the capabilities of other quantum technologies. Most of these technologies are enabled by the distribution of entangled qubits and therefore require the development of quantum repeaters in order to be implemented over longer distances or to enable a distribution via satellite. In some use cases, the entangled states have to be stored, calling for (entanglement-maintaining) quantum memories. The degree of entanglement required varies throughout the different technologies. Many of the technologies are being discussed under the umbrella term quantum information network or "Quantum Internet" (see also section 5.2). Nevertheless, it should be mentioned that while entanglement distribution will enable many new applications, not all the quantum communication applications that go "beyond QKD" and are discussed in this chapter will require entanglement.

4.3.1 Technology: Entanglement Distribution Network

As entangled qubits can serve as a resource for various applications, the distribution of entangled states in a robust and efficient way is highly desired. The technological approaches span over different kinds of entangled states, their generation, transport and storage.

The most basic entangled state is based on two qubits, often called an Einstein-Podolsky-Rosen Pair (EPR). [127] One example is the polarization entanglement of two photons, resulting in a correlation of the polarization state (both photons can be in the same or opposite polarization state). The state of each individual photon is only determined when it is measured. But more complex entangled states have been demonstrated or investigated theoretically. The most prominent is the Greenberger-Horne-Zeilinger state, [128, 129] as postulated for a three-particle entanglement in 1990 [130]and experimentally observed in 1999 [131]. For larger numbers of particles different types of entanglement states can be conceived, such as graph states [132], cluster states (e.g., [133]) or W-states [134]. In general, the larger the degree of entanglement and the number of particles, the more complex the challenge in generating and maintaining the states.

Entangled photon pairs can be generated by spontaneous parametric down conversion (SPDC) in a well-investigated manner (e.g., [135]), where one photon is converted into a pair of entangled photons. Another non-linear option is based on spontaneous four wave mixing (FWM), where the combination of two incoming photons generates the emission of two entangled photons. Entanglement can, however, be generated in multiple other ways, such as utilizing the path degree of

freedom for photons in an optical set up or by combining multiple identical photon sources. [136] However, the photons to be entangled do not have to come from a common source, as demonstrated by the entanglement swapping experiments of Zeilingers group in 1998. [137] Other approaches are needed to generate entanglement for other types of qubits, such as quantum processors for trapped ions. [138]

The transport of an entangled photon uses, in general, identical technologies as entanglement-based QKD. Over short distances, entangled photons can be sent via fibers or free-space optical links, while for longer distances entanglement distribution via satellite or entanglement swapping in quantum repeaters is required. Entanglement swapping can be realized by performing a Bell-state measurement on two photons of two separate entangled photon pairs, which can lead to an entanglement of the two remaining photons, which previously had no interaction with each other. This process can be used to entangle photons and finally stationary quantum states over large distances.

As the transport of entanglement over larger distances is best achieved using photons, but storing and working with information in stationary qubits is more practical, interfaces between stationary qubits and photons are required, if they are to be entangled. This can be realized by entangling the stationary qubit with a flying qubit [139], as demonstrated in the case of trapped atoms [140], trapped ions [141], color centers in diamond [142], or quantum dots [143] using different techniques.

This light-matter entanglement is also a main component for realizing entanglement-maintaining quantum memories that can store the entanglement over time spans. Short time periods of less than one second can be valuable for enabling the first generation of memory-based quantum repeaters, but longer time periods are desired to open a door to more exotic applications that utilize entanglement as a resource. As the lifetime of quantum memories has been extended in the past years from nanoseconds (e.g., [144]) to milliseconds [145], there are some exciting developments in this field, but the future challenges are still quite significant.

The technological requirements for entanglement distribution are therefore manifold and are unlikely to be met in a meaningful way in the short to medium term. However, a closer look at the desired tasks and applications are necessary to get a more complete picture.

4.3.2 Applications: Cryptography

QKD promises a physically secure transfer of a key over a point-to-point link and, subsequently, networks with multiple nodes. In this way, QKD can be used to share secrets between several different parties which can only be reconstructed, when a critical number of parties combine their information. This would be a quantum-enhanced version of the classical **secret sharing** approach, known as Shamir-Secret-Sharing. [146] This quantum-enhanced version was discussed by Hillery et al. [147] Potential applications for this secret sharing can be found in use cases in which authentications are only granted, when a majority of the people in charge agree (an example which illustrates this is access to nuclear codes, which may require the permission of more than one person). Similarly, a technique is investigated that enables the sharing of quantum secrets, known as the Cleve-Gottesman-Lo-scheme. [148] In this approach, a quantum state is divided into a number of shares, which are distributed between different parties. The potential of this approach is obviously closely connected to the value of quantum information and will therefore only add value if technologies based on quantum information are available. Therefore, nothing significant is expected in the short term, but there could be potential in the long term.

The same applies to approaches that promise to open a path towards **blind quantum computing**: When quantum computers become more powerful, they are expected to enable a wide range of applications based on simulations, optimization problems and many further quantum algorithms.

As long as powerful quantum computers remain expensive and dependent on respective infrastructures (comparable to current conventional supercomputers), the interest in accessing quantum computers as a client via a service provider (quantum computing as a service) will increase. However, in many cases the client might be interested in keeping the exact algorithm and its results hidden from the owner/provider of the quantum computer. This "blind quantum computing" can be implemented using different approaches. The first implementation of protecting the privacy of a computation was reported in 2012. [149] It was based on feeding a measurement-based quantum computer with entangled cluster states. Nevertheless, a simpler approach for a similar purpose was developed by the company VeriQloud based on their product "QLine". [150] The main idea behind QLine is the transfer of a quantum state through several nodes (Charlies), with each node applying or not applying a rotation to the quantum state, initially only known to the node itself. When the QLine is used for QKD, all but two nodes on the line announce publicly their applied rotations (or in the case of the start or the end node, the initial state or the measured result, respectively). By this, the two remaining nodes become Alice and Bob, providing a direct link to any two nodes on this collaborative QLine. Similarly, this approach can be used to anonymize the state of a qubit sent to a quantum computer. However, the approaches are based on photonic qubits and require the respective interfaces to the local qubits of the respective quantum computing platforms.

The birth of the research field quantum communication is often attributed to the paper of Charles Bennett and Gilles Brassard in 1984 with the development of the QKD algorithm known as BB84, which is still being used in commercial QKD systems. [151] However, BB84 is based on two thought experiments by Stephen Wiesner in the seventies, which he published finally in 1983. [152] One thought experiment was the invention of "quantum money", where the no-cloning theorem for quantum states is used to realize money that cannot be copied. Even though the original idea cannot be practically realized, it paved the way for many different variants today. These approaches fall into different categories: while the idea of **public-key quantum money** (e.g., Farhi et al. [153]) includes the quantum equivalent of banknotes, i.e., unforgeable and unclonable tokens that can be verified (in theory) by everyone, **private-key quantum money** (e.g., Aaronson et al. [154]) presupposes trusted parties (such as banks) and would be comparable to the exchange of tokens, as in the case of credit cards. So far, most approaches to quantum money either rely on some kind of quantum memory or space-time constraints (requiring trusted agents) (e.g., Kent et al. [155]) or are restricted to narrow use cases, such as online-digital payments to reduce the technological requirements. However, quantum money is only one application from the broader field of **quantum tokens**. Many different approaches to quantum tokens are being investigated: e.g. the BMBF defined the search for quantum tokens as the Grand Challenge of Quantum Communication, which is currently being tackled in six different projects. [156] An example of the implementation of quantum tokens are physically unclonable functions (PUFs). PUFs can already be created using classical cryptography and are based on functions that are too complex to be cloned and can therefore be used as a fingerprint for authentication, (e.g., in car keys). Their quantum counterparts (QPUFs) are currently being investigated. It is unlikely that practical quantum tokens will be technologically implemented and scaled up in the short or medium term. Nonetheless, quantum tokens are a promising technology, especially as they could represent one way to enable quantum authentication processes. Further approaches to quantum authentication are another strongly anticipated field of research.

Further quantum tasks that could be enabled by quantum communication are the quantum counterparts of classical cryptographic primitives that sometimes have no solution. The simplest example is probably the **quantum coin flip**, which is a way to distribute randomness between two separated parties without giving them the opportunity to cheat. [157] The protocol is closely related to the BB84 protocol for QKD and does not require entanglement. [151] Quantum coin flipping can be used to conduct a **quantum leadership election**, in which a leader is selected from several

different parties across a distance – a straight-forward implementation would be to eliminate parties by a quantum coin flip until the leader is elected. [158] No classical solution for such an election process is possible. Finally, the quantum solution to the related **byzantine agreement** should be mentioned, in which parties agree on a decision over a process that cannot be compromised by cheating (neither by actors internal or external to the communication). [159]

A more complete and in-depth discussion of quantum cryptographic primitives is provided in the review publication of Bozzio et al. [126]

4.3.3 Applications: Performance-Enhancement

The second major group of quantum communication applications, often cited as motivation for developing these technologies, are approaches to enhance the performance of complementary technologies.

Most prominently, the "quantum internet" aims for the connection of quantum computers and various other devices such as quantum sensors and quantum communication devices, comparable to connections within the classical internet. Some experts are carful with the term "quantum internet", as it might create too high expectations in functionalities known from the classical internet. In the foreseeable future, comparable functionalities are, however, not conceivable and the term is often rather used for "network of quantum networks". This connection of quantum computers over a quantum channel would allow for **distributed quantum computing** across a distance. Nevertheless, the first relevant applications are expected to be implemented over very short distances to connect different quantum computing chips at the same location. This parallel computing, which is comparable to the classical counterpart (multiple processors calculating in parallel in most commercial computers) is anticipated by manufacturers such as IBM to speed up the development of next-generation capabilities of quantum computers. [160] This will become more and more relevant, as the integration of a larger number of qubits on a single chip becomes continuously more complicated. Whether this combination of computer subsystems to form a quantum computer system capable of parallel computing should be regarded as a quantum communication technology is, however, merely a philosophical question. More obvious is the case for applications where quantum computers are accessed or combined across a distance: e.g., if the client only has direct access to very limited capabilities or complex computations, or calculations that require multiple large quantum computers. The implementation of these use cases is technically very demanding, while the added value compared to communicating the desired algorithm via a classical channel and performing the calculation entirely on a single quantum computer seems limited. Therefore, the short-term relevance of distributed quantum computing across a distance is expected to be low, due to the current technical limits and the unclear added value. Nevertheless, there are many different research activities around distributed quantum computing and progress is being made on the required qubit-photon interfaces (e.g., [161]). This depends heavily on the underlying quantum computing platform, of course.

The compliment approach for enhancing quantum technologies with distributing entanglement is **distributed quantum sensing**. Classical sensor networks have become more and more relevant to monitor larger areas or to combine the measurement of different variables to get a more complete picture of the underlying tasks. When the information of classical sensors is combined to enable these overarching insights, the measurement readings of the individual sensors must be transferred to a central node, where they are analyzed, (e.g., averaged, correlated, etc.). Depending on the number of sensors and the amount of data, this process is known to be quite expensive in terms of computational costs and data transfer capacities. While this process can also be applied to quantum sensors, they do offer a complementary approach for generating collaborative measurement results: by entangling the different quantum sensors, joint measurements can be performed. This

provides the advantage of a direct implementation of the operation, (e.g., averaging, subtraction, correlation, etc.) resulting in a single measurement for the quantum sensor network. The potential to reduce the data transfer and the post-processing is promising in theory, however, only if the entanglement distribution can be performed with low cost and effort. Even though this is not expected in the next few years, research projects are being undertaken to demonstrate the potential of distributed quantum sensing. A clear path towards first applications has not yet become clearly visible.

Finally, we want to give an example for enhancing the performance of classical information technologies: **super dense coding**. A classical bit is the smallest unit of information that can be translated into the answer to a yes-or-no question (0 or 1). As quantum bits, however, can be in a superposition of both answers, they do carry in some sense more than this binary information – nevertheless, as bound by Holevo's theorem, [162] ultimately, only binary information can be extracted because the measurement projects the bit onto the measurement basis. However, if the two communicating parties pre-share entangled qubits, this resource can be used to encode two classical bits in one qubit. It requires Alice to perform one of four gate operations on her part of the Bell-pair, which is then sent to Bob who performs a measurement on both photons of the pair to extract the two bits of classical information. The concept was developed in the first papers of Wiesner and Bennett that started quantum communication research. [152] In theory, this concept can be understood as an approach to speed up classical communication, by enhancing the number of bits transferred via a single photon. However, the practical realization is limited by the number of single photons that can be successfully transferred and detected, as well as distributing and storing the entanglement. It is therefore not expected to be used for speeding up communication in relevant time frames. Furthermore, as this approach requires distributed entanglement, it can be used for cryptographically-secure coding solutions.

4.4 6G and Quantum Communication

Mobile network technologies have evolved over several decades through significant development in physical infrastructure (from analog transmission equipment to sophisticated digital systems combining RAN, edge computing facilities and core network functions) and architecture (from large centralized systems to increasingly distributed, software defined and virtualized networks). The various stages have been categorized into so-called "generations" associated with major standardization campaigns, with each generation spanning approximately a decade. Each generation represents a combination of formal technical requirements, industry consensus, and market positioning, and its definition involves a complex eco system of organizations rather than a single defining body. They include the International Telecommunication Union (ITU), the 3rd generation Partnership Project (3GPP) as well as regional standards bodies, e.g., ETSI (Europe), ATIS (North America), plus industry associations, major equipment vendors, and network operators. In addition, research initiatives like the Next G Alliance in the US [https://nextgalliance.org], the Hexa-X European 6G flagship project [https://hexa-x.eu/], China's IMT-2030 (6G) Promotion Group, [163] the Beyond 5G Consortium in Japan [https://b5g.jp/en/], and the Korean government's (MSIT) 6G R&D implementation plan [164] contribute to the vision that will eventually be formalized by the ITU over the coming years. Contrary to previous generations, 6G aims to recognize the need for alignment with societal goals such as sustainability, digital inclusion (see, e.g., [165]) and trustworthiness from the very beginning.

Starting from the analysis of industry and consumer trends, many of the contributing organizations have explored various use case families expected to be relevant in the 2030s, in order to identify potential future applications, derive requirements and address technology demands (see, e.g., [166], [167], and references therein). Types of applications which are prominent in all these analyses are, for instance, autonomous cyber-physical systems (drones, autonomous cars, collaborating robots,

etc.), remote operation (i.e., applications involving not only audio-visual telepresence but also remote physical interaction requiring haptic feedback and precise remote control; examples are remote surgery, real-time remote control of manufacturing processes or teleoperation of machinery in hazardous environments), immersive experiences (augmented and virtual reality), Digital Twins and seamless global connectivity.

The technical challenges are obvious: Ubiquitous connectivity, for instance, requires management and interoperation of a heterogenous network of many sub-networks, combining terrestrial, space-borne and airborne systems. The resilience aspect of such complex systems is often associated with self-organization, self-healing and autonomous reconfigurability and operation, all of which are enabled by AI. Depending on the applications and services, end-to-end latency constraints can be as tight as a few milliseconds (equivalent to human reaction times) with extremely high levels of reliability. The latency requirements can often only be met with disaggregated deployments, where time-critical functions need to be placed at the network edge, again resulting in increased heterogeneity and complexity of the system architecture. Data rates consumed by 6G-applications can be immense: A true VR experience, for instance, requires streaming rates at a minimum of a Gigabit per second. [168] However, it is not only the content consumed by human end-users which adds to the network load. Significant shares of the total load are due to machine-to-machine communication required for coordination and system management, execution and training of AI elements and the exchange of sensor data needed to operate autonomous systems. In wireless networks, high data rates are achieved (among other technologies) by using multiple antenna systems to direct precise beams to the legitimate users' locations, meaning that user localization and environmental sensing have become an integral part of modern networks. This introduces new security and privacy challenges, since sensing data must be encrypted (or otherwise protected) so that user identity and location are only accessed by approved services.

Since QKD can only be established over either fiber optics or free space optics, it is obvious that QKD systems are suitable for securing relatively static segments of 6G networks. Therefore, it is anticipated that PQC mechanisms will be applied in mobile and dynamic network segments. However, current PQC methods rely on longer keys and increased complexity, which somewhat contradicts stringent latency requirements. Fast, lightweight, and easily scalable security mechanisms are required especially for the deployment of large-scale IoT with large numbers of low-cost, energy constrained and low- complexity devices. Here physical layer security (PLS) may be the solution. [169] Contrary to traditional cryptographic approaches PLS provides encryption/decryption schemes that do not rely on keys and therefore do not depend on the distribution and the management of secret keys. Instead PLS realizes secure transmission via signal adaptive design and processing, taking advantage of the intrinsic characteristics of wireless channels such as noise and fading to ensure reliable data recovery by the legitimate receiver while considerably degrading the received signal quality for the eavesdropper. The security criterion used (semantic security) can be interpreted operationally, i.e., it can be set in a direct quantitative relationship to the eavesdropper's maximum probability of success for a specific class of attacks. The calculations required for the signal and data processing are computationally relatively inexpensive compared to the key-based encryption-based method, making PLS suitable for securing low-complexity and low-cost IoT devices. [170] In addition, there are studies (e.g., [171]) suggesting that the energy consumption of PLS-based schemes is only a fraction of that of corresponding PQC schemes. This is of particular interest for IoT deployments with a large number of simple energy-limited devices.

In the coming decades, 6G networks will connect all segments of modern society providing a myriad of applications and services, including industrial control, tele-medicine, vehicular communication, entertainment, smart agriculture and much more. Different levels of security are required in different areas of life. While QKD-secured communication may be desirable for applications demanding the highest level of confidentiality, this may prove to be too costly for other ones. It is also obvious

that it cannot be provided for every scenario. As we have already emphasized, wireless communication offers numerous application scenarios that are characterized by high mobility or resource constraints and must therefore primarily be secured by PQC or PLS.

5 Infrastructure and Network Aspects

5.1 QKD Infrastructure

Quantum Key Distribution (QKD) relies on a robust infrastructure capable of transmitting quantum signals securely over significant distances. In practice, building a QKD network goes beyond simple point-to-point links and aspects such as scalability, fiber availability, multi-user architectures, and seamless integration into existing communication infrastructures must be addressed. Early QKD demonstrations connected two parties over a single fiber, but nowadays real-world deployment demands connecting multiple nodes and users across cities and even national borders. This entails optimizing resource management within quantum networks by addressing fiber availability and losses through optical routing, and coordinating quantum channels alongside classical data traffic, potentially sharing the same fibers. These considerations make it essential that quantum network planning addresses both technical and strategic aspects: Technically, quantum coherence and security must be ensured; and strategically, cost-effective deployment plans, standardization, and policy support are required. In the following subsections, specific aspects of QKD infrastructures are discussed in more detail with respect to practical deployment.

5.1.1 Fiber Availability

The foundation of any terrestrial QKD network is the availability of fiber-optic links between hubs and sites, and QKD systems that can be integrated into existing infrastructures. Ideally, QKD deployment is able to integrate into existing fiber resources, particularly dark fibers, and to establish quantum channels without being affected by conventional data channels. However, even when fibers are accessible, the distance over which quantum signals can be propagated remains inherently constrained. Typically, a quantum signal transmitted through standard telecom fibers experiences approximately 0.2 dB of attenuation per kilometer, which results in near-exponential signal weakening. Additional optical components such as multiplexers or switches cause further losses to the quantum signals, thus reducing the maximum reach. Typically, conventional QKD point-to-point links rarely exceed one hundred kilometers in length without intermediate measures. Overcoming this transmission distance limit requires either installing intermediate trusted nodes (secure relay points that essentially start a new QKD link at the cost of requiring physical security at those nodes) or pursuing advanced technologies such as quantum repeaters (discussed later in Section 6.1.3).

The availability of fiber connections and empty optical wavelength channels varies widely between regions and purposes. In urban areas with well-developed metropolitan fiber network infrastructures, a dense network of telecom fibers usually already exists, comprising “dark fiber” strands or state-of-the-art fiber cables that connect government offices, data centers, and business offices. Dark fibers provide an ideal dedicated channel for quantum signals, free from interference by intensive classical data traffic. These metropolitan-area fiber networks can be leveraged for QKD in several ways, ideally by using spare “dark fibers” that lie unused in telecom bundles, or to some extent by occupying unused wavelength channels using wavelength-division multiplexing.

For last-mile connections that link end users in offices or homes to a QKD network, there are similar but even more constraining demands on the QKD systems. In these scenarios, the simultaneous coexistence of QKD quantum channels often has to be enabled in a single fiber link that already provides conventional data communication in a passive-optical network (PON) topology. In addition to wavelength-division multiplexing, it is essential that QKD systems are able to support 1-to-N user QKD in a PON-wise fashion over a fiber of typically less than 5 km length. As of September 2024, around 32.1% of German households benefitted from “fiber-to-the-home” or “fiber-to-the-building" access. [172]

In contrast, more remote or rural areas suffer from limited availability of fiber connections or higher fiber attenuation due to older cables or longer routes. This disparity harbors the risk that, without intervention, quantum communication networks could become concentrated on urban infrastructures, and critical infrastructure or communities in non-urban regions could be left behind. Policymakers could address this risk with initiatives to expand broadband internet availability in underserved areas and at the same time encourage laying fiber infrastructures that are quantum-ready. One practical strategy is to piggyback on existing telecom projects, adding extra fiber strands for quantum use or upgrading links to meet the stringent requirements of QKD such as low-loss, low-noise channels.

Backbones that interconnect distant metropolitan areas are characterized by relatively long distances and the simultaneous need for high QKD key rates that support the large number of users at each location. Both characteristics render QKD links advantageous that multiplex a larger number of QKD channels over a dark fiber to maximize the key rates.

To optimize fiber use in different application scenarios, network designers must choose routes carefully – for instance, routing quantum links along shorter, well-maintained paths to minimize loss, even if these are not the shortest paths that classical data signals might take. They must also account for fiber quality: Factors like dispersion, polarization effects, and stray bends or splices in the fiber can all disturb quantum states and effectively reduce QKD performance.

In summary, ensuring adequate fiber availability for QKD involves bridging infrastructure gaps (especially in rural areas), repurposing what is already in the ground (like dark fibers or excess capacity), and planning physical routes with quantum channel requirements in mind.

5.1.2 Multiplexing

Since optical fiber is expensive and sometimes in short supply, signal multiplexing strategies can significantly improve the use of existing infrastructure for QKD. Multiplexing enables multiple signals to propagate simultaneously through the same fiber, separated in time slots, wavelengths, or spatial modes. In quantum communications, the most widely used approach is Wavelength-Division Multiplexing (WDM). WDM assigns different wavelengths (colors of light) to different channels. For example, a QKD channel might operate at one wavelength, while high-speed classical data channels occupy other wavelengths in the same fiber. This approach can drastically increase the utility of each fiber: Instead of dedicating one fiber to each QKD link, a network operator can send many quantum keys and conventional data streams together.

Nevertheless, the intrinsic susceptibility of quantum states to noise necessitates careful engineering and wavelength allocation planning when considering multiplexing approaches. One major noise source in multiplexing configurations is Raman scattering: When a strong classical optical signal propagates through a fiber, it can scatter and produce photons in other wavelengths, some of which may fall into the quantum channel's wavelength band, thus superposing with the quantum signals or overwhelming the single photon detectors with noise. This noise can reduce the secure key rate or even prevent QKD operation if not managed adequately.

To mitigate these issues, effective WDM QKD network design requires filters, isolation schemes, or alternative band allocations that minimize cross talk and Raman noise, and result in acceptable quantum bit error rates. One proven strategy is to operate the quantum channel in the O-band around 1310 nm (originally used for older telecom systems) and keep classical data in the C-band around 1550 nm, thereby greatly reducing Raman noise in the quantum channels. In such a configuration, QKD operation over close to 100km with over 16 dBm optical power in the simultaneously multiplexed classical channels has been reported. [173] Additionally, classical channels near the quantum channel wavelength can be operated at lower power or be temporarily switched off when QKD is active, if dynamic control is possible.

Apart from wavelength multiplexing, other options include time-division multiplexing (TDM), where quantum and classical transmissions are scheduled at different times to avoid overlapping. Spatial multiplexing uses separate cores in a multi-core fiber, where, for example, one core carries the quantum channel and adjacent cores carry classical data, providing physical isolation while sharing the same fiber.

Practical demonstrations in real-world networks, where quantum and classical channels have coexisted with minimal interference, have already confirmed the feasibility of multiplexing approaches, provided that hardware and protocols are carefully optimized. From a strategic perspective, the ability to multiplex quantum and classical data reduces both the deployment costs (no need for separate fibers) and deployment timelines of integrating QKD into existing telecom networks, making it an appealing approach for the telecom industry and operators. For policymakers and planners, it follows that upgrading network equipment with better isolation, filtering, and monitoring for quantum channels can be as important as deploying new fibers.

5.1.3 Amplification

One of the characteristics of optical quantum communication is its incompatibility with traditional optical signal amplifiers. In classical fiber networks, whenever a signal weakens, an optical amplifier (such as an erbium-doped fiber amplifier) boosts it to extend reach. But the quantum information encoded in single photons cannot be amplified. The no-cloning theorem forbids making exact copies of an unknown quantum state, and any attempt to amplify it will add noise and distort the quantum state. Therefore, there are two challenges facing the integration of any quantum communication channel into existing classical network infrastructures: how to "amplify" quantum signals in specialized ways to extend their reach; and how to mitigate the impairment effects of the classical amplifiers that are already present in the network.

Several approaches have been explored to address the first challenge of "amplifying" quantum signals. The simplest most straightforward and most commonly used method by today's standards employs trusted nodes that detect and re-initiate quantum signals. While not offering end-to-end quantum security (since each node must be secure and trusted not to leak keys), this approach is currently the only way to extend QKD over long distances and between many users, and has been used in national-scale QKD networks all around the globe. [174–178] There is therefore a trade-off associated with trusted nodes: They are easier to implement using current technology but require reliable physical security and oversight for each node.

Quantum repeaters are the most promising long-term solution. These are devices that divide the total distance to be covered into shorter segments, entangle those segments, and then perform entanglement swapping and purification, effectively extending entanglement over the entire distance. In essence, rather than amplifying the photon itself, quantum repeaters create entangled link segments and then connect (swap) them, allowing two end nodes to share strong entanglement as if they were directly connected. This can enable QKD or even direct quantum state transmission over distances far beyond the 100 km fiber limit, potentially reaching intercity or intercontinental scales. However, quantum repeaters are extremely complex, often requiring quantum memory devices and sophisticated error correction protocols. They are currently still in the research stage and rely on quantum memories and advanced protocols that are not yet commercially available.

Other approaches propose the use of heralded qubit amplifiers. These devices aim to probabilistically amplify a quantum signal without reading it – by entangling the input photon with ancillary photons and using a herald signal to indicate success. In a successful event, the quantum information from a dim input photon could be transferred to a new photon, effectively achieving amplification without violating quantum rules. Early theoretical and laboratory work has demonstrated

the potential of heralded amplifiers to extend the reach of QKD and even enable certain device-independent security proofs, but these, too, are at an experimental stage.

All these approaches – trusted relays, entanglement swapping repeaters, and heralded amplifiers – represent a toolkit for overcoming loss and distance limits. Each comes with its own engineering challenges: Quantum repeaters need reliable quantum memories and error correction schemes, and the noise added by any new amplifier device must be minimal. For policymakers and planners, a key conclusion is that extending quantum links over long distances is likely to still require significant R&D efforts. Nonetheless, steady progress is being made: Metropolitan QKD networks are already linking multiple city sites using trusted nodes, and efforts are underway to test quantum repeaters on shorter testbeds. [54, 174, 175, 178, 179]

There is also a parallel path using satellites as space-based trusted repeaters that allow optical quantum signals to travel farther. Satellite QKD has already connected sites thousands of kilometers apart by exchanging keys through space. In the long term, a combination of ground-based quantum repeater chains and satellite links could form a globe-spanning quantum network. Strategically, investing in the above-mentioned technologies appears to be crucial for nations and industries that envision truly global quantum-secure communications. This means funding research into quantum memories, single-photon detectors with lower noise, and novel quantum relay protocols now, so that the distance barrier will gradually be overcome. Until then, the practical deployment of QKD will involve a clever patchwork of shorter fiber links, well-placed trusted nodes, and perhaps hybrid quantum-classical techniques to manage keys over long distances. For example, using QKD for local and regional links, and post-quantum encryption for long-haul segments could be a temporary solution for some short-term application scenarios.

5.1.4 Optical Routing

As quantum communication networks grow in size and complexity, the ability of optical routing quantum signals within a network becomes crucial. Specifically, the notion of reconfigurable optical paths for quantum signals promises more flexible and responsive deployment, closer to how classical data networks operate. Rather than dedicating a single fiber route from one point to another, optical routing in the quantum context means dynamically selecting paths for photons or entangled photon pairs to propagate from source to destination, ideally adapting to network conditions without disturbing the quantum states. This functionality would enable redundancy, load balancing, link aggregation, and network optimization, analogous to classical network routing where packets are transmitted via optimal paths, but with additional constraints. A fundamental requirement is that any routing operation must not measure or disturb the quantum state. In classical networks, routers read packet headers, buffer data, and resend it – actions impossible for unknown quantum states because measurement would destroy the information. Therefore, quantum optical routing relies on transparent photonic switches or entanglement-based methods.

One approach is to use all-optical switches controlled by a classical network management system that can reconfigure which fiber a quantum signal goes into, without converting the photon to an electrical signal or reading its value. Technologies such as micro-electromechanical switches (MEMS mirrors) or advanced wavelength-selective switches can, in principle, reroute single photons, but must be engineered to ensure minimal additional loss and noise. Each additional beam splitter or redirector is a point of potential photon loss or decoherence, so the feasibility of dynamic optical switching depends on achieving very low-loss, low-crosstalk switching. Recent research on integrated photonics seems very promising. For example, integrated photonic chips with waveguide switches might, in the future, operate as a quantum router chip that directs photons from any input port to any output port on command.

Another approach is entanglement-assisted routing. In an entanglement-based quantum network, the secret quantum state is not sent through multiple hops. Instead, intermediate nodes share entangled pairs with their neighbors, and by performing coordinated measurements, i.e., entanglement swapping, entanglement can be extended across the network. In such a scenario, routing is about choosing where to perform entanglement swaps to establish end-to-end entangled links. This resembles a typical routing task: If one path comprising a sequence of swapping nodes is lossy or busy, a controller directs swaps along an alternate path in the network to establish a quantum channel between two distant nodes. The challenge here is maintaining quantum coherence across multiple swaps, since each swap and each link has a success probability and fidelity, and the end-to-end entanglement quality can decrease significantly if too many low-quality links are concatenated. Therefore, protocols are needed to decide the optimal route and possibly to perform entanglement purification where multiple low-purity entangled pairs are consumed to produce one higher-purity pair along the chosen route. Quantum network research is currently working on developing algorithms analogous to classical routing protocols to deal with entangled states and coordinating actions between entanglement-swapping nodes.

These dynamic routing functionalities require a sophisticated control plane that makes routing decisions in real time. Some experimental networks have begun to explore this. [180] For instance, software-defined networking techniques are being tested to control optical switches that handle both quantum and classical channels. These controllers must account for quantum channel conditions and be able to receive telemetry such as quantum bit error rates or key rates from each link and then decide the route to maximize security and throughput. Entanglement-assisted routing also implies new protocols at the application layer. If entanglement can be routed dynamically within a network, it can enable quantum teleportation to send actual quantum states (not just keys) between end nodes. This goes beyond QKD and ventures into the idea of a quantum internet.

Strategically, developing quantum routing capabilities moves toward scalable quantum networks that function more like today's communication networks in terms of flexibility. This will require collaboration between photonic hardware designers, who design quantum-enabled switches, quantum information scientists, who devise routing and swapping algorithms, and network engineers, who integrate these into a manageable system.

For industry, a practical step toward preparing and supporting dynamic routing in quantum networks is to incorporate equipment that is quantum-compatible. For policymakers, it is important to support testbeds that experiment with quantum routing and to foster standards for how quantum routing information is signaled. As QKD deployment is scaled up in the coming years, flexible optical routing will increasingly become a key enabler for resilient, multi-node quantum networks, allowing the technology to approximate the robustness and adaptability of classical networks.

5.1.5 Orchestration and Network Management

Coordinating a quantum communication network, particularly beyond simple point-to-point systems, calls for sophisticated orchestration and network management techniques that incorporate both quantum and classical resources.

Orchestration refers to the intelligent control plane that oversees all the network components by managing resources, scheduling operations, and ensuring that quantum and classical elements work together. In a classical data network, technologies like Software-Defined Networking (SDN) operate by decoupling the control logic from the hardware. In recent years, there has been interest in adapting software-defined networking concepts to QKD using centralized controllers that direct QKD devices, switches, and key management systems from a central software plane to orchestrate the allocation of quantum channels, the distribution of keys, and the relevant classical support. The

goal is to handle the complexity of large-scale QKD networks with a multitude of users using automation to efficiently assign channels, perform key relays, and monitor the systems.

A major task of quantum network orchestration is key management. An orchestration layer can, for instance, determine which links should be used when certain users or applications request a quantum-secured communication channel while simultaneously balancing key generation rates and operational constraints. This requires a management system that knows which parties need keys, how urgent their need is, and which path or link can best supply those keys. Real-time adaptive key management fits naturally into this model, as quantum key rates can vary with link conditions or usage.

For example, suppose a bank's branch office wants to establish a secure line to its headquarters. The orchestration system might schedule a QKD session between them or, if no direct link exists, orchestrate a series of QKD exchanges through intermediate nodes. The system will gather keys from these links, concatenate them via relay operations at trusted nodes to form an end-to-end key and then deliver this to the requesting parties. Doing this in real time on a potentially large scale poses a complex coordination problem. Real-time adaptive key management means the network can respond to changes immediately. If one link's key rate drops due to fiber degradation or a potential eavesdropping attack, the controller can dynamically reroute key exchanges through a redundant path or allocate more time. Similarly, if demand spikes when a large number of users request keys at the same time, the system can queue or prioritize requests based on policy. This is analogous to bandwidth management in classical networks.

SDN controllers tailored to QKD have been demonstrated in research settings (e.g., MadQCI [175]), showing that a logically centralized software can successfully configure QKD links and even dynamically adjust parameters. These controllers often have to interface with both quantum equipment through specialized APIs provided by QKD device manufacturers, and standard network equipment like standard routers or optical switches. The emergence of standardized interfaces, such as those from ETSI's QKD industry group, will be key to enabling multi-vendor orchestration.

A robust orchestration system must also be able to handle multi-domain quantum networks. Realistically, no single operator will own all the fibers at every location. A QKD service provider in one region or domain might have to hand keys over to another provider in a different region. Within a country, different government departments might operate their own segments of a quantum network that need to interconnect. Orchestration in this context means having protocols for inter-network key exchange and trust management. Frameworks are being proposed where, for example, a centralized key management server can request keys from another domain's server via a secure classical link, in effect allowing QKD-generated keys to hop between administrative domains without exposing them. Achieving this requires interoperability standards to signal key requests, infrastructures to authenticate nodes from different domains, and agreements on parameters like minimum security levels, error rates, etc., that are acceptable for handed-over keys.

Another facet of network management is resource optimization. The orchestrator must allocate quantum network resources wisely. If keys are not required by two end-user nodes at that moment, their QKD link could be idled or used to generate keys that can be stored for later, while another pair of end-user nodes with urgent needs is given priority. From a security perspective, orchestration can aid in intrusion detection and recovery. By monitoring the real-time status of QKD links in terms of channel loss or error rates, for example, the system could quickly detect anomalies indicating tampering or eavesdropping. It could then alert operators or automatically reroute communication through alternate paths if needed. For example, if a particular fiber link's error rate suddenly spiked beyond a defined threshold, the orchestrator could pause QKD on that link, use a secondary path, and flag the suspicious event for investigation.

Network management also includes other essential aspects of running any type of network including logging events, updating software, and accounting for usage. While authentication and accounting are addressed in section 5.1.6 in more detail, it is worth noting that orchestration systems will be tied into those functions since, e.g., only authenticated nodes are allowed to participate in the network.

For industry professionals, the push toward automated quantum network management means that deploying QKD at scale will gradually come to resemble the deployment of any network service, with high-level software control rather than a handcrafted link-by-link setup. Many telecom companies are already adapting their network management software to be quantum-ready, in anticipation of devices like QKD equipment, quantum repeaters, and others becoming part of their inventory and having to be managed in the same way as routers and switches. For policymakers, an orchestrated approach underscores the importance of standards and interoperability. Governments aiming to build national quantum-secure networks may have to coordinate multiple vendors and network operators and having common management protocols in place that are ideally guided by standards bodies such as ITU or ETSI will make it easier to expand and interconnect these networks.

5.1.6 Authentication/Service Access/Accounting

Like any secure communication infrastructure, quantum communication networks require solid authentication, service access control, and accounting (ASA) mechanisms to verify identities, manage permissions, and track usage.

Secure authentication is crucial on several levels. First, during each QKD-protocol run, authentication of critical information exchanged between all involved devices is inherently required for QKD-postprocessing, e.g., during sifting, error correction or privacy amplification. If not properly implemented, i.e., ideally using an information-theoretically secure authentication scheme like Wegman-Carter, an eavesdropper could conduct man-in-the-middle attacks and acquire full information about the keys. Therefore, all QKD security proofs require an initial secret authentication key that is shared between partner devices upon system initialization. Conventionally, this initial secret authentication key is manually installed locally on the partner devices during system installation or initial configuration to maintain the full chain of information-theoretical security. However, a more practical solution that is sufficient for most application scenarios could be to use post-quantum public-key cryptography to share the initial secret authentication key. As the time between the public key infrastructure (PKI) exchange and communicating the authentication tags can be kept extremely short, i.e., much shorter than any (quantum) algorithm would need to break the authentication method, this provides sufficient protection against man-in-the middle attacks during the first QKD round. Once the first round has succeeded, all subsequent rounds can then use information-theoretically secure authentication schemes, e.g., Wegman-Carter.

Second, as with any other network device, QKD devices also need authenticated access for administrative purposes, configuration tasks or logging and monitoring. In an ideal scenario, such access is itself protected by QKD keys using secure authentication methods, but this would require QKD links between the QKD devices and network administrators and operation centers. For this reason, today's QKD systems usually block remote access to security-critical configuration tasks completely and only allow remote access to non-security-critical services that are then authenticated with conventional methods and role-based access control.

Third, service access control ensures that only authorized entities can request key generation or retrieve keys from the network's key management system. This could be implemented using classical methods, e.g., a centralized key server that requires valid credentials or certificates from a user before providing keys. This approach might be suitable for a private, point-to-point QKD link but it

becomes increasingly more complex in multi-user networks, where many clients from potentially different companies or departments share a common QKD infrastructure.

Multi-domain QKD service frameworks represent an extension of this, where keys can pass from one domain to another, and the authentication and access rules of both domains must be respected. Within EuroQCI, frameworks are currently being explored within which a federated identity or trust model could allow, for example, a user from domain A to share a quantum key that originated from or transited through domain B, without either domain compromising security. Achieving this might involve trusted interfacing nodes at the boundary that authenticate each other and only pass along keys wrapped under secure encapsulation.

Beyond authentication, an accounting framework needs to be established that logs all key exchanges, resource usage, and access events. Such an accounting framework serves to provide an audit trail about which keys were distributed, to whom, and when, and whether there were any unusual access attempts. Moreover, in a commercial setting, accounting is necessary for billing, allowing a telecom service provider to track usage per client and to charge customers based on the number of keys exchanged or the duration/bandwidth of quantum-secured channels used. Accounting might also be mandated by compliance regulations in order to demonstrate fulfilment of auditing requirements for data protection laws or industry standards.

For QKD manufacturers, this entails suggests that QKD's authentication and access control should be ideally aligned with the ASA frameworks already in place to avoid the introduction of too many unfamiliar procedures for users.

5.1.7 Node Security

When deploying QKD, it is critical that the nodes themselves, including the devices and endpoints in a QKD network where quantum signals originate, terminate, or are relayed in a trusted-node fashion, are physically protected and secured. Even if the distribution channel of keys over quantum channels is secured in the long term by fundamental laws of physics, nodes that make keys accessible for their utilization are classical devices that are not inherently protected by quantum physics and require protection to not be compromised or leak keys to adversaries.

Ensuring node security means protecting the hardware against tampering, the software against hacking, and the quantum processes against side-channel attacks. On the physical front, QKD devices must be secured against direct intrusion. This includes conventional measures such as locked cabinets, tamper-resistant and tamper-detection enclosures with active tamper-response capabilities, and access control to facilities.

QKD-specific vulnerabilities and side-channel attacks remain an active field of research. In 2023, the BSI, together with other quantum security experts, compiled a comprehensive document that thoroughly analyzes implementation attacks and countermeasures for QKD node systems. [33] Countering side-channel attacks requires both design and procedural measures, and modern QKD systems have addressed many of these issues by revising the hardware. Nonetheless, continuous testing for new side channels remains imperative, similar to the penetration tests of classical cryptographic devices. For example, side-channel tests might involve monitoring the electromagnetic emissions or power consumption of a QKD device to ensure it is not revealing the key. Ultimately, a QKD system is an electronic device and could have similar side channels as any cryptographic device, e.g., power analysis attacks. Therefore, conventional protection options also apply such as shielding or mitigating correlated power analysis.

The cybersecurity of nodes is just as important because QKD devices run firmware or software to control the optics and interfaces with networks. If an attacker can remotely exploit a bug in the

device software or firmware, this could sabotage the proper functioning of the protocols in accordance with the underlying security model, e.g., by altering components' functionality or even passively reading out keys. Therefore, standard practices such as regular software updates, firewalls, and intrusion detection around the control systems are mandatory. Ideally, to minimize exposure, QKD systems would completely isolate the quantum processing unit from any external network except a dedicated management link. Cryptographic node security also encompasses secure key management. Generated keys are usually stored temporarily in the node before being delivered to the end application. Some systems therefore integrate a hardware security module that stores all security-relevant keys in encrypted form and that are erased immediately upon release or if tampering is detected. This ensures that the key material is secure and prevents attackers from reading a cache of past keys.

Standardization bodies and agencies like ETSI, ISO, or national labs are therefore working on evaluation criteria for testing QKD systems under various attack scenarios. A certified QKD node would give users confidence that it meets a high security standard. In addition, just as classical cryptography features redundancy (multiple algorithms, etc.), it would also be possible to achieve resilience at the node level by, for example, using different types of key distribution methods or QKD devices in parallel to maintain security even if one method or device had a hidden flaw or side channel.

In summary, securing quantum nodes requires a multi-layered approach: physical security to block unauthorized physical access, protection against side-channel and optical attacks to ensure the integrity of quantum processes, cybersecurity measures to cryptographically protect control systems and key storage, and incorporating certain QKD techniques such as MDI-protocols to eliminate whole classes of implementation vulnerabilities.

Further references for this section include [46, 181–188].

5.2 Quantum Information Networks

Beyond immediate QKD deployments, the broader goal for quantum communication envisions networks capable of distributing quantum information of various types on a large scale, not merely cryptographic keys. Such quantum information networks (QIN) would distribute entanglement between multiple nodes and enable more advanced applications beyond QKD (see section 4.3). While present-day QKD trusted node networks can be regarded as the first generation of quantum networks[8], future networks will include technologies such as quantum memories and quantum repeaters, enabling entanglement-based applications, e.g., quantum teleportation, distributed quantum computing, and novel quantum sensor applications.

A fully realized QIN would allow any two (or more) nodes in the network to establish quantum links on demand, much as today's internet allows any two computers to exchange data. A key issue for this evolution is the interoperability with classical networks. Rather than constructing dedicated infrastructure, it is more likely that QINs will have to make use of existing infrastructures at least to some extent, e.g., by multiplexing quantum and classical signals as discussed in section 5.1.2 or by upgrading classical repeater nodes to bypass quantum states or redirect them to quantum repeaters as discussed in section 5.1.3. For end users and applications, the quantum network's inner workings should ideally become invisible and be based on familiar procedures, with the quantum layer providing additional specialized functions "under the hood". Achieving interoperability requires standardized interfaces, for instance, by developing standard APIs for an application to request a

[8] In this report we regard quantum networks as all types of networks via which quantum states can be sent

secure key or an entangled qubit pair from the network. It also requires designing network architectures that can incorporate quantum links into existing network topologies similar to the way that new wavelengths channels or new fiber links are added today.

As these hybrids of classical and entanglement-based networks evolve, the role of entanglement as a fundamental resource will become pivotal for reaching the full potential of quantum communication. To date, the first small entanglement networks with three or four nodes entangled in a line or a triangle have demonstrated important building blocks in lab and field trials such as quantum memory and repeater prototypes, proof-of-concepts for primitives like entanglement swapping between nodes, and even simple network protocols for requesting entanglement. As the technology matures, these are expected to be scaled up to a larger number of nodes and greater distances. Europe's Quantum Internet Alliance and similar initiatives elsewhere are investing in building a functional quantum information network that can deliver entanglement on-demand between distant sites.

However, this vision is accompanied by challenges. Increasing link distances, even with quantum repeaters, mean that every added link in an entanglement chain lowers the fidelity unless quantum purification is carried out, which itself requires extra entangled pairs and classical communication. Interoperability poses other technical and organizational challenges. Getting different quantum devices to work together is non-trivial, since unlike classical communication and computing, quantum hardware is not yet standardized and still undergoing research to a large extent. For example, connecting a quantum memory based on single trapped ions to another based on atomic ensembles or solid-state spins in one network and entangling them will require standard quantum interface protocols or the respective converters. Technical complexity and costs are further challenges associated with constructing large-scale QINsbecause they will initially be very costly and require highly trained specialists to maintain. However, as with any technology, costs are expected to come down with economies of scale and over time. Solid-state and photonic integration are likely to produce more compact and cost-effective quantum network elements in the future. Until then, deployment might be limited to high-value use cases (national security, critical infrastructure, financial networks), whose importance and benefits justify the expense involved.

Despite these challenges, incremental but meaningful milestones toward full quantum information networks are already becoming visible and more can be expected in the coming decade, with each success reinforcing investment and interest. These could include the rollout of national QKD networks with dozens of nodes and path redundancy, the demonstration of a small quantum network linking perhaps half a dozen cities with entanglement, and possibly hybrid networks where satellites provide one link and fiber networks provide others, achieving global reach. For policymakers, facilitating this evolution means continuing to support basic research on quantum networking, building testbed infrastructures for academia and startups to experiment with, and crafting policies that encourage telecom operators to participate. It also requires training a workforce skilled in quantum technologies in an interdisciplinary effort combining photonics, computer science, and quantum physics to construct and maintain these networks. [189–192]

5.3 EuroQCI

Infobox: EuroQCI [51]

In 2019, seven EU Member States signed **the European Quantum Communication Infrastructure (EuroQCI)** declaration, agreeing to explore how to develop and deploy a QCI across Europe within the next ten years. By July 2021, 27 countries had signed this declaration.

EuroQCI builds on the innovative technologies developed as part of EU initiatives, in particular the **OpenQKD project** funded under Horizon 2020. OpenQKD has established 16 open testbeds in 9 Member States (DE, FR, NL. ES. PL, AT, CZ, IT, GR), the UK, and Switzerland and has demonstrated more than 30 use cases in different application areas. [193]

EuroQCI, as a logical extension of OpenQKD, will move toward technological deployment and establishing operational systems. Supported by the Digital Europe Programme (DEP) and the commitment of the Member States, 21 national projects are developing national terrestrial QKD networks (TerrQCI) and using these networks to demonstrate advanced use cases. According to the funding guideline, these should **primarily target public use cases by linking public authorities within a country**, but a wide range of applications are being explored, such as education, defense, healthcare, finance, critical infrastructure, and foreign affairs. In addition to the national projects, the DEP includes several industrial projects to develop technological building blocks and one Coordination Support Action to link the actors involved in a network (Petrus).

At the same time, EuroQCI is also building the space infrastructure segment (SpaceQCI) through its cooperation with ESA [194] and ESA's Security and cryptGrAphic mission (SAGA). ESA and an industrial consortium are currently working on the EU's first quantum satellite prototype, Eagle-1, due to be launched in early 2026.

To achieve the objective of an EU-wide communications infrastructure (EU-QCI), the national networks and the space segment need to be interconnected. Activities to do so are funded with 90 million EUR, which does not include national or industry co-funding.[195] The TerrQCIs operated by the Member States in combination with the SpaceQCI developed by ESA [196] will together form the EU-QCI as described in the ConOps. [197]

Some stakeholders believe that the program contributes not only to technology deployment but also to **awareness-raising** by involving various actors and convincing them of the future reliability of QKD.

6 Standardization, Certification and Approval

6.1 Standardization

Introduction

Standardization is the process of developing, implementing, and promoting standardization documents9 to ensure consistency, interoperability, quality, and safety across products, services, and systems. It involves establishing agreed-upon standards and specifications through consensus among industry experts, stakeholders, and governing bodies. The aim of standardization is to facilitate compatibility, enhance efficiency, reduce costs, and promote innovation while meeting the needs of all relevant parties. By providing a common framework, standardization helps to streamline processes, ensure reliability, and support global trade and communication.

A standard is a consensus-driven document approved by a recognized standardization body or standards developing organization (SDO). It outlines rules, guidelines, or characteristics for activities and their outcomes, representing the current state of the art. Such standards are rooted in the collective results of science, technology, and experience, with the goal of maximizing benefits for the entire community.

Standardization in quantum communication

Standardization is essential for emerging fields, as proactively establishing interfaces and terminology helps avoid expensive revisions farther down the line. Standards should be broadly applicable across the diverse range of quantum technologies, and specialized standards, such as those for quantum communication, should only be developed when truly necessary. This strategy promotes efficiency and cohesion in the advancement of quantum technologies.

Potential suitable areas for standardization include terminology, measurement, testing, interfaces, and compatibility. Moreover, as quantum technologies reach market application, standards detailing services, products, and quality will become increasingly relevant. This comprehensive approach ensures the seamless integration and adoption of quantum technologies across various sectors.

In the BMBF-funded project SQuaD, DIN provides essential support for standardization efforts, particularly in quantum communication. DIN offers a comprehensive overview of relevant standards in this field [198] and has organized several workshops focused on the "Needs Analysis of Norms and Standards for Quantum Communication along the Value Chain." These workshops examined the production of necessary components and systems, their integration into existing communication infrastructures, and potential end-user applications. [199] Key issues mentioned in these workshops by the experts include the lack of:

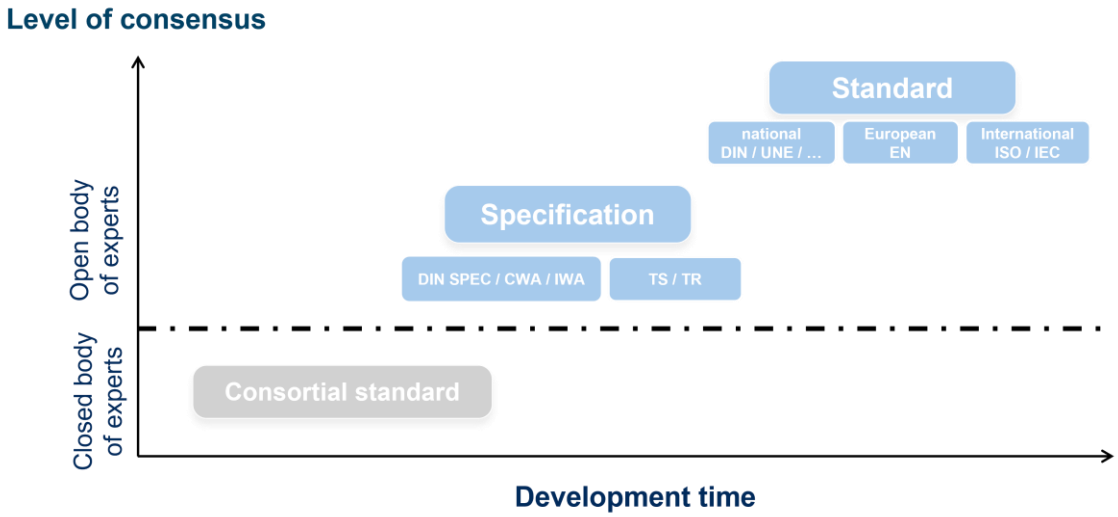
- migration procedures from classical cryptography to QKD/PQC
- secure QKD protocols
- definitions and requirements for trusted nodes
- standards for hardware authentication and its implementation
- certification in general and relevant documentation.

[9] In this text, the term "standard" refers to all types of standardization documents.

Standardization process

Before delving into specific procedures, an overview of the different types of standardization documents is provided, as illustrated in Figure 3. To aid in understanding these distinctions, the terms "specification" and "standard" are employed, although these are frequently used interchangeably. The discussion aims to explain the differences between these documents, offering insights into their roles and implications in the evolving landscape of quantum communication standardization.

Figure 3: Overview of standardization documents.



In terms of development time, in many cases, consortial standards (illustrated in Figure 3) are the quickest to become established. Also known as industry, informal, or de facto standards, these are defined by their development process, which does not require the inclusion of all interested parties. They are typically created by closed groups of experts, such as industry-specific consortia comprised of various companies. While consortial standards share some features with traditional standardization documents, such as defined procedures and documentation rules, they are often developed privately and may not be freely accessible.

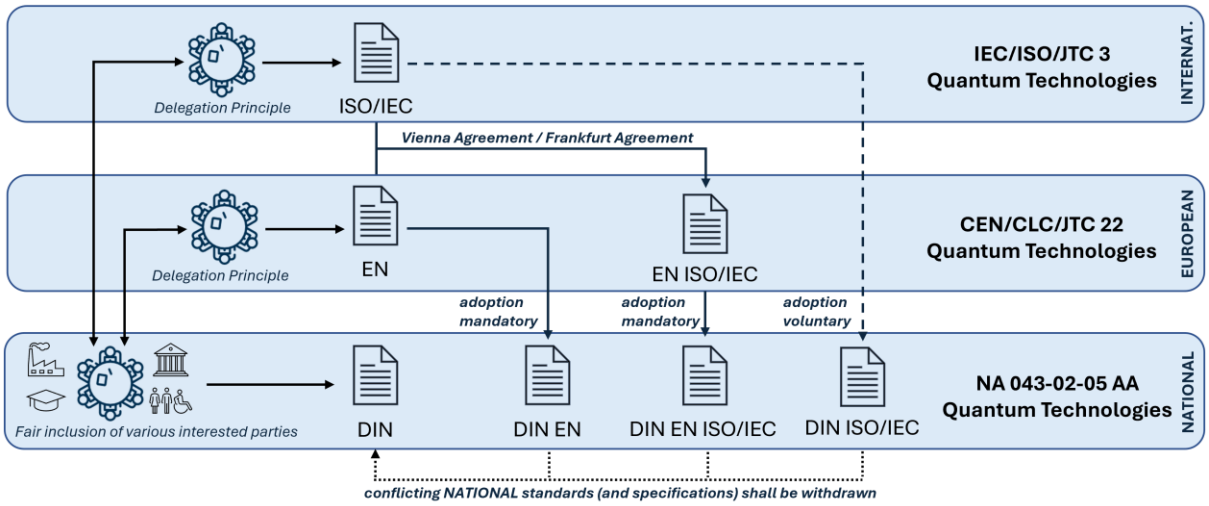
In the strictest sense, standards are developed within a formal standardization system, requiring the inclusion of all interested parties when developing the documents. Achieving consensus, which is defined as the general agreement of all participants without sustained objections to key content, is essential. These committees include diverse stakeholders from science, consumer groups, and industry to ensure the neutrality of the documents. Anyone can submit a proposal for a standard, which means a public comment period is mandatory in the development process.

Unlike consensus-based standards, specifications do not require consensus, nor the involvement of all interested parties. Anyone may apply to create a specification, whose scope is then compared with the existing standardization repository. Followed by an open call for participation, its development and final publication are agreed upon within a consortium. Specifications can also be developed by standards committees if the final consensus needed to publish a standard cannot be reached. These are referred to as CEN or ISO Technical Specifications (TS). Technical Reports (TR) are documents developed and approved by a technical committee, providing information on technical content and ongoing standardization work.

Relevant players, institutions and ongoing activities

Figure 4 shows the development of standards at national, European, and international level in the field of quantum communication as part of quantum technologies.

Figure 4: Development of standardization documents at national, European and international level in quantum technology.



Every country has its own national standardization body or national committee, which includes specialized committees focused on specific areas, such as quantum communication. In Germany, for instance, this is managed by the **NA 043-02-05 AA Quantum Technologies** [200] committee. These national committees have to ensure fair representation of all interested parties and develop national standards, such as the DIN standards in Germany.

These national committees play a vital role as they send delegates from so-called national mirror committees to European and international committees to represent the national opinion. In the realm of quantum communication, **CEN/CLC/JTC 22 Quantum Technologies**, [201] and especially **CEN/CLC/JTC 22/WG 4 - Quantum Communication and Quantum Cryptography**, [202] are responsible for developing European (EN) standards. Once an EN standard is established, it becomes mandatory for European member states to adopt it, and any conflicting national standards must be withdrawn, resulting in a harmonized European standardization repository.

At the international level, **IEC/ISO/JTC 3 Quantum Technologies** [203] is responsible for establishing international ISO/IEC standards. Unlike European standards, these do not require mandatory adoption unless they are adopted at the European or national level, which is at the discretion of the respective country. To prevent the duplication of efforts, European and international standards can be developed concurrently, as outlined in the Vienna and Frankfurt Agreements.

In the realm of quantum communication, various other organizations play significant roles. At the national level in Europe, there are dedicated cybersecurity authorities, such as Germany's **Bundesamt für Sicherheit in der Informationstechnik** (**BSI**), [204] (the Federal Office for Information Security). While America's standardization approach differs from that of Europe, it has a crucial impact on security standardization. One of the key organizations here is the **American National Standards Institute** (**ANSI**), which oversees the development of voluntary consensus-based standards and coordinates the international standardization efforts of the U.S. ANSI works alongside national organizations like **Underwriters Laboratories** (**UL**), the **American Society of Mechanical Engineers** (**ASME**), the **Institute of Electrical and Electronics Engineers Standards Association** (**IEEE SA**), and **the American Society for Testing and Materials** (**ASTM**). Additionally, the **National Institute of Standards and Technology** (**NIST**), a non-regulatory agency under the U.S. Department of Commerce, plays a vital role in American standardization efforts.

In Europe, the **European Telecommunications Standards Institute** (**ETSI**) is also very relevant, particularly the **ETSI Industry Specification Group for Quantum Key Distribution (ISG-QKD)**

[205] and the **ETSI Technical Committee CYBER Working Group on Quantum-Safe Cryptography (WG QSC)** [206]. On the international stage, the **International Telecommunication Union (ITU)** is a key player, with its Study Groups **ITU-T/SG 13 Future Networks** [207], **ITU-T/SG 17 Security** [208], and the **Focus Group on Quantum Information Technology for Networks (FG-QIT4N)** [209]. The **Internet Engineering Task Force (IETF)** and the **Internet Research Task Force (IRTF)** also contribute significantly, particularly through groups like the **Quantum Internet Research Group (QIRG)** [210] and the **Crypto Forum Research Group (CFRG)** [211].

Outlook

Given the multitude of ongoing activities, it is essential to coordinate standardization efforts to avoid redundancies. Standards developed within established structures, such as the national standardization bodies, CEN/CENELEC, and ISO/IEC, offer significant advantages over others. While numerous standardization documents exist, only a limited number qualify as true standards. As previously discussed, an open process and the equitable inclusion of all stakeholders are critical for the field of quantum communication. Established collaboration between authorities such as the European Commission (EC) and Germany's Federal Office for Information Security (BSI) with National Standardization Bodies (NSBs), National Committees (NCs) and organizations such as CEN and CENELEC plays a pivotal role in creating robust security standards and ensuring their application through the acceptance of these stakeholders.

Moreover, it is important to note that quantum communication is just one application within the broader scope of quantum technology. Therefore, standards should be applicable across various applications. This inclusivity can be ensured through CEN/CLC/JTC 22, which maintains close links among its working groups. Such collaboration ensures that the developed standards are as open as possible to all applications, with specific requirements delineated only when necessary for certain applications.

Currently, several activities are underway in quantum communication, including:

- ISO/IEC WD TR 25544 - The effect of different transmission media on the security evaluation of quantum key distribution
- prCEN/CLC/TR XXX (WI=JT022006) - Hybridization of Quantum Computing
- prCEN/CLC/TR XXX (WI=JT022001) - Quantum Network Best Practices
- prCEN/CLC/TR XXX (WI=JT022002) - QKD and PQC: An Equitable Analysis and Comparison of Both Technologies
- prCEN/CLC/TR XXX (WI=JT022003) - Gap Analysis of Current Quantum Communication and Quantum Cryptography Standards
- prCEN/CLC/TR XXX (WI number not assigned yet, but topic has been approved) - Standardization needs for satellite based QKD

6.2 Certification and Approval

Introduction

The certification and approval of IT security products is essential to ensure trust in the reliability of these technologies. Specific processes are required here, which not only provide a framework for evaluating the security claims of QKD implementations but also ensure that they meet the stringent standards set by governing bodies. This section aims to give a basic overview of the principles and methodologies of the certification process for QKD technologies and highlights the importance of these evaluations in promoting trust in the reliability of quantum communication systems.

Certification and approval in quantum communication

Common Criteria Certification is always related to a specific product. For quantum communication, this means that each QKD product has to be evaluated to be certified. The first product certification step is to define the requirements that have to be fulfilled. The set of implementation-independent IT-security requirements is defined by a protection profile (PP). The PP itself has to be certified by national security agencies as proof that it is complete, consistent, and technically coherent. [38]

The first steps have been taken to certify prepare-and-measure QKD systems. The European Telecommunications Standards Institute (ETSI) has developed a protection profile for the security evaluation of P&M QKD systems under the Common Criteria for Information Technology Security Evaluation. [212] The German Federal Office for Information Security (Bundesamt für Sicherheit in der Informationstechnik - BSI) has validated this PP and issued a certification.

Analogous to certification, the **approval** of IT security products is always related to a specific product. In Germany, IT security products used to process, transmit or store classified information in federal or state governments need to be approved by the BSI. This ensures that security requirements are fulfilled, and the products are safe to use. An application for the approval of an IT security product can only be submitted by a federal authority user (in German "Bedarfsträger"). Beyond the actual QKD systems, additional devices such as key management systems or encryptors have to be approved, as the entire system needs to meet the security requirements.

The first QKD system has recently received a national security certification in South Korea. [45] The Korea Information and Communications Technology Association (TTA) as designated authorized testing agency for quantum cryptography equipment, was responsible for the certification process. Tests for the security conformity verification were carried out by the Korea Research Institute of Standards and Science (KRISS) and the security function was finally verified by TTA. [213] Little details about the exact process and the evaluation are known to the authors of this report but were reported to include "rigorous and comprehensive evaluation of optical and digital subsystems". [45] In Europe, so far, no QKD system has been certified.

Certification and approval process

The **certification process** for QKD systems according to the Common Criteria Protection Profile involves several steps. The following steps illustrate how the process works in Germany with the BSI as the certification body: [214]

1) A company (e.g., the manufacturer of a QKD system or another interested legal person, such as the user of this system) contacts the BSI to request the certification of a specific QKD product. The BSI leads the certification process.
2) The company submits a certification application to the BSI.
3) The company commissions an accredited testing center to evaluate the QKD system.
4) The testing center evaluates the QKD system according to the requirements laid out in the PP. The company is obliged to support the evaluation, e.g., by providing access to the QKD system and the documentation.
5) The testing center writes an evaluation report and sends this and all evaluation results to the BSI.
6) The BSI examines the evaluation results in detail and issues the certification if all the requirements have been fulfilled.

More details on the process can be found on the BSI's homepage. [214] This structured approach ensures that the requirements are met and provides assurance to the user regarding the security

and functionality of the QKD system. However, additional components, such as key management systems and encryptors, are needed to use QKD systems for secure communication, and these must be certified as well.

The **approval process** for IT security products (and thus also for QKD systems) also consists of several steps: [215]

1) A federal authority user contacts the BSI with a request for approval of a specific product.
2) Evaluation of the product, including technical inspection and security evaluation according to a classified information requirement profile (VS-Anforderungsprofil). These profiles have a similar format as the common criteria protection profiles and include various aspects, such as technical requirements, supply chain aspects, requirements for the employees, access to the manufacturer's premises, and many more. If no classified information requirement profile exists for the product type, the manufacturer, the operator, the user and the BSI jointly define the security requirements for this product in a new classified information requirement profile. This is a separate process and not part of the approval process
3) Product approval if all the requirements have been met.

A product does not need to be certified for its approval, as approval and certification are separate processes. More details about the approval process can be found on the BSI's homepage. [215]

Relevant players, institutions, and activities

National security agencies are the most relevant players for certification and approval. These include the BSI in Germany, the Agence nationale de la sécurité des systèmes d'information (ANSSI) in France, the National Cyber Security Centre (NCSC) in the UK, and the National Security Agency (NSA) in the US. Product testing is typically carried out by accredited testing centers that are different in each country. In Germany, for example, these include atsec information security GmbH, Deutsche Telekom Security GmbH, and TÜV Informationstechnik GmbH. [216]

All the players and committees that promote standardization also support certification. Certification and approval processes typically rely heavily on standards that, for example, define the testing method for specific aspects of the product. Those responsible for defining the requirements for certification, e.g., by developing a protection profile (such as ETSI), also play a very important role.

Other important players include the manufacturer, operator or user of a product who wants to prove the functioning and security of the device and starts the certification or approval process.

Outlook

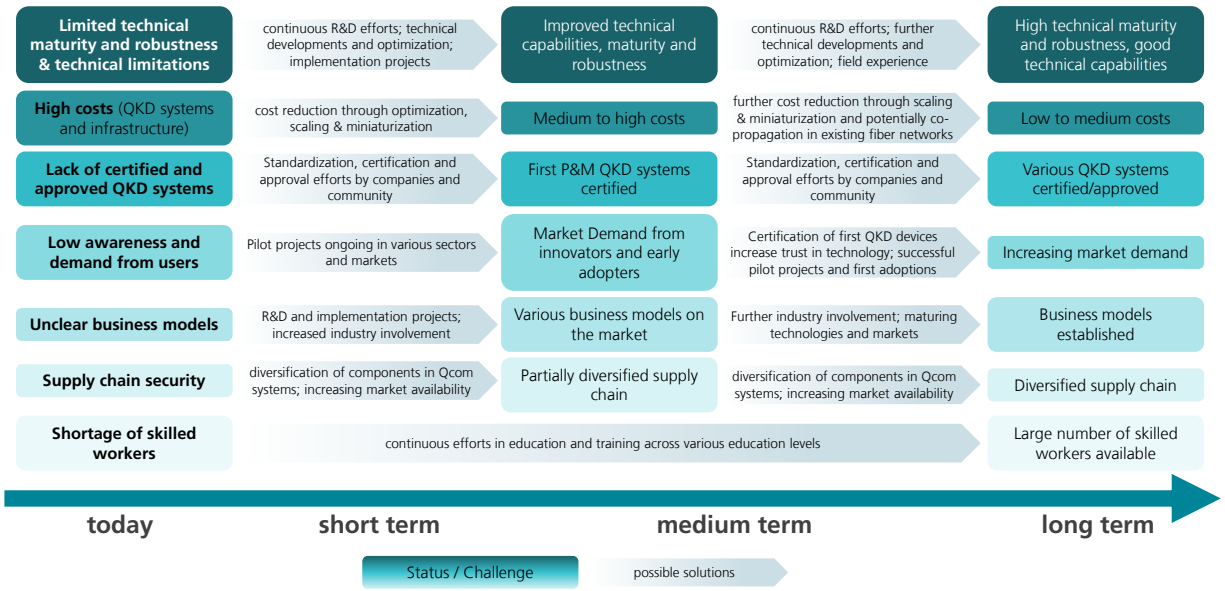
In Germany and Europe, there are high requirements for the certification and approval of IT security products to ensure their security and functionality. The steps toward certification are clearly defined. ETSI has developed and the BSI has approved the first protection profile defining the requirements for the certification of prepare-and-measure QKD systems. This means the first steps have been taken toward a certification of QKD systems, but various necessary standards are still missing. It is therefore difficult to estimate how long it will take until the first QKD products are certified, and different players are more or less optimistic about this. Some argue that this might be possible by 2027, others think it more likely that the first QKD products will be certified around 2030. Ultimately, this will depend on the standardization efforts by the community, the progress made toward certification, technological development, and how certain components such as trusted nodes are evaluated.

7 Perspectives toward QKD Adoption

7.1 Main Challenges for QKD Adoption

The main current and future challenges for QKD adoption and ways to overcome them are summarized in Figure 5 and discussed below.

Figure 5: The main challenges for QKD adoption and how they could be solved.



Limited technical maturity and robustness, technical limitations:

The current state of QKD technology poses significant challenges in terms of technical maturity, robustness, and technical limitations (such as distance or key rate limitations). Many QKD systems are still at an early stage of development, and their reliability varies under different operational conditions. To address this in the short term, continuous R&D efforts, technical developments and optimizations are essential to achieve high technical maturity and robustness and improve the technical capabilities. These ongoing efforts, coupled with experiences from implementation projects, are expected to enhance system performance. In the long term, further technical developments, optimization, and field experience will contribute to the availability of robust and mature QKD systems, with enhanced technical capabilities.

High costs of QKD systems and infrastructure:

The high costs associated with QKD systems, resulting from the current market situation rather than the actual costs of the technology, and their infrastructure (including dark fibers, ground stations for satellite QKD, etc.) remain a significant barrier to adoption across multiple sectors. In the short to medium term, cost reductions can be achieved through the optimization, scaling, and miniaturization of QKD systems. In the medium to long term, further cost reductions of the QKD systems are anticipated through further scaling and miniaturization, as well as potential infrastructure cost reductions, e.g., due to co-propagation in existing fiber networks, which could bring costs into a more acceptable range. In the long term, costs are expected to stabilize at low to medium levels, making QKD technology more feasible for broader adoption.

Lack of certified and approved QKD systems:

Certification and approval are crucial for building trust in QKD technology and are even stringently required in sectors like public administration and military. In the short term, ongoing standardization and certification efforts by companies and the community are needed to establish a foundation for trust. In the medium term, the certification of the first QKD devices will be critical for increasing confidence in the technology. In the long term, established certification and approval processes for different types of QKD devices are likely to facilitate widespread adoption across various sectors.

Low awareness and demand from users:

There is a general lack of awareness regarding the benefits of and necessity for QKD among potential users. In the short term, ongoing pilot projects in various sectors should demonstrate the technology's value and effectiveness. Successful pilot projects and initial adoptions will help to increase the trust in and demand for QKD solutions in the medium term. In the long term, improved awareness and understanding of QKD's benefits are expected to drive increased adoption and investment.

Unclear business models:

The absence of clear and established business models for QKD solutions contributes to uncertainty among potential adopters. In the short term, ongoing R&D and implementation projects are essential to develop viable business models. Increased industry involvement in the medium term will lead to the establishment of various business models that clarify the value proposition of QKD. In the long term, mature technologies and markets will support a diverse range of business models, facilitating broader adoption.

Supply chain security:

Ensuring supply chain security is vital when aiming for technology sovereignty in quantum communication. In the short term, the diversification of components in QKD systems is necessary to mitigate risks. As QKD markets grow, there should be an increasing market availability of components from various vendors, which will help to diversify the market. In the medium term, a partially diversified supply chain will enhance supply chain security and limit one-sided dependencies. In the long term, ideally, a fully diversified supply chain will further strengthen the technological sovereignty of Europe in quantum communication.

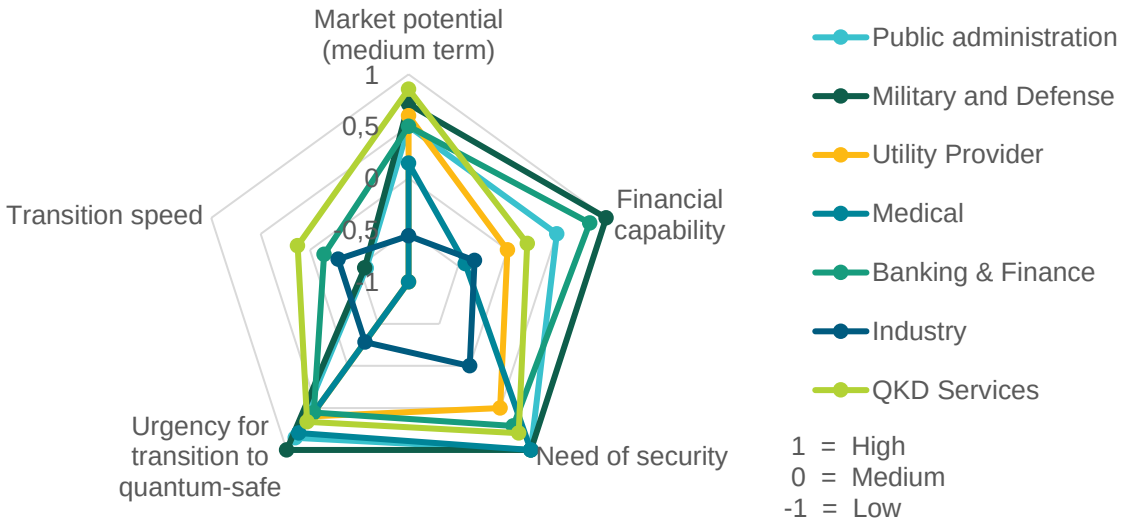
Skilled workforce:

The successful implementation of QKD technology requires a skilled workforce capable of operating and maintaining complex systems. In the short term, there may be a shortage of trained personnel. However, increasing market demand will drive efforts to cultivate a larger, skilled workforce. Continuous education and training initiatives across different levels are essential to ensure that sufficient qualified personnel are available in the long term.

7.2 Overview of Sectors

Figure 6 summarizes the results from assessing the potential application sectors including the public administration, the military and defense sector, utility provider, the medical sector, industry, and QKD services.

Figure 6: Expert assessment of different sectors according to the criteria market potential for QKD in the medium term, financial capability (and willingness to pay for security), need for and requirements of security, urgency for transition to quantum-safe cryptography (long-term criticality of data), and transition speed in the sector.



Public Administration:

The public administration is considered to be one of the key potential customers for QKD due to its need for very high data security. The currently limited maturity of QKD combined with the lack of standards, and certified and approved products are greatly hampering the use of this technology in this sector, at least in European countries. In the future, with greater maturity, and certified and approved products, the high security needs of this sector could lead to widespread adoption and a significant market. However, the transition speed in this sector is generally low.

Military and Defense:

The military and defense sector has the highest demands on communication security in terms of both short-term and long-term information sensitivity and is therefore potentially a natural adopter of QKD technologies with a reasonable market size and high financial capabilities. However, QKD must first achieve the corresponding technological maturity, as the military in most countries may only use approved technologies. For this reason and the bureaucratic processes involved, the transition speed is expected to be rather slow. However, since most military sites already have high security measures in place, implementing trusted nodes at these locations might involve significantly less effort than other use cases. Whether this enables the roll-out of a nationwide QKD network depends on the distances between these locations, which could vary greatly in different countries.

Utility Provider:

There is an emerging QKD market in the area of critical infrastructure, but this is constrained by the lack of a regulatory framework. Due to the important tasks of providing public services, the potential for QKD is considered high. From this point of view, data criticality is also high. Financial options are limited because operators need to work cost-effectively; however, if there were regulatory requirements for IT security, cost-intensive solutions could also be implemented. In this sector, the devices must be particularly robust to perform reliably in outdoor environments. Ultimately, system costs and regulatory requirements will determine the market potential in this sector.

Medical Sector:

Handling patient data is highly sensitive and the need for long-term data security is also very high. On the other hand, the medical sector has notoriously low financial capabilities and tends to only implement IT security solutions when required to do so by law. This, coupled with limited awareness and a generally very low transition speed, significantly limits the market potential for QKD in this sector.

Banking and Finance:

The banking and finance sector handles sensitive financial and customer data and has high security needs. Since business in this sector is built on the trust of its customers, QKD could have significant potential here. On the other hand, many banks are rather hesitant to implement new technologies unless they are required to do so by law. The market size is therefore assessed as medium to high in the short to medium term. This sector has the financial capabilities, but banks tend to invest with the goal of high returns. It is assumed that interest in this sector will increase once costs decrease. Then, the financial market could potentially become a major user of QKD. The transition speed here is rated as medium, as the sector is generally hesitant to implement new IT technologies, but this could accelerate if the relevant regulations require the use of quantum-safe technologies.

Industry:

Individual industrial players such as large automobile manufacturers or other large conglomerates are beginning to look at QKD solutions. However, economic feasibility depends heavily on data security requirements, technological advances, and especially cost reductions. The willingness to invest in QKD is low because security is often considered an additional service. The security level is moderate, as some data are critical, but many are only of interest to competitors. The degree of urgency varies, although company data often have to be secured for about 10 years. Technical hurdles, such as distance restrictions and integration into existing systems, complicate the introduction. Furthermore, the transition speed is slow. The advantage is that certifications are typically not required in industry.

QKD Services:

Due to QKD's promising prospects, various players are positioning themselves to offer QKD as a service. Demand for advanced security solutions will increase due to growing cybersecurity concerns and threats. The obstacles vary by sector but often involve high initial investment costs. At present, infrastructure is often being financed at least partly by research projects because telecommunication providers have to operate profitably, and QKD services are not profitable due to high costs and slow adoption. Data centers are a possible application where QKD can be used to secure very critical data through different service offers, making it potentially a financially rewarding business model. The speed of transition depends largely on the market pull, i.e., the end user demand

for QKD services, but is currently considered medium. Technological challenges include necessary infrastructure upgrades and ensuring compatibility with existing encryption standards.

Table 15: Overview of sectors and their main challenges for QKD adoption:

Sector	Assessment of sector	Main challenges for QKD adoption
Public Administration	High need for security, high urgency to transition to quantum-safe cryptography; but low transition speed and high regulatory requirements.	Technological maturity and robustness; approval of QKD products
Military and Defense	High need for security, high urgency to transition to quantum-safe cryptography, but low transition speed and high regulatory requirements.	Technological maturity and robustness; approval of QKD products
Utility Provider	Medium market potential and need for security. Market development depends on official guidelines/regulations.	Costs, robustness and official regulations
Medical sector	High need for security and urgency, at the same time rather low short and medium-term market potential due to the lack of financial capability and awareness.	High costs and lack of awareness
Banking and Finance	Medium to high market potential with high need for security and principally high financial capabilities, but often hesitant to implement new technologies.	Costs, maturity, and lack of awareness
Industry	Low market potential because of limited security needs. The level of security and the degree of urgency depend on the user and the corresponding data; transition speed is low.	Distance limitations, complexity of integration into existing systems, and costs
QKD Services	In many sectors, QKD adoption is limited due to high upfront investment costs. Offering QKD services as a business model could reduce these investment costs for the end customers significantly and could therefore have a high market potential.	Costs and awareness

7.3 QKD Systems and Their Anticipated Developments

As we look ahead to the future of QKD applications across various sectors, it is essential to anticipate the development status of the key performance indicators (KPIs) of QKD systems in the coming years. This chapter outlines a roadmap that categorizes the developmental stages of QKD technology into three perspectives: today (2025), short-term (2025-2030), and long-term (post-2035). The KPI values and features associated with these development stages were obtained from the experts and discussions during our workshop and reflect the insights and forecasts of professionals in the field. This should provide a solid understanding of the evolving landscape of QKD technology and its anticipated advancements. However, the technological variety associated with QKD is huge and the KPIs achieved by current and potential future systems are heavily dependent on the respective

framework conditions. Furthermore, most KPIs are interdependent and cannot be regarded separately (e.g., if the key rate is not of interest, impressively large distances can be achieved via fiber links). For these reasons, the following discussion can only outline the main trends and expectations concerning the future development of QKD technologies on an abstract level. The discussed KPIs are to be understood as indications of potential development trajectories, but over the entire time frame regarded, technologies with strongly deviating KPI profiles to the ones discussed here are expected to come onto the market. The purpose of introducing the following hypothetical systems is to outline what typical systems could look like and clarify which technological developments are needed to successfully implement QKD in the use cases discussed (see section 7.4).

The development timeline serves as a foundation for understanding the trajectory of QKD applications and their implications for various sectors and can be used to guide stakeholders in their strategic planning and investment decisions. As we progress through these developmental stages, the potential of QKD to enhance security in an increasingly digital world will become more and more relevant.

Development Status 1: Today

In the current QKD technology landscape, the key rate achieved is often limited to a few kilobits per second, which is scalable depending on factors such as price and distance. The technology operates effectively over distances of up to 150 kilometers, primarily utilizing fiber optics, with a preference for dark fibers. However, the system's stability remains vulnerable to large temperature changes and dust accumulation. The systems are commonly enclosed in a 19-inch rack and tailored for use by specialized technicians, which means a certain level of expertise is required to operate them. The significant maintenance required can already be partially performed by the customers themselves. For many technologies, the overall cost of implementation is around €200,000 per QKD system. Notably, current QKD systems have yet to be certified or approved by the relevant authorities in most countries.

Development Status 2: 2025 - 2030

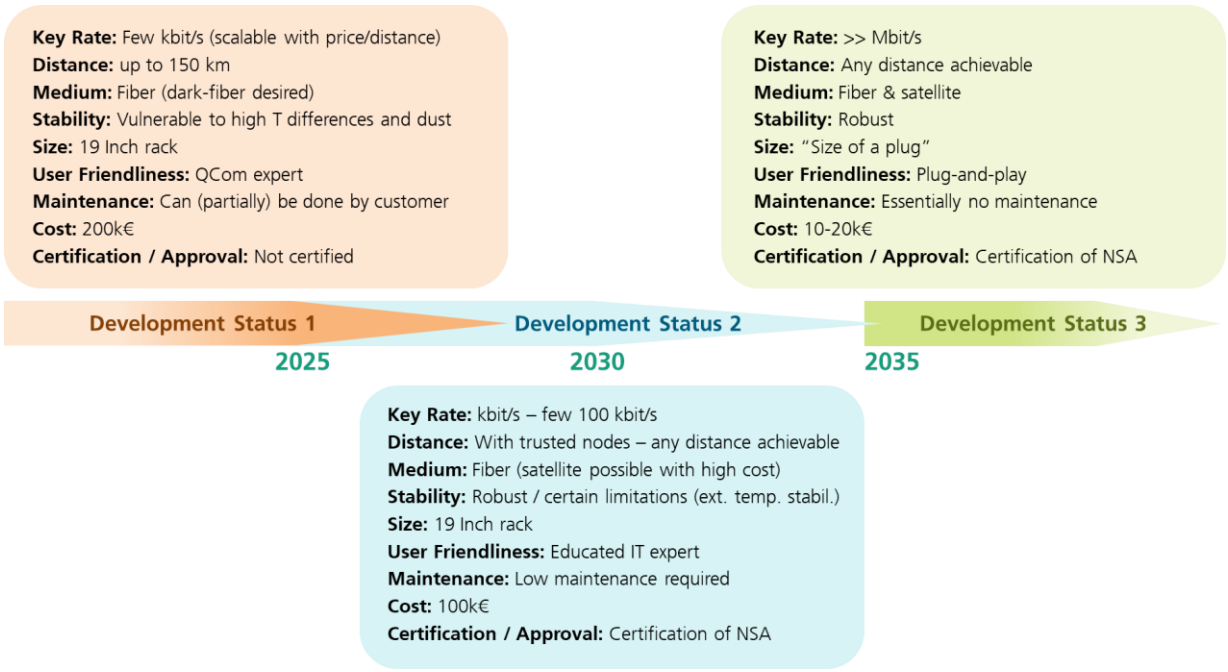
Looking ahead to the short-term horizon, experts anticipate considerable advancements in QKD technology. Key rates are likely to improve further, from a few kilobits per second to a few hundred kilobits per second, again strongly dependent on the application's implementation and requirements. In theory, the use of trusted nodes will enable fiber-based QKD over any distance. Transmission will still be predominantly via fiber optics, with the possibility of incorporating satellite technology, albeit at high cost. Stability will show marked improvement with the help of external auxiliary systems like temperature stabilization. Operating the technology will become more accessible to those with training in related fields, such as IT, which indicates reduced complexity for users. Maintenance requirements will diminish, and overall costs are projected to decrease to investments of typically €100,000 per system. Importantly, certification and approval by important national security agencies is anticipated during this period.

Development Status 3: Post-2035

In the long-term perspective, the vision of QKD technology takes a transformative path. Key rates are expected to improve to values that can ensure even very demanding use cases (potentially exceeding megabits per second). With the successful development of fiber- and satellite-based systems, QKD is possible over any distance. The system is expected to become robust, making it reliable for applications in demanding environments. Miniaturization (e.g., via photonic integration) could reduce the technology to the size of a plug, emphasizing user-friendliness with a plug-and-play design that requires minimal technical expertise. Maintenance is expected to be minimal, which increases its usability. The anticipated costs are expected to drop to figures between €10,000 and

€20,000 per system, making QKD technology more feasible for widespread adoption. Additionally, certification and/or approval by all relevant national security agencies is achieved for many QKD devices and use cases, reinforcing the legitimacy and security of the technology.

Figure 7: Possible and exemplary future development statuses of QKD systems.

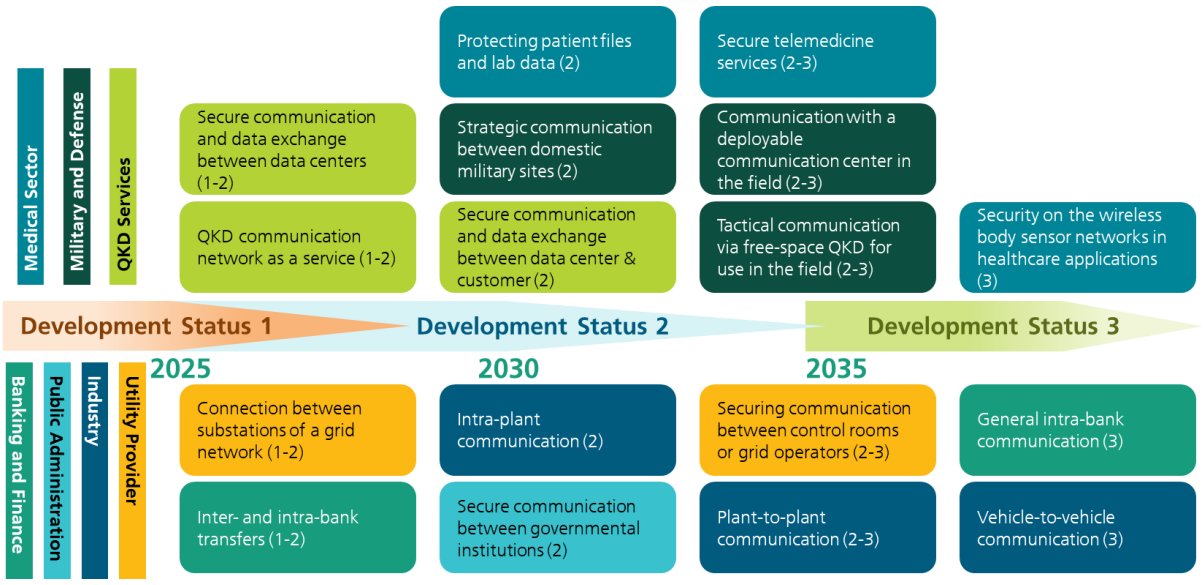


7.4 Overview of Use Cases and Timeline for Adoption

The simplified stages of the future development of QKD systems (section 7.3) can be used for a roadmap for the adoption of QKD technologies in the use cases presented in section 4.2.2. In the workshop, the use cases were matched with the development status of the previous chapter, resulting in .

While QKD will only become attractive for most use cases following further development, this analysis shows that relevant market penetration could be already reached in the next few years (Development Status 2). While extensive optimization of QKD is required to address some use cases (Development Status 3), large market shares could already be gained as soon as the technology is slightly improved and/or is certified/approved by the relevant public authorities. For some use cases, adoption is also possible in the short term, for example, to generate business offering QKD as a service or for protecting data traffic between data centers. Even though significant challenges still have to be addressed, QKD could become commercially relevant in the next few years. The following paragraphs briefly discuss the timeline for adoption of use cases in each sector and are summarized in Table 16.

Figure 8: Possible timeline of adoption of various use cases in different sectors in Europe and how they depend on the technical development stage of QKD.



Public Administration:

QKD can be used to connect governmental authorities and institutions such as ministries. This includes institutions at the state, federal and European level and could therefore constitute a significant market. High regulatory requirements currently limit the use of QKD to test projects that aim at increasing its technological maturity, implement infrastructure and bring it closer to real applications. This sector will only implement and adopt QKD products once these are approved, which could be achieved for first QKD products by 2030.

Military and Defense:

As trusted nodes could be implemented here with less effort than in other sectors, a QKD network connecting domestic military sites over large distances seems possible in the medium term (if the relevant authorities approve the technology). Connecting deployable systems using QKD-links depends on QKD satellite systems, which will take longer, as this requires conscientious mission planning and robust technologies. A roll-out of QKD for tactical use cases including mobile units, is not expected in the next decade, due to the demanding requirements and limited advantages over complementary technologies, such as PQC.

Utility provider:

QKD can be integrated into electricity, gas and water infrastructure to transmit secure control commands between key network nodes (e.g., transformer stations, pumping stations), and particularly in smart grids, to safeguard infrastructure and avert potential sabotage by preventing unauthorized control commands from being executed. QKD could also be used to secure communications data for energy or water supply between control centers or different grid providers. There are ongoing public test projects for secure communication of command control and other data related to critical infrastructure. Protection against sabotage is ensured by secure communication, among other things. The adoption of such applications is conceivable after 2030.

Medical Sector:

QKD can be used in healthcare to protect sensitive patient or laboratory data. Another important application is securing communication channels in telemedicine, which protects patient privacy

during virtual consultations. In addition, QKD could secure the transmission of wireless body sensors that collect sensitive health data such as a person's vital signs. However, this is a use case for the more distant future. In Europe, there are already various test projects for transmitting and storing data, and telemedicine. It is difficult to estimate when a breakthrough could happen as this sector has low financial capability, a low transition speed, but high data security requirements and a high degree of urgency at the same time.

Banking and Finance:

QKD can be used to secure money transfers within and between banks. There are implementation projects for this use case and a slow market adoption is likely in the next few years. Large-scale market adoption would need regulations or at least pressure from competitors. Securing all the communication between different sites of a bank represents a much larger market and would require significantly lower costs and probably miniaturized QKD systems and is thus expected only in the long term.

Industry:

QKD can be used to secure (supply chain) communications from plant to plant to protect sensitive operational data, as well as to protect and store intellectual property. This is especially critical for manufacturers operating at multiple locations. Inter-plant communications can also be secured using QKD, particularly IoT devices in smart manufacturing within increasingly digitalized production processes. For these use cases, QKD could be used without major regulatory issues, but there is currently little interest in the technology due to its high costs and the low criticality of the data involved, so these use cases are more likely to be of interest in the next decade.

In addition, QKD could provide secure communication channels between autonomous vehicles in the future, increasing safety and data integrity. However, this use case is still a distant prospect, as there is no clear plan yet for key exchanges between vehicles.

QKD Services:

QKD can be used by telecommunications providers or IT cybersecurity companies to offer QKD-secured communication networks as a service and to provide QKD infrastructure for various industries. The QKD transmission itself can also be offered as a service, including hardware, data encryption and the transmission of information. One application is secure communication between data centers to increase data security against cyberattacks. Another use case is secure communication between servers and customers, especially for cloud services. Since certifications are typically not required in the private sector, QKD services could soon be offered more widely as their costs decrease and their technical maturity increases.

Table 16: Overview of sectors, use cases, their status quo, milestones that need to be achieved before adoption, and the estimated timeframe of adoption in Europe.

Sector/Use Case	Status quo in Europe	Milestones to be achieved before adoption	Estimated timeframe of adoption in Europe
Public Administration			
Communication between ministries at state, federal and EU level	Testbeds for government use (e.g., via EuroQCI)	Increase technological maturity and robustness; certification and approval	Medium to long term
Military and Defense			
Communication between domestic military sites	Test projects ongoing, continuous observation of QKD	Robustness and technological maturity; certification and approval	Medium term
Communication to deployed communication centers in the field	No large tests so far	Robustness and technological maturity; certification and approval; Scaling of satellite QKD	Medium to long term
Communication to/from mobile/airborne/underwater units in the field	Test projects for specific use cases (e.g., underwater QKD)	Significant increase of robustness; maturity of satellite and/or free-space QKD	Long term
Utility Provider			
Connection between substations of the networks	Test projects ongoing	Robustness and technological maturity	Medium term
Securing communication between control rooms or grid operators	Test projects ongoing	Technological maturity and distance improvements	Medium to long term
Medical sector			
Protecting patient files and lab data	Test projects ongoing	Simplicity and compatibility of systems, regulatory framework	Medium to long term
Secure telemedicine services	Test projects ongoing	Comparability, miniaturization, network and distance improvements as well as price reduction	Long term
Secure body sensor networks	No test approaches so far	Miniaturization, network and distance improvements as well as price reduction	Long term
Banking and Finance			
Intra- and inter-bank transfers	Test projects ongoing	Cost reduction, regulations needed for widespread adoption	Slow implementation likely to start in the short term

Sector/Use Case	Status quo in Europe	Milestones to be achieved before adoption	Estimated timeframe of adoption in Europe
General communication between banks		Strong cost reduction and miniaturized products necessary; regulations needed for widespread adoption	Long term
Industry			
Plant-to-plant communication	Research activities in companies	Price reduction, standardization and interoperability	Medium to long term
Intra-plant communication	Research activities in companies	Price reduction, standardization and interoperability	Medium to long term
Vehicle-to-vehicle communication		Comparability, miniaturization, network and distance improvements as well as price reduction	Long term
QKD Services			
Communication network as a service	Testbeds being set up	Distances, co-propagation in existing fiber networks, costs	Medium to long term
Secure communication and data exchange	Test projects ongoing	Compatibility of systems, network improvements, cost reduction	Medium to long term
Data exchange between servers and customers		Miniaturization, compatibility, network improvements, cost reduction	Long term

8 Conclusions

The quantum computing threat on classical cryptography calls for a **transition towards quantum-safe approaches of encryption**. Considering the 'harvest now, decrypt later' approach, a transition is urgently needed – at least in sectors where the long-term security of data is required. Quantum key distribution (QKD) offers the potential to increase IT security beyond the level that is possible with classical and PQC approaches. Therefore, there is real potential for QKD adoption in various sectors, generally in combination with PQC. The public administration and military/defense sector seem very promising in the long-term due to the very high sensitivity and need for long-term security of the data. However, certification and approval and thus highly mature and robust QKD systems will be required. Furthermore, the certification and approval also require a certain lead time. Other sectors such as banking and finance, or the QKD service sector in association with private-sector clients have lower regulatory requirements and thus a greater market potential in the short-term. Several challenges still have to be overcome before QKD can be widely adopted in a variety of sectors.

QKD is still an emerging technology, and although there are already various different QKD systems on the market in 2025, they are not yet established and require improvements in terms of stability and robustness. Demonstration projects in which the integration of such devices into existing infrastructure is tested are important to further improve these technical challenges. In the coming years, **public funding for R&D projects in general, including such demonstration projects, will still be necessary in Europe**, to rapidly advance QKD technology at the interface to existing IT security infrastructure. If the various QKD systems are to be interoperable in what may be a large-scale quantum network, standards for interfaces are mandatory. Policymakers, R&D actors, industry and **the whole community should put significant efforts into standardization**, in order to make systems robust, certifiable, approvable, interoperable and integrable into existing IT security and network infrastructure. **Certification and approval are of great importance** as well for QKD adoption in the public sector and should be pursued vigorously.

The **infrastructure** itself, especially glass fiber, **needs to be rolled out**, ideally in a "quantum-ready" form, i.e. including dark fibers suitable for quantum signals. In parallel, ways of using the existing fiber infrastructure, including co-propagation with traditional signals, need to be further explored. For satellite QKD, the respective infrastructure needs to be rolled out in parallel as well. **Network management and orchestration need to be developed** and implemented or at least considered early on in order to efficiently coordinate future quantum networks. All these aspects will also lead to the efficient use of infrastructure and thus reduce the costs for the users.

Costs are currently among the biggest bottlenecks for a wide-spread adoption of QKD. Together with reducing the infrastructure costs and the development of business models for making QKD end-user friendly without the need for high upfront investments, the cost reduction of the QKD systems is of great importance. **Efforts must continue in scaling and miniaturization in order to reduce system costs**.

Awareness of the quantum threat and QKD as a possible option for quantum-safe cryptography needs to be improved. **Policymakers as well as the whole community need to raise awareness in industry, society and policy in order to ensure long-term IT security in Europe**. This bottleneck exists for all potential sectors where QKD could be adopted.

At the same time, the value chains have to be diversified, and quantum communication should move forward to **reach technological sovereignty for Europe. Quantum communication is a strategically important field of technology** and should be considered as such by policymakers, industry and society. Public funding is therefore strategically important at this early stage of development.

9 Acknowledgements

The authors gratefully acknowledge the funding by the Federal Ministry of Research, Technology and Space - Bundesministerium für Forschung, Technologie und Raumfahrt (BMFTR), Germany.

Funding reference: 16KISQ116

We would like to thank all the experts from academia and industry who supported us by participating in interviews. Furthermore, we would like to thank our colleagues from Fraunhofer ISI: Karin Herrmann for the layout, and Louise Antill-Blum, Gillian Bowman-Köhler and Barbara Sinnemann for English language corrections and translations.

We would like to thank our colleagues from PTB, UDS and BSI for their valuable input.

10 References

[1] Frank K. Wilhelm, Rainer Steinwandt, Daniel Zeuch, Paul Lageyre, Susanna Kirchhoff 2024 *Status of quantum computer development: Entwicklungsstand Quantencomputer* (Federal Office for Information Security)

[2] National Institute of Standards Technology 2024 *Announcing Approval of Three Federal Information Processing Standards (FIPS) for Post-Quantum Cryptography* https://csrc.nist.gov/News/2024/postquantum-cryptography-fips-approved (accessed 21 Mar 2025)

[3] Bennett C H and Brassard G 2014 Quantum cryptography: Public key distribution and coin tossing *Theoretical Computer Science* **560** 7–11

[4] Bennett C H, Brassard G and Mermin N D 1992 Quantum cryptography without Bell's theorem *Physical review letters* **68** 557–9

[5] Deutschen Institut für Normung DIN EN ISO/IEC 27001:2024-01, Informationssicherheit, Cybersicherheit und Datenschutz_- Informationssicherheitsmanagementsysteme_- Anforderungen (ISO/IEC_27001:2022); Deutsche Fassung EN_ISO/IEC_27001:2023 (Berlin: DIN Media GmbH) https://www.dinmedia.de/de/norm/din-en-iso-iec-27001/370680635 (accessed 7 Apr 2025)

[6] Bundesamt für Sicherheit in der Informationstechnik 2023 *IT-Grundschutz-Kompendium (Edition 2023)* https://www.bsi.bund.de/SharedDocs/Downloads/DE/BSI/Grundschutz/IT-GS-Kompendium/IT_Grundschutz_Kompendium_Edition2023.html (accessed 6 Apr 2025)

[7] Bundesgesetzblatt 2015 *Gesetz zur Erhöhung der Sicherheit informationstechnischer Systeme (IT-Sicherheitsgesetz)*

[8] Bundesgesetzblatt 2016 *Verordnung zur Bestimmung Kritischer Infrastrukturen nach dem BSI-Gesetz (BSI-Kritisverordnung - BSI-KritisV)*

[9] Dürig M and Fischer M 2018 Cybersicherheit in Kritischen Infrastrukturen *Datenschutz Datensich* **42** 209–13

[10] Marjanov T, Konstantinou M, Jóźwiak M and Spagnuelo D 2023 Data Security on the Ground: Investigating Technical and Legal Requirements under the GDPR *PoPETs* **2023** 405–17

[11] Bundesgesetzblatt 2021 *Zweites Gesetz zur Erhöhung der Sicherheit informationstechnischer Systeme (2. IT-SiG)*

[12] EU 2022 *Directive (EU) 2022/2555 of the European Parliament and of the Council of 14 December 2022 on measures for a high common level of cybersecurity across the Union, amending Regulation (EU) No 910/2014 and Directive (EU) 2018/1972, and repealing Directive (EU) 2016/1148 (NIS 2 Directive) (Text with EEA relevance)*

[13] Deutscher Bundestag 2024 *Entwurf eines Gesetzes zur Umsetzung der NIS-2-Richtlinie und zur Regelung wesentlicher Grundzüge des Informationssicherheitsmanagements in der Bundesverwaltung (NIS-2-Umsetzungs- und Cybersicherheitsstärkungsgesetz)*

[14] Falk Steiner 2025 *NIS2-Umsetzung und Kritis-Dachgesetz endgültig gescheitert* https://www.heise.de/news/NIS2-Umsetzung-und-Kritis-Dachgesetz-endgueltig-gescheitert-10259832.html (accessed 7 Apr 2025)

[15] European Commission 2022 *Directive (EU) 2022/2557 of the European Parliament and of the Council of 14 December 2022 on the resilience of critical entities and repealing Council Directive 2008/114/EC*

[16] Hornung G, Muttach J-P and Schaller T 2024 Richtlinie über die Resilienz kritischer Einrichtungen: neue Pflichten für Unternehmen und Umsetzungsbedarf in Deutschland *Computer und Recht* **40** 229–37

[17] *Entwurf eines Gesetzes zur Umsetzung der Richtlinie (EU) 2022/2557 und zur Stärkung der Resilienz kritischer Anlagen: Richtlinie (EU) 2022/2557*

[18] eco 2024 *Cybersicherheit: Nur wenige Unternehmen in Deutschland sind auf NIS2 vorbereitet* https://www.eco.de/presse/cybersicherheit-nur-wenige-unternehmen-in-deutschland-sind-auf-nis2-vorbereitet/ (accessed 21 Mar 2025)

[19] Bundesministerium des Innern und für Heimat 2024 *Rechtsrahmen für mehr Cybersicherheit: Stärkung der Zusammenarbeit von Staat und Wirtschaft im Bereich der Cybersicherheit* https://www.bmi.bund.de/DE/themen/it-und-digitalpolitik/it-und-cybersicherheit/rechtsrahmen-cybersicherheit/rechtsrahmen-cybersicherheit-node.html (accessed 21 Mar 2025)

[20] Deutscher Bundestag 2024 *Regulation (EU) 2024/2847 of the European Parliament and of the Council of 23 October 2024 on horizontal cybersecurity requirements for products with digital elements and amending Regulations (EU) No 168/2013 and (EU) 2019/1020 and Directive (EU) 2020/1828 (Cyber Resilience Act) (Text with EEA relevance)*

[21] Bressner S, Gaden N and Riediger J 2023 Der Cyber Resilience Act *Datenschutz Datensich* **47** 327–31

[22] Paar C, Pelzl J and Güneysu T 2024 *Understanding Cryptography: From Established Symmetric and Asymmetric Ciphers to Post-Quantum Algorithms* (Berlin, Heidelberg: Springer Berlin Heidelberg)

[23] Buell D 2024 *Grundlagen der Kryptographie* (Cham: Springer International Publishing)

[24] Herrmann D and Pridöhl H 2020 Basic Concepts and Models of Cybersecurity *The Ethics of Cybersecurity (The International Library of Ethics, Law and Technology)* ed M Christen *et al* (Cham: Springer International Publishing) pp 11–44

[25] Singer P W and Friedman A 2013 *Cybersecurity and cyberwar : what everyone needs to know / P.W. Singer, Allan Friedman (What everyone needs to know)* (New York: Oxford University Press, USA; Oxford University Press)

[26] Federal Office for Information Security 2024 *BSI fordert mit Partnern aus 17 EU-Mitgliedsstaaten zum Übergang zur Post-Quanten-Kryptographie auf* https://www.bsi.bund.de/DE/Service-Navi/Presse/Pressemitteilungen/Presse2024/241127_PQC-Joint-Statement.html (accessed 21 Mar 2025)

[27] IDQ *Clavis XG QKD System* https://www.idquantique.com/quantum-safe-security/products/clavis-xg-qkd-system/ (accessed 21 Mar 2025)

[28] Lucamarini M, Yuan Z L, Dynes J F and Shields A J 2018 Overcoming the rate-distance limit of quantum key distribution without quantum repeaters *Nature* **557** 400–3

[29] Zhuang S-C *et al* 2024 *Ultrabright-entanglement-based quantum key distribution over a 404-km-long optical fiber*

[30] Yin H-L *et al* 2016 Measurement-Device-Independent Quantum Key Distribution Over a 404 km Optical Fiber *Phys. Rev. Lett.* **117** 190501

[31] Liu Y *et al* 2023 Experimental Twin-Field Quantum Key Distribution over 1000 km Fiber Distance *Physical review letters* **130** 210801

[32] Orsucci D, Kleinpaß P, Meister J, Marco I D, Häusler S, Strang T, Walenta N and Moll F 2024 *Assessment of practical satellite quantum key distribution architectures for current and near-future missions*

[33] Christoph Marquardt, Ulrich Seyfarth, Sven Bettendorf, Martin Bohmann, Alexander Buchner, Marcos Curty, Dominique Elser, Silas Eul, Tobias Gehring, Nitin Jain, Thomas Klocke, Marie Reinecke, Nico Sieber, Rupert Ursin, Marc Wehling, Henning Weier 2023 *Implementation Attacks against QKD Systems* https://www.bsi.bund.de/SharedDocs/Downloads/EN/BSI/Publications/Studies/QKD-Systems/QKD-Systems.pdf?__blob=publicationFile&v=3 (accessed 25 Mar 2025)

[34] Schmaltz T, Endo C, Eßwein R, Groth J, Gruber S, Kroll H, Molina Vogelsang M, Neuhäusler P and Weymann L 2025 *Schwerpunktstudie „Quantentechnologien und Quanten-Ökosysteme"* (Expertenkommission Forschung und Innovation (EFI))

[35] OpenKRITIS 2025 *KRITIS – auf den zweiten Blick* https://www.openkritis.de/ (accessed 7 Apr 2025)

[36] Bundesamt für Sicherheit in der Informationstechnik 2024 *Orientierungshilfe zum Einsatz von Systemen zur Angriffserkennung* https://www.bsi.bund.de/SharedDocs/Downloads/DE/BSI/KRITIS/oh-sza.html (accessed 6 Apr 2025)

[37] Deutschen Institut für Normung DIN EN ISO/IEC 15408-1:2020-12, Informationstechnik_- IT-Sicherheitsverfahren_- Evaluationskriterien für IT-Sicherheit_- Teil_1: Einführung und allgemeines Modell (ISO/IEC_15408-1:2009); Deutsche Fassung EN_ISO/IEC_15408-1:2020 (Berlin: DIN Media GmbH) https://www.dinmedia.de/de/norm/din-en-iso-iec-15408-1/327254991 (accessed 7 Apr 2025)

[38] Federal Office for Information Security *Protection profiles according to Common Criteria (CC) for IT products* https://www.bsi.bund.de/DE/Themen/Unternehmen-und-Organisationen/Standards-und-Zertifizierung/Zertifizierung-und-Anerkennung/Zertifizierung-von-Produkten/Zertifizierung-nach-CC/Schutzprofile-Protection-Profiles-PP/schutzprofile-protection-profiles-pp.html (accessed 21.03.3025)

[39] CAS 2017 *Beijing-Shanghai Quantum Communication Network Put into Use* https://english.cas.cn/newsroom/archive/news_archive/nu2017/201703/t20170324_175288.shtml (accessed 28 May 2025)

[40] Mehic M *et al* 2021 Quantum Key Distribution *ACM Comput. Surv.* **53** 1–41

[41] Jinan Institute of Quantum Technology 2017 *Quantum communication network of party and government organs in Jinan* https://www.jiqt.org/index/index/show/action/science/id/19 (accessed 28)

[42] People's Daily Online 2017 *China's first commercial quantum private communication network completed* http://en.people.cn/n3/2017/0912/c90000-9268031.html

[43] ID Quantique 2022 *IDQ and SK Broadband complete phase one of nation-wide Korean QKD Network* https://www.idquantique.com/idq-and-sk-broadband-complete-phase-one-of-nation-wide-korean-qkd-network/ (accessed 28 May 2025)

[44] Korea IT News 2020 *SK Broadband to Become the First Telecommunications Company to Apply Quantum Cryptography Technology to Public Network* https://english.etnews.com/20201022200001 (accessed 28 May 2025)

[45] ID Quantique *Clavis XG Series QKD obtains National Security Certification: ID Quantique's Clavis XG: The World's First Quantum Key Distribution (QKD) Product to Obtain National Security Certification.*

[46] U.S. National Security Agency *Quantum Key Distribution (QKD) and Quantum Cryptography (QC)* https://www.nsa.gov/Cybersecurity/Quantum-Key-Distribution-QKD-and-Quantum-Cryptography-QC/ (accessed 11 Apr 2025)

[47] NCSC(National Cyber Security Centre) 2020 *Quantum security technologies* https://www.ncsc.gov.uk/whitepaper/quantum-security-technologies (accessed 28 May 2025)

[48] French Cybersecurity Agency, Federal Office for Information Security, Netherlands National Communications Security Agency and Swedish National Communications Security Authority, Swedish Armed Forces *Position Paper on Quantum Key Distribution* https://www.bsi.bund.de/SharedDocs/Downloads/EN/BSI/Crypto/Quantum_Positionspapier.pdf?__blob=publicationFile&v=4 (accessed 25 Mar 2025)

[49] European Commission 2024 *Recommendation on a Coordinated Implementation Roadmap for the transition to Post-Quantum Cryptography* https://digital-strategy.ec.europa.eu/en/library/recommendation-coordinated-implementation-roadmap-transition-post-quantum-cryptography (accessed 21 Mar 2024)

[50] BMI *BMI-OESII5-20230313-SF-A003* https://www.verwaltungsvorschriften-im-internet.de/BMI-OESII5-20230313-SF-A003.htm (accessed 28 May 2025)

[51] EU *The European Quantum Communication Infrastructure (EuroQCI) Initiative* https://digital-strategy.ec.europa.eu/en/policies/european-quantum-communication-infrastructure-euroqci?utm_source=chatgpt.com (accessed 11 Apr 2025)

[52] KIRAS Security Research *QKD4GOV – Quantum-safe Cryptography for Securing Governmental data: Establishment of a secure communication network between public authorities to investigate novel encryption schemes based on quantum key distribution (QKD) and post-quantum cryptography (PQC).* https://www.kiras.at/en/financed-proposals/detail/qkd4gov/ (accessed 21 Mar 2025)

[53] qci.dk *The Consortium* https://qci.dk/the-consortium/ (accessed 21 Mar 2025)

[54] Quantum Delta NL *Deployment of the first national quantum networks in the Netherlands* https://quantumdelta.nl/qcined (accessed 21 Mar 2025)

[55] Cao Y, Zhao Y, Wang Q, Zhang J, Ng S X and Hanzo L 2022 The Evolution of Quantum Key Distribution Networks: On the Road to the Qinternet *IEEE Commun. Surv. Tutorials* **24** 839–94

[56] Bundeswehr *Cyber and information space - a new domain* https://www.bundeswehr.de/en/organization/the-cyber-and-information-domain-service (accessed 28 May 2025)

[57] IISS 2023 *Cyber Capabilities and National Power Volume 2* https://www.iiss.org/research-paper/2023/09/cyber-capabilities-national-power-volume-2/ (accessed 7 Apr 2025)

[58] PIB Delhi 2022 *MoD all set to take a leap in Quantum Communication Technology to celebrate 'Azadi Ka Amrit Mahotsav' Bengaluru-based start-up, under iDEX, innovates advanced secured communication through Quantum Key Distribution Systems Indian Army issues commercial RFP after successful trials* https://pib.gov.in/PressReleaseIframePage.aspx?PRID=1851732 (accessed 21 Mar 2025)

[59] Ciel Qi 2024 *China's Quantum Ambitions: A Multi-Decade Focus on Quantum Communications* https://www.yalejournal.org/publications/chinas-quantum-ambitions (accessed 21 Mar 2025)

[60] NATO 2024 *Summary of NATO's Quantum Technologies Strategy* https://www.nato.int/cps/en/natohq/official_texts_221777.htm (accessed 21 Mar 2025)

[61] Krelina M 2021 Quantum technology for military applications *EPJ Quantum Technol.* **8**

[62] Bundeswehr *Standorte* https://www.bundeswehrkarriere.de/entdecker/jobs/standorte (accessed 28 May 2025)

[63] Bundeswehr *Standorte der Bundeswehr* https://www.bundeswehr.de/de/organisation/standorte-bundeswehr (accessed 30 Jan 2025)

[64] Wenning M 2023 *Ist die effiziente Nutzung von Quantenschlüsseln eine wesentliche Basis für kryptografische Sicherheit?* https://www.advasecurity.com/de-de/news-room/blog/20231023-is-efficient-use-of-quantum-keys-the-cornerstone-of-cryptographic-safety (accessed 28 May 2025)

[65] NATO *Quantum Technologies and the Science for peace and security programe* (NATO)

[66] European Defence Agency 2024 *QuantaQuest project explores application of quantum technologies in defence* https://eda.europa.eu/news-and-events/news/2024/01/19/quantaquest-project-explores-application-of-quantum-technologies-in-defence (accessed 21 Mar 2025)

[67] Universität der Bundeswehr München *MuQuaNet: Das Quanten-Netzwerk im Großraum München* https://www.unibw.de/muquanet (accessed 21 Mar 2025)

[68] Paglierani P, Fahim Raouf A H, Pelekanakis K, Petroccia R, Alves J and Uysal M 2023 A Primer on Underwater Quantum Key Distribution *Quantum Engineering* **2023** 1–26

[69] Dennis Rösch, André Kummerow, Thomas Bauer, Katerina Simou, und Friederike Wenderoth 2024 *Cyber-Fit: Investitionen in die Cybersicherheit der Stromwirtschaft: Rentabilität von Cybersicherheitsmaßnahmen* https://www.dena.de/infocenter/cyber-fit-investitionen-in-die-cybersicherheit-der-stromwirtschaft/ (accessed 6 Apr 2024)

[70] Bundesnetzagentur *IT-Si-cher-heits-ka-ta-log für Ener-gie-an-la-gen* https://www.bundesnetzagentur.de/DE/Fachthemen/ElektrizitaetundGas/Versorgungssicherheit/IT_Sicherheit/Anlagenbetreiber/start.html (accessed 2 Jun 2025)

[71] Bundesministerium für Wirtschaft und Klimaschutz 2024 *Entwurf eines Gesetzes zur Änderung des Energiewirtschaftsrechts im Bereich der Endkundenmärkte, des Netzausbaus und der Netzregulierung: Referentenentwurf des Bundesministeriums für Wirtschaft und Klimaschutz Einleitung* https://www.bmwk.de/Redaktion/DE/Downloads/Gesetz/20240828-aenderung-energiewirtschaftsrecht-endkundenmaerkte.pdf (accessed 21 Mar 2025)

[72] Liu R, Rozenman G G, Kundu N K, Chandra D and De D 2022 Towards the industrialisation of quantum key distribution in communication networks: A short survey *IET Quantum Communication* **3** 151–63

[73] *OpenQKD in Action: Our testbeds and use cases* https://openqkd.eu/openqkd-in-action/ (accessed 27 May 2025)

[74] Krüger-Brand H E 2017 *IT-Sicherheit im Krankenhaus: Cyberrisiken als Herausforderung* https://www.aerzteblatt.de/archiv/it-sicherheit-im-krankenhaus-cyberrisiken-als-herausforderung-2f538512-fb4c-4154-ab37-8221491bc22b (accessed 7 Apr 2025)

[75] Bundesamt für Bevölkerungsschutz und Katastrophenhilfe *KRITIS-Sektor: Gesundheit* https://www.bbk.bund.de/DE/Themen/Kritische-Infrastrukturen/Sektoren-Branchen/Gesundheit/gesundheit_node.html (accessed 21 Mar 2025)

[76] DKG *Informationssicherheit im Krankenhaus: Branchenspezifischer Sicherheitsstandard (B3S)* https://www.dkgev.de/themen/digitalisierung-daten/informationssicherheit-und-technischer-datenschutz/informationssicherheit-im-krankenhaus/ (accessed 28 May 2025)

[77] Bundesgesetzblatt 2019 *Gesetz für eine bessere Versorgung durch Digitalisierung und Innovation (Digitale-Versorgung-Gesetz – DVG)*

[78] Kassenärztliche Bundesvereinigung 2020 *Richtlinie nach § 75b SGB V über die Anforderungen zur Gewährleistung der IT-Sicherheit*

[79] Federal Office for Information Security *KRITIS in Zahlen* https://www.bsi.bund.de/DE/Themen/Regulierte-Wirtschaft/Kritische-Infrastrukturen/KRITIS-in-Zahlen/kritis-in-zahlen_node.html (accessed 21 Mar 2025)

[80] Tanja Bratan, Diana Schneider, Nils Heyen, Liliya Pullmann, Michael Friedewald, Dirk Kuhlmann, Nicole Brkic, Bärbel Hüsing 2022 *E-Health in Deutschland: Entwicklungsperspektiven und internationaler Vergleich* https://www.e-fi.de/fileadmin/Assets/Studien/2022/StuDIS_12_2022.pdf (accessed 6 Apr 2025)

[81] Federal Office for Information Security 2023 *Abschlussbericht Projekt CyberPraxMed – Sicherheit in Arztpraxen: Eine IT-Sicherheitsbetrachtung aktueller Arztpraxen mit Handlungsempfehlungen* https://www.bsi.bund.de/SharedDocs/Downloads/DE/BSI/DigitaleGesellschaft/CyberPraxMed_Abschlussbericht.pdf?__blob=publicationFile&v=8 (accessed 6 Apr 2025)

[82] 2024 Gesetz zur Beschleunigung der Digitalisierung des Gesundheitswesens (Digital-Gesetz — DigiG)

[83] Federal Office for Information Security *Criteria catalogue C5* https://www.bsi.bund.de/EN/Themen/Unternehmen-und-Organisationen/Informationen-und-Empfehlungen/Empfehlungen-nach-Angriffszielen/Cloud-Computing/Kriterienkatalog-C5/kriterienkatalog-c5_node.html (accessed 21 Mar 2025)

[84] Toshiba *Ensuring Long-Term-Secure Government and Medical Communications with QKD* https://www.toshiba.eu/quantum/resources/ensuring-long-term-secure-government-and-medical-communications-with-qkd/ (accessed 28 May 2025)

[85] IBM Security 2023 *Cost of a Data Breach Report 2023* https://d110erj175o600.cloudfront.net/wp-content/uploads/2023/07/25111651/Cost-of-a-Data-Breach-Report-2023.pdf (accessed 25 Mar 2025)

[86] V A D and V K 2023 Enhanced BB84 quantum cryptography protocol for secure communication in wireless body sensor networks for medical applications *Personal and ubiquitous computing* **27** 875–85

[87] ID Quantique *IDQ & SK Broadband expand use of QKD to protect critical data in South Korea* https://www.idquantique.com/id-quantique-and-sk-broadband-expand-the-use-of-quantum-key-distribution-to-protect-critical-information-in-south-korea/ (accessed 28 May 2025)

[88] KPMG AG and Bundesamt für Sicherheit in der Informationstechnik *Marktumfrage Kryptografie und Quantencomputing* (KPMG AG and Bundesamt für Sicherheit in der Informationstechnik)

[89] Federal Office for Information Security *Was sind Kritische Infrastrukturen?* https://www.bsi.bund.de/DE/Themen/Regulierte-Wirtschaft/Kritische-Infrastrukturen/Allgemeine-Infos-zu-KRITIS/allgemeine-infos-zu-kritis_node.html (accessed 21 Mar 2025)

[90] Paschou V 2024 *NIS2 vs. DORA: Unterschiede und verbreitete Missverständnisse* https://www.activemind.de/magazin/nis2-dora/ (accessed 7 Apr 2025)

[91] Joachim Wuermeling 2022 *Digitalisierung und die Zukunft der Banken: Gastbeitrag in der ZfgK anlässlich des Bundesbank-Symposiums* https://www.bundesbank.de/de/presse/gastbeitraege/digitalisierung-und-die-zukunft-der-banken-899584 (accessed 21 Mar 2025)

[92] Marcus Schmid / Nizar Jeribi 2024 *Countdown zur Cyber-Resilienz: DORA Anforderungen für den Finanzsektor umsetzen* https://de.newsroom.ibm.com/Cyber-Resilienz-DORA-Finanzsektor (accessed 7 Apr 2025)

[93] Kollmann R 2025 *Der Digital Operational Resilience Act (DORA) für mehr Cybersicherheit im Finanzbereich* https://www.tuev-nord.de/de/unternehmen/bildung/wissen-kompakt/informationssicherheit/dora-verordnung/ (accessed 7 Apr 2025)

[94] World Economic Forum and Financial Conduct Authority 2024 *Quantum Security for the Financial Sector: Informing Global Regulatory Approaches* https://www3.weforum.org/docs/WEF_Quantum_Security_for_the_Financial_Sector_2024.pdf (accessed 25 Mar 2025)

[95] Die Deutsche Kreditwirtschaft *Position Paper of the German Banking Industry Committee* (Die Deutsche Kreditwirtschaft)

[96] UK Finance 2023 *Minimising the risks - quantum technology and financial services* (UK Finance)

[97] Monetary Authority of Singapore *ADVISORY ON ADDRESSING THE CYBERSECURITY RISKS ASSOCIATED WITH QUANTUM* https://www.mas.gov.sg/-/media/mas-media-library/regulation/circulars/trpd/mas-quantum-advisory/mas-quantum-advisory.pdf (accessed 2 Jun 2025)

[98] JPMorgan 2024 *JPMorgan Chase establishes quantum-secured crypto-agile network* https://www.jpmorgan.com/technology/news/firm-establishes-quantum-secured-crypto-agile-network (accessed 21 Mar 2025)

[99] Toshiba *Quantum Key Distribution and Blockchain: Securing the Future of Financial Transactions* (Toshiba)

[100] European Insurance and Occupational Pensions Authority *Digital Operational Resilience Act (DORA)* https://www.eiopa.europa.eu/digital-operational-resilience-act-dora_en (accessed 28 May 2025)

[101] A. Poppe *et al* 2005 Practical quantum key distribution with polarization entangled photons

[102] Digital China Information Services *Quantum communication to protect financial technology* https://www.dcits.com/fintech/content_17.html (accessed 28 May 2025)

[103] Toshiba *Securing the critical link between front office and back office operations of major financial institutions* https://www.global.toshiba/ww/products-solutions/security-ict/qkd/cases/case2.html (accessed 21 Mar 2025)

[104] Matthew Beedham 2019 *Dutch researchers are developing quantum technology to secure your bank account* https://thenextweb.com/news/quantum-key-distribution-to-secure-bank-account (accessed 21 Mar 2025)

[105] ID Quantique 2020 *ID Quantique and Mt Pelerin start testing their quantum-safe digital asset custody solution in Geneva*

[106] JPMorgan 2022 *JPMorgan Chase, Toshiba and Ciena Build the First Quantum Key Distribution Network Used to Secure Mission-Critical Blockchain Application: Proof of Concept Showed Ability to Detect and Defend Against Potential Threats and Eavesdroppers* https://www.jpmorganchase.com/newsroom/press-releases/2022/jpmc-toshiba-ciena-build-first-quantum-key-distribution-network (accessed 21 Mar 2025)

[107] Bent Dalager *Quantum-safe data transfer performed at Danske Bank: In the race against cyber criminals researchers have successfully taken quantum communication out of the lab and used it to securely transfer data* https://kpmg.com/dk/en/home/media/press-releases/2022/02/quantum-safe-data-transfer-performed-at-danske-bank.html (accessed 28 May 2025)

[108] NEC 2022 *Successful Joint Verification Test for Low Latency Transmission of Highly Confidential Data Using Quantum Cryptography for Large-volume Financial Transaction Data* https://www.nec.com/en/press/202201/global_20220114_01.html (accessed 2 Jun 2025)

[109] HSBC 2023 *HSBC becomes first bank to join the UK's pioneering commercial quantum secure metro network* https://www.hsbc.com/news-and-views/news/media-releases/2023/hsbc-becomes-first-bank-to-join-the-uks-pioneering-commercial-quantum-secure-metro-network (accessed 21 Mar 2025)

[110] Monetary Authority of Singapore 2024 *MAS Collaborates with Banks and Technology Partners on Quantum Security* https://www.mas.gov.sg/news/media-releases/2024/mas-collaborates-with-banks-and-technology-partners-on-quantum-security (accessed 2 Jun 2025)

[111] Ralf Wintergerst 2024 *Wirtschaftsschutz 2024* https://www.bitkom.org/sites/main/files/2024-08/240828-bitkom-charts-wirtschaftsschutz-cybercrime.pdf (accessed 7 Apr 2025)

[112] TÜV SÜD *EU-Maschinenverordnung 2023/1230* https://www.tuvsud.com/de-de/branchen/produzierende-industrie/maschinen-geraete-ausruestung/maschinenbau/maschinenverordnung (accessed 2 Jun 2025)

[113] TÜV NORD 2024 *IT-Sicherheitsgesetz, KRITIS-Verordnung und Normen in Deutschland* https://www.tuev-nord.de/de/unternehmen/bildung/wissen-kompakt/informationssicherheit/gesetze-und-normen-zur-it-sicherheit/ (accessed 7 Apr 2025)

[114] TÜV NORD *Zertifizierung nach IEC 62443 von Cyber und Industrial Security: Sicherheit rund um die Industrie 4.0 nach neuesten Zertifizierungsstandards* https://www.tuev-nord.de/de/unternehmen/zertifizierung/produktzertifizierung/funktionale-sicherheit/sicherheit-fuer-die-industrie-40/zertifizierung-nach-iec-62443/ (accessed 21 Mar 2025)

[115] Jain N, Hoff U, Gambetta M, Rodenberg J and Gehring T 2023 *Quantum key distribution for data center security -- a feasibility study*

[116] Silvia Knittl 2023 *Cyber Security – Der Schutzschild für die globale Vernetzung* https://www.pwc.de/de/cyber-security/sicherheit-in-kritischen-infrastrukturen/cyber-security-und-kritis-in-der-it-und-telekommunikation.html (accessed 7 Apr 2025)

[117] Achim Haller *ISO 27001 ISMS – Das Informationssicherheits-Managementsystem* https://it-cybersicherheit.de/iso-27001/iso-27001-isms/ (accessed 21 Mar 2025)

[118] Bundesamt für Sicherheit in der Informationstechnik 2025 *ISO 27001-Zertifikate auf der Basis von IT-Grundschutz* https://www.bsi.bund.de/DE/Themen/Unternehmen-und-Organisationen/Standards-und-Zertifizierung/Zertifizierung-und-Anerkennung/Zertifizierung-von-

Managementsystemen/ISO-27001-Basis-IT-Grundschutz/ErteilteZertifikate/iso27001zertifikate_node.html (accessed 6 Apr 2025)

[119] Cavaliere F, Prati E, Poti L, Muhammad I and Catuogno T 2020 Secure Quantum Communication Technologies and Systems: From Labs to Markets *Quantum Reports* **2** 80–106

[120] SQuaD *Testbeds: Testbed-Karte zur Quantenkommunikation in Deutschland* https://www.squad-germany.de/testbeds/ (accessed 2 Jun 2025)

[121] AWS 2023 *Implementing a quantum-secured network in a metropolitan area* https://aws.amazon.com/de/blogs/quantum-computing/implementing-a-quantum-secured-network-in-a-metropolitan-area/ (accessed 2 Jun 2025)

[122] *DemoQuanDT: Quantenschlüsselaustausch im deutschen Telekommunikationsnetz für höhere IT-Sicherheit* https://www.forschung-it-sicherheit-kommunikationssysteme.de/projekte/demoquandt (accessed 27 May 2025)

[123] Quantum Xchange *Phio Product Guide* https://quantumxc.com/featured/phio-product-guide/ (accessed 2 Jun 2025)

[124] KPN 2016 *KPN to implement quantum encrypted connection (QKD)* https://www.overons.kpn/nieuws/en/kpn-to-implement-quantum-encrypted-connection-qkd/ (accessed 2 Jun 2025)

[125] SK Telecom *SKT Joins Hands with Equinix to Expand Quantum Business*

[126] Bozzio M, Crépeau C, Wallden P and Walther P 2024 Quantum cryptography beyond key distribution: theory and experiment *arXiv*

[127] Einstein A, Podolsky B and Rosen N 1935 Can Quantum-Mechanical Description of Physical Reality Be Considered Complete? *Phys. Rev.* **47** 777–80

[128] Greenberger D M, Horne M A and Zeilinger A 1989 Going Beyond Bell's Theorem *Bell's Theorem, Quantum Theory and Conceptions of the Universe (Fundamental Theories of Physics* vol 37*)* ed M Kafatos (Dordrecht: Springer) pp 69–72

[129] Kafatos M (ed) 1989 *Bell's Theorem, Quantum Theory and Conceptions of the Universe (Fundamental Theories of Physics* vol 37*)* (Dordrecht: Springer)

[130] Greenberger D M, Horne M A, Shimony A and Zeilinger A 1990 Bell's theorem without inequalities *American Journal of Physics* **58** 1131–43

[131] Bouwmeester D, Pan J-W, Daniell M, Weinfurter H and Zeilinger A 1999 Observation of Three-Photon Greenberger-Horne-Zeilinger Entanglement *Phys. Rev. Lett.* **82** 1345–9

[132] Hein M, Eisert J and Briegel H J 2003 Multi-party entanglement in graph states

[133] van Loock P, Weedbrook C and Gu M 2007 Building Gaussian cluster states by linear optics *Phys. Rev. A* **76**

[134] Dür W, Vidal G and Cirac J I 2000 Three qubits can be entangled in two inequivalent ways *Phys. Rev. A* **62**

[135] Kwiat P G, Mattle K, Weinfurter H, Zeilinger A, Sergienko A V and Shih Y 1995 New high-intensity source of polarization-entangled photon pairs *Phys. Rev. Lett.* **75** 4337–41

[136] Erhard M, Krenn M and Zeilinger A 2020 Advances in high-dimensional quantum entanglement *Nat Rev Phys* **2** 365–81

[137] Pan J-W, Bouwmeester D, Weinfurter H and Zeilinger A 1998 Experimental Entanglement Swapping: Entangling Photons That Never Interacted *Phys. Rev. Lett.* **80** 3891–4

[138] Häffner H *et al* 2005 Scalable multiparticle entanglement of trapped ions *Nature* **438** 643–6

[139] Bock M, Eich P, Kucera S, Kreis M, Lenhard A, Becher C and Eschner J 2018 High-fidelity entanglement between a trapped ion and a telecom photon via quantum frequency conversion *Nature communications* **9** 1998

[140] Blinov B B, Moehring D L, Duan L-M and Monroe C 2004 Observation of entanglement between a single trapped atom and a single photon *Nature* **428** 153–7

[141] Stute A, Casabone B, Schindler P, Monz T, Schmidt P O, Brandstätter B, Northup T E and Blatt R 2012 Tunable ion-photon entanglement in an optical cavity *Nature* **485** 482–5

[142] Togan E *et al* 2010 Quantum entanglement between an optical photon and a solid-state spin qubit *Nature* **466** 730–4

[143] Greve K de *et al* 2012 Quantum-dot spin-photon entanglement via frequency downconversion to telecom wavelength *Nature* **491** 421–5

[144] Tanabe T, Notomi M, Kuramochi E, Shinya A and Taniyama H 2007 Trapping and delaying photons for one nanosecond in an ultrasmall high-Q photonic-crystal nanocavity *Nature Photon* **1** 49–52

[145] Zhou Y, Malik P, Fertig F, Bock M, Bauer T, van Leent T, Zhang W, Becher C and Weinfurter H 2024 Long-Lived Quantum Memory Enabling Atom-Photon Entanglement over 101 km of Telecom Fiber *PRX Quantum* **5**

[146] Shamir A 1979 How to share a secret *Commun. ACM* **22** 612–3

[147] Hillery M, Bužek V and Berthiaume A 1999 Quantum secret sharing *Phys. Rev. A* **59** 1829–34

[148] Cleve R, Gottesman D and Lo H-K 1999 *How to Share a Quantum Secret*

[149] Barz S, Kashefi E, Broadbent A, Fitzsimons J F, Zeilinger A and Walther P 2012 Demonstration of blind quantum computing *Science (New York, N.Y.)* **335** 303–8

[150] Polacchi B, Leichtle D, Limongi L, Carvacho G, Milani G, Spagnolo N, Kaplan M, Sciarrino F and Kashefi E 2023 *Multi-client distributed blind quantum computation with the Qline architecture*

[151] Bennett, Charles H., and Gilles Brassard 1984 An update on quantum cryptography *Workshop on the theory and application of cryptographic techniques*

[152] Wiesner S 1983 Conjugate Coding *ACM Sigact News*

[153] Farhi E, Gosset D, Hassidim A, Lutomirski A and Shor P 2012 Quantum money from knots *Proceedings of the 3rd Innovations in Theoretical Computer Science Conference ITCS '12: Innovations in Theoretical Computer Science (Cambridge Massachusetts, 08 01 2012 10 01 2012) (ACM Conferences)* ed S Goldwasser (New York, NY: ACM) pp 276–89

[154] Aaronson S and Christiano P 2012 Quantum money from hidden subspaces *Proceedings of the 44th symposium on Theory of Computing STOC'12: Symposium on Theory of Computing (New York New York USA, 19 05 2012 22 05 2012) (ACM Conferences)* ed H Karloff (New York, NY: ACM) pp 41–60

[155] Kent A and Pitalúa-García D 2020 Flexible quantum tokens in spacetime *Phys. Rev. A* **101**

[156] BMBF abgerufen 2025 *Grand Challenge der Quantenkommunikation* https://www.forschung-it-sicherheit-kommunikationssysteme.de/forschung/it-sicherheit/grand-challenge-der-quantenkommunikation

[157] Ambainis A, Buhrman H, Dodis Y and Roehrig H 2003 Multiparty Quantum Coin Flipping

[158] Ganz M 2017 Quantum leader election *Quantum Inf Process* **16**

[159] Ben-Or M and Hassidim A 2005 Fast quantum byzantine agreement *Proceedings of the 37th Annual ACM Symposium on Theory of Computing: STOC'05; Baltimore, Maryland, USA, May 22 - 24, 2005 STOC05: Symposium on Theory of Computing (Baltimore MD USA, 22 05 2005 24 05 2005)* ed H Gabow and R Fagin (New York, NY: ACM Press) pp 481–5

[160] IBM 2024 *Quantum Roadmap: Strategic Milestones* https://www.ibm.com/roadmaps/quantum/

[161] HPCwire 2024 *Nu Quantum Unveils Qubit-Photon Interface to Enable Distributed Quantum Computing Networks* https://www.hpcwire.com/off-the-wire/nu-quantum-unveils-qubit-photon-interface-to-enable-distributed-quantum-computing-networks/ (accessed 2025)

[162] Holevo A S 1973 Bounds for the quantity of information transmitted by a quantum communication channel *Problemy Peredachi Informatsii*

[163] IMT-2030 (6G) Promotion Group 2021 *White Paper on 6G Vision and Candidate Technologies* (IMT-2030 (6G) Promotion Group)

[164] Ministry of Science and ICT *6G, Korea takes the lead once again '6G R&D implementation plan' established* https://www.msit.go.kr/eng/bbs/view.do?sCode=eng&bbsSeqNo=42&nttSeqNo=517 (accessed 2 Jun 2025)

[165] United Nations *Sustainable Development Goals* https://www.undp.org/sustainable-development-goals (accessed 2 Jun 2025)

[166] 2024 *German perspective on 6G - Use Cases, Technical Building Blocks and Requirements. Insights by the 6G Platform Germany. White Paper* (FAU University Press)

[167] NGMN 2022 *6G USE CASES AND ANALYSIS* (NGMN)

[168] Fettweis G and Boche H 2021 6G: The Personal Tactile Internet—And Open Questions for Information Theory *IEEE BITS Inform. Theory Mag.* **1** 71–82

[169] Mitev M, Chorti A, Poor H V and Fettweis G P 2023 What Physical Layer Security Can Do for 6G Security *IEEE Open J. Veh. Technol.* **4** 375–88

[170] Sun L and Du Q 2018 A Review of Physical Layer Security Techniques for Internet of Things: Challenges and Solutions *Entropy (Basel, Switzerland)* **20**

[171] Suomalainen J, Kotelba A, Kreku J and Lehtonen S 2018 Evaluating the Efficiency of Physical and Cryptographic Security Solutions for Quantum Immune IoT *Cryptography* **2** 5

[172] Andreas Wilkens 2024 *Glasfaser: 32,1 Prozent der Haushalte haben einen Anschluss* https://www.heise.de/news/Glasfaser-32-1-Prozent-der-Haushalte-haben-einen-Anschluss-9775583.html (accessed 2 Jun 2025)

[173] Grünenfelder F, Sax R, Boaron A and Zbinden H 2021 The limits of multiplexing quantum and classical channels: Case study of a 2.5 GHz discrete variable quantum key distribution system *Applied Physics Letters* **119**

[174] Chen T-Y *et al* 2021 Implementation of a 46-node quantum metropolitan area network *npj Quantum Inf* **7**

[175] Martin V *et al* 2024 MadQCI: a heterogeneous and scalable SDN-QKD network deployed in production facilities *npj Quantum Inf* **10**

[176] Bundesministerium für Bildung und Forschung 2024 *Wichtiger Erfolg auf dem Weg zu Quantenkommunikationsnetzwerken: Zweites QuNET-Schlüsselexperiment: Die vom Bundesforschungsministerium geförderte QuNET-Initiative vernetzt in der Metropolregion Berlin erstmals mehrere Nutzende gleichzeitig quantengesichert miteinander.* https://www.forschung-

it-sicherheit-kommunikationssysteme.de/service/aktuelles/qunet-schluesselexperiment?utm_source=chatgpt.com (accessed 11 Apr 2025)

[177] Dynes J F *et al* 2019 Cambridge quantum network *npj Quantum Inf* **5**

[178] Sasaki M *et al* 2011 Field test of quantum key distribution in the Tokyo QKD Network *Optics express* **19** 10387–409

[179] *HellasQCI: Greece strengthens the resilience of its critical infrastructure against cyber threats by leveraging quantum technologies* https://hellasqci.eu/ (accessed 2 Jun 2025)

[180] QuNET abgerufen 2024 *Die QuNET-Initiative* https://qunet-initiative.de/

[181] Diamanti E, Lo H-K, Qi B and Yuan Z 2016 Practical challenges in quantum key distribution *npj Quantum Inf* **2**

[182] Brazaola-Vicario A, Ruiz A, Lage O, Jacob E and Astorga J 2024 Quantum key distribution: a survey on current vulnerability trends and potential implementation risks *Opt. Continuum* **3** 1438

[183] Bruno N *et al* 2016 Heralded amplification of photonic qubits *Optics express* **24** 125–33

[184] Krutyanskiy V, Canteri M, Meraner M, Bate J, Krcmarsky V, Schupp J, Sangouard N and Lanyon B P 2023 Telecom-Wavelength Quantum Repeater Node Based on a Trapped-Ion Processor *Physical review letters* **130** 213601

[185] Briegel H-J, Dür W, Cirac J I and Zoller P 1998 *Quantum repeaters for communication*

[186] Cao Y, Zhao Y, Lin R, Yu X, Zhang J and Chen J 2019 Multi-tenant secret-key assignment over quantum key distribution networks *Optics express* **27** 2544–61

[187] Chen Y-A *et al* 2021 An integrated space-to-ground quantum communication network over 4,600 kilometres *Nature* **589** 214–9

[188] Liao S-K *et al* 2017 Satellite-to-ground quantum key distribution *Nature* **549** 43–7

[189] European Comission abgerufen 2024 *The European Quantum Communication Infrastructure (EuroQCI) Initiative* https://digital-strategy.ec.europa.eu/en/policies/european-quantum-communication-infrastructure-euroqci

[190] Castelvecchi D 2018 The quantum internet has arrived (and it hasn't) *Nature* **554** 289–92

[191] Pompili M *et al* 2021 Realization of a multinode quantum network of remote solid-state qubits *Science (New York, N.Y.)* **372** 259–64

[192] Wehner S, Elkouss D and Hanson R 2018 Quantum internet: A vision for the road ahead *Science (New York, N.Y.)* **362**

[193] Andreas Poppe *Open QKD: Open European Quantum Key Distribution Testbed*

[194] EU 2019 *Technical agreement signed for a European plan on quantum communication infrastructure* https://digital-strategy.ec.europa.eu/en/news/technical-agreement-signed-european-plan-quantum-communication-infrastructure (accessed 11 Apr 2025)

[195] EU *Quantum communication infrastructure (EuroQCI)* https://hadea.ec.europa.eu/programmes/connecting-europe-facility/about/quantum-communication-infrastructure-euroqci_en (accessed 13 Apr 2025)

[196] EU 2025 *Kommission und Europäische Weltraumorganisation unterzeichnen EuroQCI-Umsetzungsvereinbarung* https://digital-strategy.ec.europa.eu/de/news/commission-and-european-space-agency-sign-euroqci-implementation-agreement (accessed 13 Apr 2025)

[197] EU 2022 *EuroQCI CONOPS (Betriebskonzept)* https://digital-strategy.ec.europa.eu/de/miscellaneous/euroqci-conops-concept-operations (accessed 13 Apr 2025)

[198] DIN e. V. *SQuaD: Schirmprojekt Quantenkommunikation Deutschland* https://www.din.de/de/forschung-und-innovation/partner-in-forschungsprojekten/ki/squad (accessed 28 May 2025)

[199] SQuaD 2024 *Results of the Workshops on Requirements Analysis of Norms and Standards for Qcom published* https://www.squad-germany.de/en/results-of-the-workshops-on-needs-analysis-of-norms-and-standards-for-qcom-published/ (accessed 28 May 2025)

[200] DIN e. V. *NA 043-02-05 AA: Quantentechnologien* https://www.din.de/de/wdc-grem:din21:360529594 (accessed 13 Apr 2025)

[201] CEN *CEN/CLC/JTC 22: Quantum Technologies* https://standards.cencenelec.eu/dyn/www/f?p=205:7:0::::FSP_ORG_ID:3197951&cs=15741D1431D56DC6C1EC9D1C3C9B8A385 (accessed 13 Apr 2025)

[202] CEN *CEN/CLC/JTC 22/WG 4: Quantum Communication and Quantum Cryptography* https://standards.cencenelec.eu/dyn/www/f?p=205:7:0::::FSP_ORG_ID:3317382&cs=11DAE6C6C13C31C1B4D6A7E635FCBEDF7 (accessed 13 Apr 2025)

[203] ISO 2024 *IEC/ISO JTC 3: Quantum technologies* https://www.iso.org/committee/10138914.html (accessed 13 Apr 2025)

[204] Federal Office for Information Security *BSI homepage* https://www.bsi.bund.de/ (accessed 28 May 2025)

[205] ETSI *Industry Specification Group (ISG) on Quantum Key Distribution (QKD)* https://www.etsi.org/committee/qkd (accessed 13 Apr 2025)

[206] ETSI *Technical Committee (TC) CYBER (Cybersecurity)* https://www.etsi.org/committee/cyber (accessed 28 May 2025)

[207] ITU 2025 *ITU-T Study Group 13: Future networks, with focus on IMT-2020, cloud computing and trusted network infrastructure* https://www.itu.int/en/ITU-T/about/groups/Pages/sg13.aspx (accessed 13 Apr 2025)

[208] ITU 2025 *ITU-T Study Group 17 - Security* https://www.itu.int/en/ITU-T/about/groups/Pages/sg17.aspx (accessed 13 Apr 2025)

[209] ITU 2025 *ITU-T Focus Group on Quantum Information Technology for Networks (FG-QIT4N)* https://www.itu.int/en/ITU-T/focusgroups/qit4n/Pages/default.aspx (accessed 13 Apr 2025)

[210] IRTF *Quantum Internet Research Group QIRG* https://www.irtf.org/qirg.html (accessed 13 Apr 2025)

[211] IRTF *Crypto Forum Research Group CFRG* https://www.irtf.org/cfrg.html (accessed 12 Apr 2025)

[212] ETSI 2024 *ETSI GS QKD 016 V2.1.1: Quantum Key Distribution (QKD); Common Criteria Protection Profile - Pair of Prepare and Measure Quantum Key Distribution Modules* (ETSI)

[213] TAA 2025 *TTA Issues Security Function Certificate for Korea's First Quantum Key Distribution Equipment (QKD)*

[214] Federal Office for Information Security 2024 *Verfahrensbeschreibung zur Zertifizierung von Produkten (VB-Produkte.PD) - Version 5.1* https://www.bsi.bund.de/SharedDocs/Downloads/DE/BSI/Zertifizierung/VB-Produkte.html?nn=127500 (accessed 28 May 2025)

[215] Federal Office for Information Security *Zulassung*
https://www.bsi.bund.de/DE/Themen/Oeffentliche-Verwaltung/Zulassung/zulassung_node.html (accessed 28 May 2025)

[216] Federal Office for Information Security *Liste CC / ITSEC Prüfstellen*
https://www.bsi.bund.de/DE/Themen/Unternehmen-und-Organisationen/Standards-und-Zertifizierung/Zertifizierung-und-Anerkennung/Zertifizierung-von-Produkten/Zertifizierung-nach-TR/Pruefstellen-Auditoren/Liste_CC-Pruefstellen/Liste_CC-Pruefstellen_node.html (accessed 28 May 2025)