Bundesministerium
Klimaschutz, Umwelt,
Energie, Mobilität,
Innovation und Technologie

Bayerisches Staatsministerium
für Digitales

Quantenverschlüsselte Kommunikation ohne Grenzen

Studie zu Konzeption und Machbarkeit eines bayerisch-österreichischen QCI-Testbeds

Wien, Erlangen 2021

Impressum

Medieninhaber, Verleger und Herausgeber:
Bundesministerium für Klimaschutz, Umwelt, Energie, Mobilität, Innovation und Technologie, Radetzkystraße 2, 1030 Wien

Autoren: Hannes Hübel, Florian Kutschera, Stefan Petscharnig, Martin Stierle
AIT Austrian Institute of Technology GmbH
Giefinggasse 4, 1210 Wien
+43 50 550 – 0
office@ait.ac.at
ait.ac.at

und

Christoph Marquardt
Max Planck Institute for the Science of Light
Staudtstraße 2, 91058 Erlangen
+49 (0)9131 7133 401
MPLpresse@mpl.mpg.de
https://mpl.mpg.de/de/

Wien, 2021. Stand: 27. Oktober 2021

Vorwort

Mit dem Start der Quantum Communication Infrastructure Initiative (EuroQCI) gibt es die Vision eines pan-europäischen Kommunikationsnetzwerkes basierend auf Quantenkommunikation. In der ersten Stufe von EuroQCI (5-Jahre Ziel) ist das Ausrollen eines QKD-Netzwerkes zur abhörsicheren Datenkommunikation zwischen Behörden in Europa geplant.

Die technologische Reife der QKD-Geräte ist bereits so weit fortgeschritten, dass sie im Feldeinsatz zu größeren Netzwerken zusammengeschlossen und getestet werden können. Dieser Schritt geht jedoch weit über die bisherigen QKD-Netzwerk-Demonstrationen hinaus, die lokal in kleinen urbanen Fasernetzwerken gezeigt wurden.

Transnationale QKD-Verbindungen sind an sich keine Besonderheit oder Neuheit, wenn, wie bisher publiziert, die QKD-Module Alice und Bob sowie das Key-Management von demselben Lieferanten kommen und von der selben Betreiber:in gemanagt werden.

Was bisher weder demonstriert noch in der Standardisierung festgelegt wurde, ist eine Situation in der zwei verschiedene QKD-Netzwerkbetreiber:innen aus verschiedenen Staaten ihre Netze zusammenschließen. Im Falle eines europäischen QCI-Netzes ist jedoch mit Sicherheit davon auszugehen, dass insbesondere an den nationalen Grenzen unterschiedliche QKD-Betreiber:innen ihre Netze zusammenschalten müssen. Dies beinhaltet sowohl technische aber auch organisatorische, sicherheitstechnische und regulatorische Fragestellungen.

Wie dieses Thema gelöst werden kann, ist die zentrale Frage der vorliegenden Studie.

In Kapitel 1 werden die physischen Anforderungen an einen Grenzknoten für die Zusammenschaltung von zwei QKD-Netzwerken betrachtet. Diese Anforderungen sind in Kapitel 1.1. dargestellt und unterscheiden sich nicht von Anforderungen an Kollokationsräume in der Telekommunikation. In Kapitel 1.2. sind jene Prozesse zusammengestellt, die für die Implementierung eines Betreibermodells festgelegt werden müssen. Hierfür gibt es in Europa noch keine bekannten und publizierten Vorbilder. Allerdings sind die meisten Themen in der Telekommunikationsbranche mit Spezifikationen für andere Technologien in ähnlicher Form bekannt.

Im Kapitel 2 wird das Thema „QKD-Key-Management-System“ sehr ausführlich und umfangreich dargestellt. Die Vorgehensweise wurde vor allem deshalb gewählt, weil es

bisher keinen Standard für den Zusammenschluss von zwei QKD-Netzwerken gibt. Die verschiedenen dargestellten Aspekte des Key Managements spannen quasi den Entscheidungsraum auf für die Beantwortung der in Kapitel 3 gestellten zentralen Fragen. Diese müssen für eine Zusammenschaltung von zwei nationalen QKD-Netzwerken beantwortet und in den Key Management Systemen der beteiligten Staaten implementiert werden:

- Wie werden Knoten Domain-übergreifend identifiziert und adressiert? Gibt es zentrale KMS-Instanzen für die nationalen Subnetze?
- Wie werden die Routen für die Schlüsselverteilung hergestellt?
- Wer darf die Verbindungen auf- und abbauen?
- Wie erfolgt die Verrechnung und/oder Ressourcenbudgetierung?

In Kapitel 4 wird das Thema der Streckenführung von einem Wiener Knoten z. B. ein Standort eines Bundesministeriums an die Grenze nach Bayern beispielshaft aufgezeigt. Wichtig an dieser Stelle ist die abgeleitete Größenordnung der Zahl der benötigten QKD-Verbindungen und der Trusted-Repeater-Standorte.

In Kapitel 5 wird die Streckenführung und Anbindung von einem Münchner Knoten an die Grenze nach Österreich diskutiert.

In Kapitel 6 werden die relevanten Schlussfolgerungen aus dieser Studie zusammengestellt. Dabei werden insbesondere jene Themen dargestellt, die beim Design künftiger Projekte für QKD-Testnetzwerke beachtet werden sollten.

In den Anhängen sind relevante QKD-Standards und verwendete Abkürzungen zusammengestellt.

Inhalt

Executive Summary

Ziel der vorliegenden Studie ist es, die Machbarkeit eines bayerisch-österreichischen QCI-Testbed aufzuzeigen und insbesondere jene Themen herauszuarbeiten, die für eine Umsetzung von zentraler Bedeutung sind.

Das zentrale Ergebnis der Studie ist, dass die Zusammenführung mehrerer nationaler QKD-Netzwerke mit unterschiedlichen Operator-Schlüsselverwaltungs-Systemen zu einem gesamten Netzwerk machbar ist. Allerdings wurden diesbezügliche Analysen und Architekturüberlegungen bisher nirgends veröffentlicht und nach bestem Wissen der Studienautoren auch nicht durchgeführt. Das EU-Programm CEF - Connecting Europe Facility könnte zur Errichtung eines bayerisch-österreichischen QKD-Testbeds genutzt werden.

Im Rahmen der klassischen Telekommunikation ist es seit Jahrzehnten selbstverständlich, Netzwerke unterschiedlicher Betreiber:innen an sogenannten Interconnection-Standorten zusammenzuschalten. Dies galt früher insbesondere für Sprachnetzwerke und SS7-Verkehr und heute für IP-Netzwerke. Sämtliche Funktionen für das Zusammenspiel der Netzwerke von der Adressierung bis zum Monitoring von Quality-of-Service-Parametern und notwendigen Information für die Verrechnung sind für die Telekommunikationsnetzwerke durch Implementierung der relevanten Standards beispielsweise in den Routern technisch umgesetzt.

Für das Zusammenschalten von zwei oder mehreren QKD-Netzwerken unterschiedlicher Betreiber:innen sieht die Welt aktuell noch anders aus. Es gibt hier einerseits keine geeigneten Standards und andererseits auch keine geeigneten Architekturüberlegungen. Obwohl im Rahmen von EuroQCI mehrere Studien zur Spezifikation der EuroQCI-Architektur gestartet wurden, liegen hier noch keinerlei Ergebnisse vor, wie QKD-Netzwerke unterschiedlicher Domainen miteinander verbunden werden können. Die zentrale Rolle spielt hierbei das QKD-Key-Management-System.

Aus diesem Grund hat sich die vorliegende Studie ganz zentral mit dem Thema QKD-Key-Management-System auseinandergesetzt. Im Rahmen der Studie haben wir gezeigt, dass die Verknüpfung von zwei QKD-Key-Management-Systemen für unterschiedliche QKD-Netzwerke möglich ist. Die Herausforderung besteht jedoch darin, dass bereits für das

Key-Management-System eines QKD-Netzwerks in einem Staat eine Vielzahl von Freiheitsgraden existiert, die aktuell nicht durch Standardisierung festgelegt sind. Für das Zusammenspiel zweier QKD-Key-Management Systeme müssen daher technische Spezifikationen für beide Systeme verbindlich festgelegt werden und darüber hinaus Fragen zur Adressierung, zum Routing und zum Verbindungsauf- und -abbau festgelegt und implementiert werden.

Weiterhin wurde im Rahmen der Studie gezeigt, dass die Themen Sicherheitsstandards am Übergabepunkt, Trusted Repeater Standorte und Wegeführung keine größere Herausforderung für die Umsetzung eines bi- oder multi-nationalen QCI Testbeds darstellen.

Im Rahmen der Studie wurden auch die Prozesse für den Betrieb eines QKD-Netzwerkes betrachtet. Es geht hier im Wesentlichen um die Themen Planung, Errichtung, Wartung und Entstörung sowie Abbau von QKD-Geräten in einem Netzwerk. Hierzu gibt es zwar keine Publikationen. Allerdings sind die Prozesse geübte Praxis in Telekommunikations-unternehmen und unterscheiden sich für QKD-Geräte nicht besonders von anderen Telekommunikationsgeräten.

Die Definition von übergreifenden Prozessen und die Festlegung von geeigneten Qualitätsparametern und Service Level Agreements wären jedoch Themen, die in einem künftigen Projekt für ein grenzüberschreitendes QCI-Testbed spezifiziert werden sollten. Hier spielt auch die Frage der Governance und Transparenz gegenüber den anderen QKD-Domainen eine Rolle, z. B. will man anderen Mitgliedsstaaten mitteilen, welche kritischen Infrastrukturen im eigenen Land über QKD adressierbar sind und welche nicht?

Zusätzlich sollten in einem künftigen Projekt für ein grenzüberschreitendes QCI-Testbed Themen wie Verrechnungsansätze und Haftungsfragen für das Zusammenschalten von QKD-Netzwerken bearbeitet werden.

Das von der EU vorbereitete Connecting Europe Facility Programm sieht den Aufbau transnationaler QCI-Testbeds vor. In einem gemeinsamen bayerisch-österreichischen Projekt könnten die in der Studie herausgearbeiteten Fragen zur Zusammenführung unterschiedlicher QKD-KMS, zur transnationalen Synchronisation und Transparenz der Prozesse, zur transnationalen Produktspezifikation für das QoS sowie zur Haftung gegenüber den Endkunden getestet und beantwortet werden.

1 Spezifikationen für die Zusammenführung von zwei nationalen Testbeds an einem Übergabepunkt

Abbildung 1 Übersichtsbild für die Zusammenschaltung von QKD-Netzwerken an der Grenze Bayern - Österreich

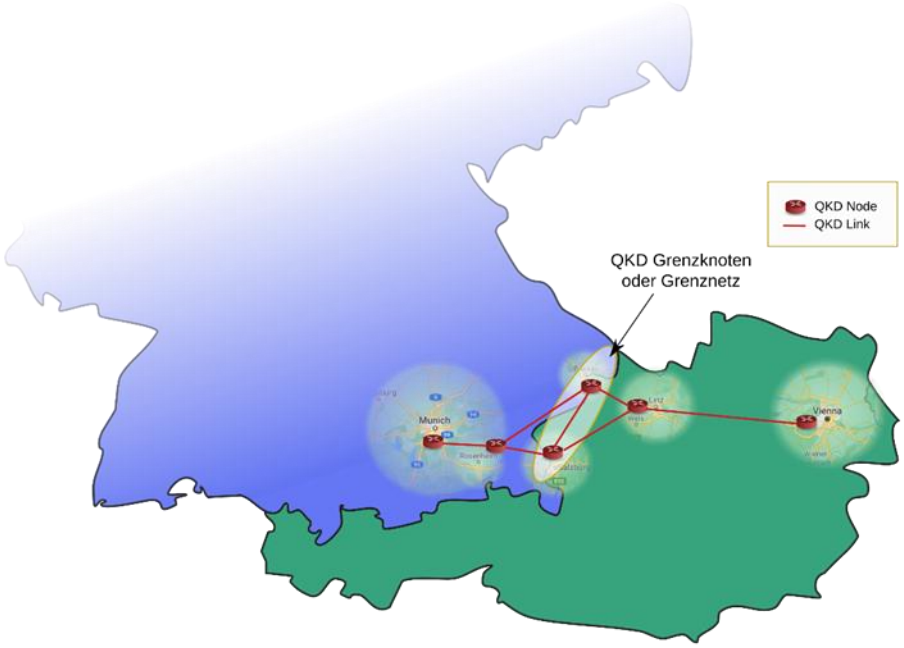


Abbildung 1 skizziert eine mögliche Verbindung zwischen einem QKD-Netzwerk in München mit einem in Wien. Prinzipiell könnte eine deutsche Betreiber:in ihr QKD-Netzwerk bis nach Wien aufbauen oder eine österreichische Betreiber:in bis nach München. Das zentrale Thema der Studie ist die Definition des Übergabepunktes zwischen zwei QKD- Netzwerken. Zur besseren Veranschaulichung wurde in Abbildung 1 jedoch die Grenze als geeigneter Ort der Zusammenschaltung der QKD-Netze in Bayern und Österreich gewählt.

Die Darstellung der Pfade stellt die physikalischen Notwendigkeiten für den Quantenkanal dar, der zum Austausch der QuBits dient. Zusätzlich zum Quantenkanal gibt es einen klassischen Kanal, der in der Betrachtung vorausgesetzt ist und dessen Einschränkungen und Limitationen bezüglich der Bandbreite oder zeitlichen Verfügbarkeit im Vergleich zum Quantenkanal vernachlässigbar sind.

1.1 Physische Anforderungen an einen Übergabepunkt

Die technischen Anforderungen eines Grenzknotens unterscheiden sich nur unwesentlich von denen eines Trusted-Nodes innerhalb des QKD-Netzwerkes.

Für die Standortauswahl und die Sicherheitsstandards am Übergabepunkt kommen dieselben Normen und Vorschriften zur Anwendung wie für klassische Telekommunikationsinfrastruktur. Es handelt sich dabei insbesondere um folgende Normen

- EN 50600 Informationstechnik
- Einrichtungen und Infrastrukturen von Rechenzentren
- VDS 2463 Übertragungseinrichtungen für Gefahrenmeldungen
- Netz- und Informationssystemsicherheitsgesetz (NISG)

Dies bedeutet, dass bei der Standortsicherheit die Umgebungsrisiken betrachtet werden müssen. Hierzu zählen die relevanten Risikofaktoren für den Brandschutz wie z. B.

- Brand in der Umgebung
- Feuer und/oder Rauchentwicklung in der Übergabestation
- Explosionsgefährdende Produktions- und Lagerstätten in der Umgebung

Ähnliches gilt für die relevanten Risikofaktoren aus der physikalischen Umgebung, wie z. B.

- Hochwasser- und Überschwemmungsgebiet
- Extremwetterlagen und ungünstige klimatische Bedingungen (Regen, Hagel, Schnee, Blitze)
- Verkehrswege – Gefahrengut und Katastrophen (Straßenverkehrswege, Bahn, Flugverkehr)
- Schwingungswellen (Hammerwerke, Gleisanlagen)

- Trümmerkegel höherer Bauwerke
- Erschütterung durch Erdbeben
- Eindringen von Verschmutzungen
- Luftverunreinigung - natürliche Ursachen
- Unterirdische Hohlräume

Auch die elektrische Betriebsumgebung wie etwa die Störfestigkeit und die Empfindlichkeit gegenüber elektromagnetischer Felder sind zu betrachten.

Ein wichtiger Aspekt ist die Absicherung gegen Fremdzugriff. Hierbei sind folgende Themen von Relevanz:

- Fremdzugriff und Diebstahl
- Einbruch bzw. unkontrolliertes, unbefugtes Betreten des Standortes
- Sabotage und Vandalismus
- unkontrolliertes Arbeiten in Räumlichkeiten mit mehreren Mietern

Für die Absicherung des Standorts kommen die folgenden Normen zur Anwendung.

- Sicherheitseinrichtungen lt. zugrundeliegendem Sicherheitskonzept auf Basis der Risikoanalyse
- Überwachung/Sicherheitstechnik z. B.: gemäß ÖVE Richtlinien 2910
- bauliche Sicherheit/Einbruchschutz z. B.: gemäß EN 1627, Nationaler Anhang A DIN 1627
- Brandschutz
- baulich z. B.: gemäß OIB RL, Bauordnung bundesländerspezifisch, EN 1363-1, EN 1047-2
- technisch z. B.: gemäß EN 54

Für die Verfügbarkeit sind bei der Standortauswahl noch die Themen der elektrischen Versorgung, d. h. Notstrom sowie unterbrechungsfreie Stromversorgung (USV) und das Thema der Klimatisierung von Relevanz. Die folgenden Normen sind hier zu betrachten:

- Elektrische Versorgung angelehnt an EN 50600–2-2
- Klimatisierung angelehnt an EN 50600-2-3, ASHRAE 9.9
- Fernwartung und Meldenetz z. B.: gemäß EN 50518-1
- Erdung und Potentialausgleich z. B.: gemäß EN 50310, E 8101

1.1.1 Conclusio

Bestehende Standorte für Telekommunikationseinrichtungen oder Rechenzentren erfüllen normalerweise die beschriebenen Anforderungen.

1.2 Betreibermodell und Governance

Zur Spezifikation eines Betreibermodells für QKD-Netzwerke müssen zumindest die folgenden Themen festgelegt werden.

- Prozesse für die Planung neuer QKD-Verbindungen einschließlich der Bewertung neuer Standorte, Leitungen und QKD-Systeme.
- Prozesse für die Abnahme neuer Standorte, die Messung und Abnahme neuer Leitungen sowie Abnahmeprozesse für die Installation und Inbetriebnahme neuer QKD-Geräte.
- Prozesse im Bereich der Qualitätssicherung der QKD-Netzwerke im Bereich der Überwachung, Fernwartung, SW-Updates, sowie Entstörung.

Im Planungsprozess wird eine detaillierte Risikoanalyse für die ausgewählten Standorte, eine Streckenplanung mit Dämpfungsabschätzung sowie die Auswahl des am besten geeigneten QKD-Lieferanten abhängig von der Netzwerktopologie erfolgen.

Im Installationsprozess muss dann die Abnahme des Standorts, die Abnahme der Leitung durch Dämpfungsmessung und entsprechendem Übergabeprotokoll, die Inbetriebnahme des QKD-Geräts sowie die Integration des QKD-Geräts in das Key-Management-System (KMS) erfolgen.

Im Rahmen der Betriebsprozesse geht es um das Monitoring und allenfalls die Entstörung der QKD-Systeme. Zusätzlich braucht es insbesondere aufgrund der Sicherheitsrelevanz der Trusted Repeater klare Prozesse für die Bewältigung von Sicherheitsvorfällen bei unbefugtem Zugang zu den Standorten des QKD-Netzwerks. Schließlich muss die Verfügbarkeit der Glasfasern durch geeignetes SLA-Management überwacht werden.

1.2.1 Conclusio

Es existieren bisher in Europa keine größeren QKD-Netzwerk-Installationen. Die meisten QKD-Links werden nach dem Konsortium vorliegenden Informationen von der Herstellerfirma IdQuantique betrieben.

Im Testnetzwerk in Madrid arbeiten Huawei, die Technische Universität Madrid sowie Telefonica zusammen. Unterlagen zu Betreibermodellen sind bisher nicht öffentlich zugänglich.

Die hier genannten Prozessthemen sollten daher in den künftigen Testnetzwerken im Rahmen des Digital Europe Programms entwickelt werden.

1.3 Betreibermodell spezifisch

Für den Betrieb eines österreichischen QCI-Testnetzwerks kommen prinzipiell folgende Betreiber:innen in Fragen:

- Ein Telekommunikationsunternehmen wie z. B.: A1, Magenta, 3, oder kleinere lokalere Betreiber:innen wie Energie AG, Wien Energie etc.
- Ein IT-Integrator wie z.B: Kapsch, ACP, S&T
- Kleinere IT Security Firmen wie z. B.: ARES CI etc.

Solange das QCI-Netzwerk noch ein Testnetzwerk ist, könnte es auch vom ACONet oder einer Forschungseinrichtung betrieben werden.

Sobald jedoch klassifizierte Daten im QCI-Testnetzwerk übertragen werden, kommen ACONet und Forschungseinrichtung wegen allfälliger Haftungsthemen als Betreiber:innen nicht mehr in Frage.

1.3.1 Conclusio

Zur Vorbereitung eines nationalen Testnetzwerkes bzw. eines transnationalen bayerisch-österreichischen Testnetzwerks sollten zumindest die oben genannten Unternehmen bezüglich des jeweiligen Interesses zum Betrieb des QCI-Testbeds abgefragt werden.

2 Das QKD-Key-Management- System (QKD-KMS)

2.1 QKD-KMS Charakterisierung

Ein QKD-Key-Management-System (KMS) unterscheidet sich gegenüber klassischen Key-Management-Systemen durch folgende Aspekte:

- Ein QKD-KMS stellt informationstheoretisch sicheres Schlüsselmaterial für kryptographische Verfahren bereit.
- Die Quantenschlüssel sind Einmalschlüssel. Das heißt, dass das Schlüsselmaterial, welches in kryptographischen Prozessen wie Verschlüsselung oder Authentifizierung verwendet wird, nach der Anwendung vernichtet wird.
- Die verwalteten Quantenschlüssel sind rein symmetrisch. Dies bedeutet, dass eine Sicherheitsverletzung schweren Schaden verursachen kann. Eine Angreifer:in, welche in den Besitz eines Schlüssels kommt, kann sofort eine Chiffre, welche eben durch diesen Schlüssel geschützt wird, entschlüsseln. Da Quantenschlüssel üblicherweise als Einmalschlüssel verwendet werden, begrenzt sich in diesem Fall der Schaden auf diese eine Offenlegung.
- QKD-KMS bedienen ein Synchronisierungsprotokoll, um eine homogene Verteilung von Schlüsselmaterial entlang eines Pfades durch das QKD-Netz zu gewährleisten. Dieses Protokoll wird üblicherweise selbst durch Quantenschlüssel abgesichert.

Abgesehen von diesen oben angeführten Eigenschaften sind QKD-KMS reine Logikbausteine, welche in Software umgesetzt werden. Haben QKD-Geräte über quantenphysikalische Effekte Schlüsselmaterial produziert, dann erinnert aus der Sicht eines QKD-KMS nichts mehr an den „Quanten-Ursprung“ des erzeugten Schlüssels. Wird der Schlüssel vom QKD-Gerät an das KMS übergeben, dann gilt dieser Schlüssel als Zeichenkette mit maximaler Entropie, welcher über die gleiche Identifikation bei genau einem Peer dieses KMS geteilt wird. Dieser Peer-KMS muss nicht zwingend über einen physikalischen Quantenkanal verbunden sein. Die alleinige Tatsache, dass ein bestimmter Schlüssel mit einem anderen Peer-KMS geteilt wird, stellt eine logische, wenn auch nicht direkt physikalische, Verbindung von KMS-Systemen dar.

Abbildung 2 logische Schlüsselverbindungen zwischen nicht direkt benachbarten KMS

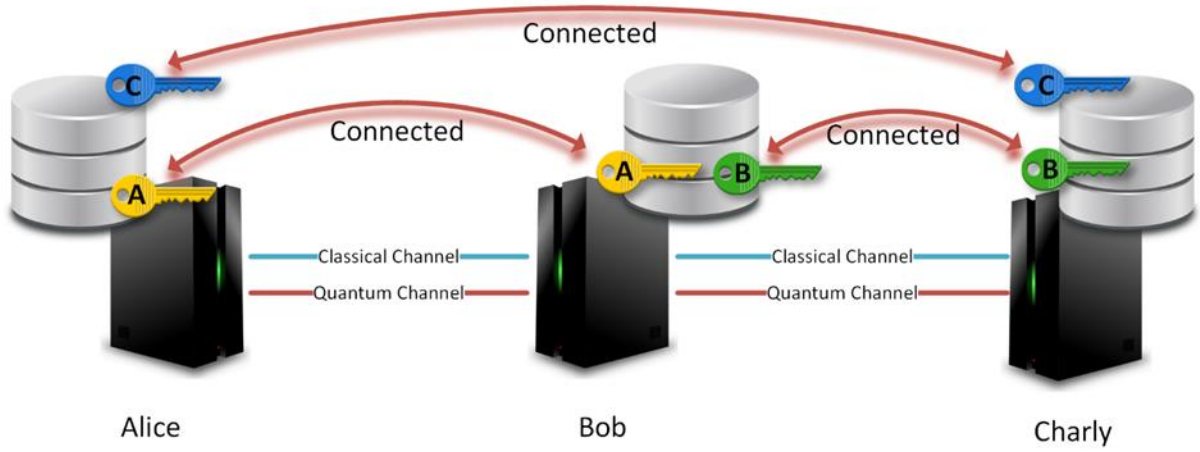


Abbildung 2 stellt diesen Zusammenhang dar. Die KMS-Systeme bei Alice und Bob teilen sich gemeinsam den Schlüssel A, während Bob und Charly sich den Schlüssel B teilen. Schlüssel C wird nun zwischen Alice und Charly geteilt, ohne dass eine direkte physikalische Verbindung besteht. Dennoch gilt das KMS bei Alice und das KMS bei Charly als über diesen Schlüssel C verbunden. Eine Verbindung zwischen zwei KMS ist daher stets als eine logische Verbindung zu sehen, welche über verschiedene tatsächliche physikalische Kanäle realisiert werden kann. Schlüssel A und B gelten dabei als direkte Schlüssel, C hingegen als indirekter.

Da die verwaltenden Schlüssel in den KMS selbst im Grunde „nur“ Bitsequenzen mit einem Satz an ebenfalls klassischen Metainformationen sind, können die KMS an Alice und Charly nicht eindeutig feststellen – sofern die Metadaten nicht Gegenteiliges anzeigen – ob der Schlüssel C mittels QKD erzeugt wurde oder aber als reine Zufallszahl durch Operator an beiden Stellen in das System gebracht wurde. Somit kann Schlüssel C als Initialschlüssel für neue direkte quantenphysikalische Verbindungen zwischen Alice und Charly betrachtet oder für eine „direkte“ klassische verschlüsselte oder authentifizierte Kommunikation zwischen Alice und Charly verwendet werden.

2.1.1 Conclusio

Durch die einfache XOR Operation können die informationstheoretisch sicheren Schlüssel der Teilstücke in eine Kette von A nach B und nach C zu einem informationstheoretisch sicheren Schlüssel von A nach C zusammengesetzt werden.

2.2 KMS im Netzwerk

2.2.1 Planes

Eine moderne Methode zur Strukturierung und Klassifizierung der Funktionalitäten eines Netzwerks ist die Anwendung des Begriffs der Planes (Netzwerkebenen). Planes sind Gruppierungen von Netzwerkfunktionen, die unterschiedlichen Zwecken dienen und unterschiedliche Schnittstellen haben.

Mit dem Aufkommen von SDN (und insbesondere OpenFlow) gewannen Protokolle und Komponenten von Netzwerkmodellen, die sich unabhängig von ihrer Position in einem hierarchischen Schichtenmodell in ihrer Intention und ihren Daten unterscheiden, an Bedeutung und rückten moderne Netzwerkarchitekturen und -analysen in den Mittelpunkt.

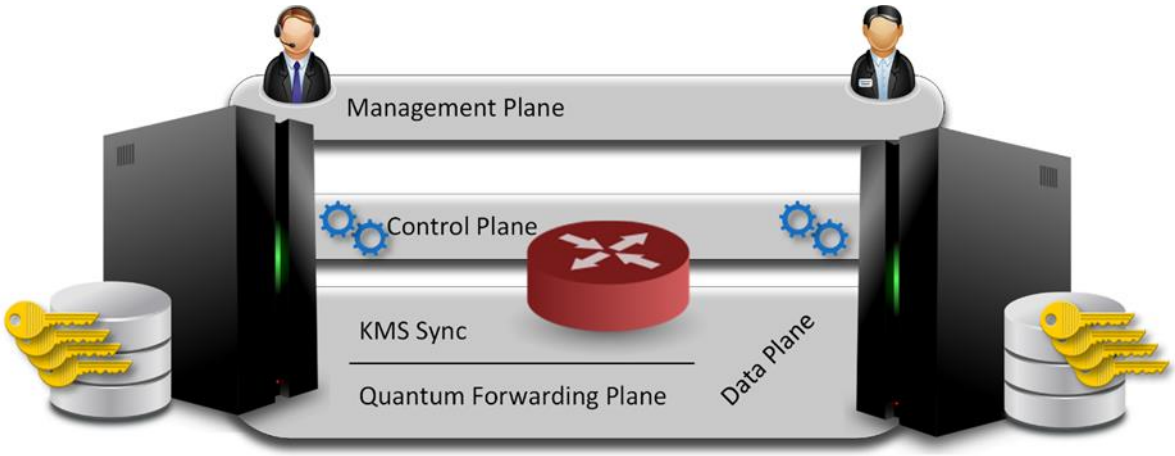
Netzwerkebenen gruppieren Komponenten, d. h. in Software- oder Hardware-Entitäten verkörperte Protokolle und API sowie deren Artefakte (wie Routing-Tabellen) grob in drei Ebenen:

- die Benutzer:in- oder Datenebene: Data Plane.
- die Steuerungsebene: Control Plane.
- die Managementebene: Management Plane.

Abb. 3 skizziert die Einbettung eines QKD-KMS in die Data Plane eines Netzwerkes. In einem Quantennetzwerk fungiert die Quantum Forwarding Plane (QFP) als Datenebene in einer untersten Schicht und stellt die Menge der Funktionalitäten dar, die der Erzeugung, der Manipulation, dem Transport und der Messung von Quantensignalen und der damit verbundenen klassischen Verarbeitung im Auftrag der Quantenkommunikationsprotokolle (QLCP – Quantum Level Communication Protocol) gewidmet sind.

Ein Kommunikationsprotokoll auf dieser Quantenebene ist der Satz von Operationen auf Quanten- und klassischen Signalen, die es zwei entfernten Parteien ermöglichen, QuBits zu übertragen oder, im Allgemeinen, nicht-klassische Korrelationen zu teilen. Ein QLCP kann die Messung von Quantensignalen und die klassische Verarbeitung beinhalten, die erforderlich ist, um das Endergebnis zu erhalten, wie eben einen Schlüssel.

Abbildung 3 QKD-KMS in der Data Plane



Alle QKD-Protokolle (Prepare and Measure, Measurement Device Independent oder Entanglement Based) sind Kommunikationsprotokolle auf Quantenebene, wobei diese Definition auch die Weiterleitung symmetrischer Schlüssel einschließt. Diese Definition umfasst auch Verschränkungsaufbau- und Fehlerkorrekturprotokolle, bis hin zu Bell-Messungen als Mittel zur Verschränkungsweiterleitung in zukünftigen Quantumrepeatern.

Das QKD-KMS nutzt die QFP als Data Plane für die Ermittlung direkter Schlüssel und zur Synchronisation mit dem Partner:in-KMS. Zusammen mit dem QFP kann nun das QKD-KMS eine Data Plane für beliebige Ende-zu-Ende-Schlüsselpaare darstellen.

2.2.2 Schichten

Neben dem modernen Ansatz der Netzwerkplanes hat das konventionelle Model der Schichten eines Netzwerks nach wie vor große Bedeutung. Abb. 4 zeigt die Einordnung des QKD-KMS im Sinn des Netzwerkschichtenmodells.

Abbildung 4 Verortung des QKD-KMS mit Ende-zu-Ende-QKD im TCP/IP Netzwerk Schichtenmodel

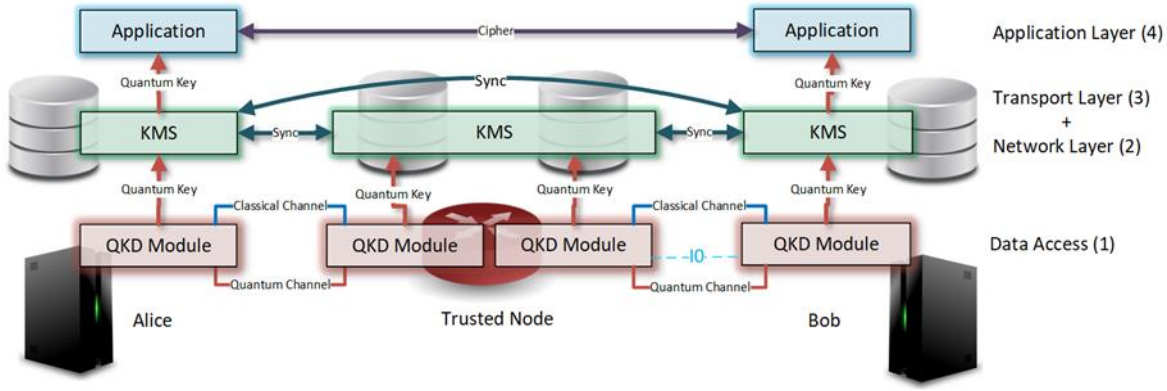


Abb. 4 zeigt das Netzwerkschichtenmodel mit QKD-KMS. Auf der untersten Schicht sind die QKD-Module. Diese führen die QLCP-Protokolle („Data Access“) sowie das QKD-Post-Processing wie in der QFP beschrieben. Darauf aufbauend nimmt das QKD-KMS die Schlüssel entgegen und gewährleistet eine Schlüsselspeichersynchronisation mit dem direkten Nachbarn („Network Layer“), beziehungsweise baut synchronisierte Schlüssel-speicher mit nicht benachbarten KMS auf. Auf Anfrage werden nun Applikationen Ende-zu-Ende-Schlüssel ausgegeben („Applikation Layer“). Die Applikationen müssen dabei nicht unbedingt user-zentrische Applikationen sein, wie im Peer-to-peer-Model, sondern können auch Server im Service-to-Service-Modus sein, welche Dienste für Benutzer:innen, welche z. B. gerade offline sind, vorhalten.

2.2.3 KMS-Arten

KMS-Systeme kann man aufgrund der Verortung in einem QKD-Netzwerk und der zur Verfügung gestellten Funktionalität in verschiedene Klassen einteilen.

Tabelle 1 KMS-Klassen

Name	Beschreibung
Key Buffer	Schlüsselverwaltungseinheit auf dem QKD-Gerät. Der Key-Buffer ist kein voll funktionsfähiges QKD-KMS, jedoch benötigen QKD-Geräte ebenfalls einen Speicherort für ihre produzierten Schlüssel. Die darin gehaltenen Schlüssel werden an das eigentliche KMS am QKD-Knoten weitergeleitet.
Plattform KMS	Ein Plattform-KMS ist dasjenige KMS an einem QKD-Knoten, welches die generierten Schlüssel eines QKD-Geräts entgegennimmt. Dabei handelt es sich um die tatsächlich generierten Schlüssel einer Quantenleitung.
Operator KMS	Das Operator-KMS kann mit beliebig vielen anderen Operator-KMS in einem Netzwerk gemeinsame Schlüsselspeicher auf- und abbauen. Im Mittelpunkt steht hier die Ende-zu-Ende-Verbindung aufgrund der gespeicherten Schlüsseldaten sowie die Weiterleitung (Routing) der Userdaten (grundsätzlich ein weiterer Schlüssel).
Service KMS	Ein Service-KMS ist nun ein Operator-KMS, welches in der Lage ist, Anfragen von Applikationen entgegen zu nehmen, einen Zufallszahl mit einem QRNG (TRNG) zu erzeugen und diese als User Schlüssel an die Applikation auszuhändigen.

Ein KMS an einem QKD-Knoten kann gleichzeitig Service-, Operator- und Plattform-KMS sein. Ein Service- und Operator-KMS muss allerdings nicht zwingend ein Plattform-KMS sein, jedoch muss für dessen Betrieb das Schlüsselmaterial „nachgefüllt“ werden, wenn dieses nicht durch die Plattform-KMS Eigenschaft garantiert wird.

Ein Operator-KMS übernimmt die Verteilung und Transport von Schlüsselmaterial an benachbarte und nicht benachbarte KMS. Ein Plattform-KMS ist somit immer auch ein Operator-KMS.

Letztlich sind Service-KMS an den User Geräten, an den eigentlichen Servicerechnern oder aber an den Ingress- und Egress-Knoten eines QKD-Netzwerks zu finden. Ein Service-KMS ist immer auch ein Operator-KMS.

Die technische Implementation dieser verschiedenen KMS-Arten muss sich nicht unterscheiden, sondern kann durch eine einzige Software bereitgestellt werden.

2.2.4 Conclusio

Aktuell unterscheiden die QKD-Lieferanten nicht zwischen Plattform-, Operator- und Service-KMS. Dadurch ergibt sich im wesentlichen eine Lieferantensituation mit Vendor-Lock in.

Es sind bisher keine QKD-Netzwerke mit unterschiedlichen QKD-Link-Lieferanten mit einem gemeinsamen KMS bekannt. Darüber hinaus gibt es auch kein QKD-Gesamtnetzwerk in dem zwei unterschiedliche Operator-KMS zu einem gesamten KMS zusammengeschalten sind.

Beides wird jedoch für ein grenzüberschreitendes QKD-Netzwerk relevant.

2.3 Schlüsselausgabe

Greifen Applikationen auf die Schlüssel eines lokalen QKD-KMS zu, so haben sich in der bisherigen Diskussion zwei unterschiedliche Paradigmen bei der Schlüsselkonsumation herauskristallisiert:

- Einmalschlüsselsysteme
- Schlüsselstromsysteme

Beide Verfahren weisen Vor- als auch Nachteile auf und ein Verfahren allein eignet sich nicht pauschal für alle Applikationstypen und -muster.

2.3.1 Einmalschlüssel

Der wohl naheliegende Ansatz ist der des Einmalschlüssels: die Applikation fordert das lokale KMS auf, für jeden einzelnen Vorgang einen Schlüssel zur Verfügung zu stellen. Diese Anfrage ist jedes Mal erneut zu formulieren und somit losgelöst von vorherigen Anfragen.

Das daraus resultierende Interface and Processing ist sehr einfach, da abgesehen von einer reduzierten AAA[1]-Verwaltung keine applikationsspezifischen Zustände am lokalen

[1] AAA: Authentication, Authorization and Accounting.

KMS gehalten werden müssen. Dieses Vorgehen lässt sich sehr schnell und leicht als RESTful-Webservice implementieren.

Damit ist ebenfalls auch schon der Nachteil induziert: dieses Verfahren verfügt über kein Session-Konzept und kann daher nativ kein QoS einfordern. Die Schlüsselausgabe bleibt „best effort“, weil kein beteiligtes KMS für den zukünftigen Schlüsselverbrauch Ende-zu-Ende heuristisch stichhaltige Aussagen machen kann.

Dennoch können die Applikationen punktuelle Schlüsselmerkmale anfragen, sofern die KMS-Implementationen diese unterstützen.

Beispiele:

- Nur direkte Schlüssel.
- Schlüssel, welche nicht über bestimmte Knoten oder Subnetze erzeugt wurden.
- Schlüssel, welche nur von bestimmten QKD-Geräten erzeugt wurden.
- Schlüssel, welche nicht von bestimmten QKD-Geräten erzeugt wurden.
- Schlüssel mit einem maximalen ε.

Da jedoch ein Sessionkonzept in diesem Ansatz fehlt, ist ein Auflösen dieser Anforderungen mit einem Zusatzaufwand in der Implementierung des Protokolls verbunden.

Die primäre Entität dieser Systeme ist der Schlüssel selbst, d. h. Schlüssel müssen eindeutig im Netzwerk identifizierbar sein und Peer-Applikationen müssen über die Identität der jeweils gewählten Schlüssel Einigkeit erreichen.

Dieses Verfahren eignet sich somit für alle Applikationen, die keine QoS-Anforderungen stellen müssen und Daten zeitverzögert oder offline zur Verfügung stellen. Beispiel sind: QKD-Email, QKD-Data-Storage & Archive, …

Vorteile:

- Einfachheit.
- Zustandslos.
- Leicht zu implementieren.

Nachteile:

- Nur Best Effort, keine QoS-Garantien möglich.
- Anfragen mit Qualitätsangaben an Schlüssel komplex zu integrieren.

Beispiele:

- ETSI Standard GS QKD 014: „Quantum Key Distribution (QKD); Protocol and data format of REST-based key delivery API“

2.3.2 Schlüsselstrom

Dem Einmalschlüsselansatz steht das Verfahren des Schlüsselstroms gegenüber. Beide Applikationen vereinbaren zeitgleich einen Schlüsselstrom, über den konkrete Schlüssel auf beiden Seiten der Verbindung ausgeteilt werden. Dieser Schlüsselstrom erzwingt daher ein Sessionkonzept, auf welches das Ende-zu-Ende-QKD-KMS-Netzwerk reagieren kann, um QoS durchzusetzen.

Neben einem „Best Effort“ könnten Applikationen einen Mindestdurchsatz an Schlüsselmaterial fordern, oder Pfade über das Netzwerk definieren (z. B. nur Schlüssel von Geräten eines bestimmen Herstellers oder nur Schlüssel, an deren Konstruktion Geräte eines Herstellers nicht beteiligt waren), oder Schlüssel mit einem maximalen ε angefordert werden. Da das Sessionkonzept ein zentraler Bestandteil ist, können auf diesem aufbauend weitere QoS-Merkmale einfacher definiert werden[2].

Die primäre Entität dieser Systeme ist nicht der Schlüssel selbst, sondern der Schlüsselstrom, über den die beteiligten Applikationen und das KMS Einigung erzielen. Die jeweiligen Applikationen tauschen untereinander nicht die ID eines Schlüssels, sondern die ID des Schlüsselstroms aus. Können beide Applikationen auf ihrer Seite den Schlüsselstrom eindeutig und zweifelsfrei adressieren, dann werden in Folge einzelne Schlüssel an den jeweiligen Enden der Verbindung sequentiell ausgeteilt.

[2] Das bedeutet nicht, dass der Einmalschlüsselansatz nicht ebenfalls ein entsprechendes QoS anbieten kann. Bei Einmalschlüssel ist das allerdings punktuell jedes Mal erneut zu verhandeln. Für das Schlüsselstrom-Konzept ist diese Eigenschaft der QoS fundamental.

Da ein Schlüsselstrom eine Verbindung durch das QKD-Netzwerk darstellt, können hier ebenfalls Circuit- oder Label-Switching-Technologien angeknüpft sein.

Einmalschlüsselsysteme lassen sich auf Schlüsselstromsysteme aufbauen: Erstellen einer Verbindung mit Best-Effort-QoS, Austeilen des Schlüssels, Abbau der Verbindung.

Dieses Verfahren eignet sich für Applikationen, welche zeitgleich operieren und ein Mindestmaß an Qualität einfordern: QKD-Live-Telekommunikation, QKD-Streaming, QKD-enhanced VPNs, …

Dem gegenüber steht, dass der Entwurf und die Umsetzung dieses Verfahrens wesentlich komplexer scheint als Einmalschlüsselsysteme. Auch sind die QKD-KMS-Systeme, und damit das gesamte QKD-KMS-Netzwerk, nicht mehr zustandsfrei: die errichteten, offenen Sessions binden Ressourcen.

Vorteile:

- QoS
- Aufbauend von bestehendem Session-Konzept können weitere Qualitätsanforderungen einfach integriert werden.

Nachteile:

- Komplexer im Vergleich zu Einmalschlüssel.

Beispiele:

- ETSI Standard GS QKD 004: „Quantum Key Distribution (QKD); Application Interface“

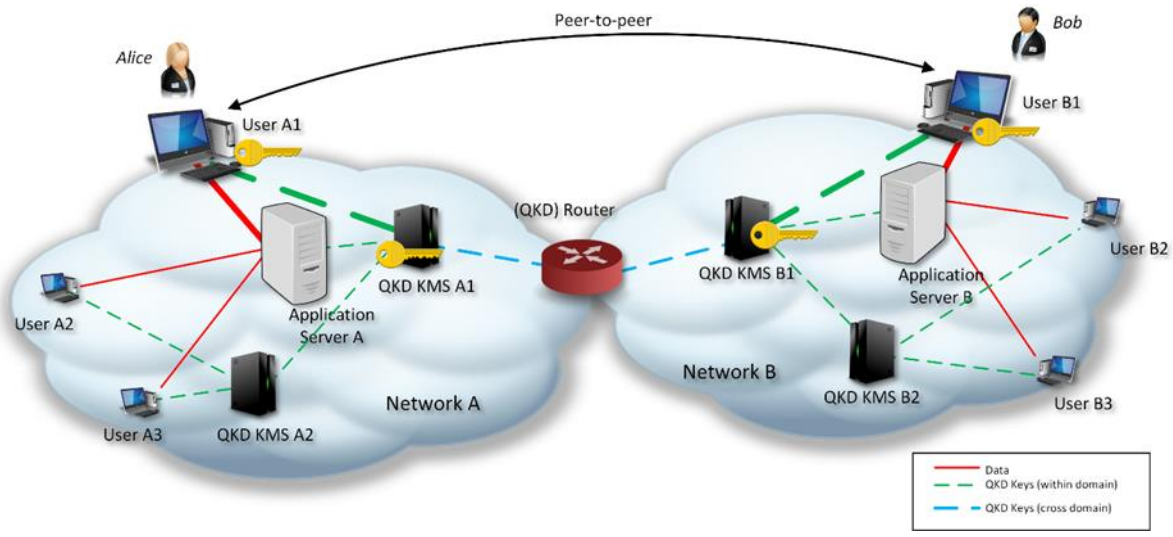
2.4 Schlüsselkonsumation

Ein weiterer Aspekt ist die Schlüsselkonsumation, welche unterschiedliches Applikationsverhalten abbildet.

2.4.1 Peer-to-Peer

Der naheliegende Ansatz ist, die Schlüssel direkt an die Applikation der jeweiligen Clientsysteme zu liefern. Dort verarbeiten die laufenden Applikationen das Schlüsselmaterial entsprechend.

Abbildung 5 Peer-to-peer-Schlüssel Verbrauch.



Dies bedeutet auch, dass das ausgehändigte Schlüsselmaterial nahe zum oder am Verbrauchspunkt gespeichert wird. Alle restlichen Netzwerkeinheiten halten damit keine Ressourcen für den konkreten Anwendungsfall. Die involvierten Applikationsserver stellen entweder die Serviceinfrastruktur oder speichern die verschlüsselten und/oder authentifizierten Daten.

Beispiel: mit QKD abgesicherte Telekommunikation.

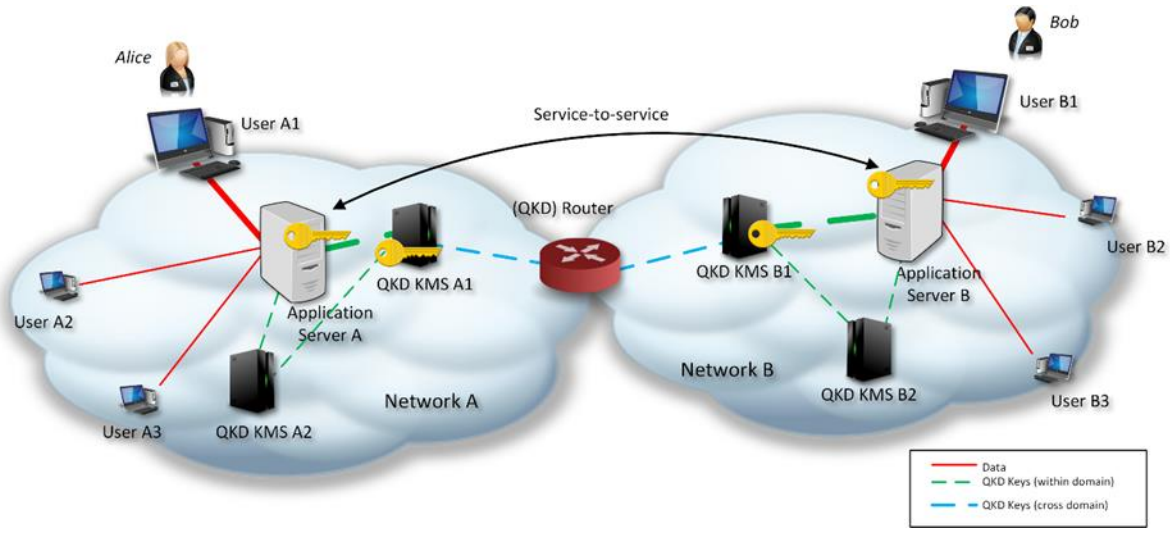
- Alice auf dem Gerät „User A1“ möchte eine Live-Kommunikation mit Bob auf „User B1“.
- Auf den Endgeräten wird gleichzeitig eine entsprechende Kommunikationsapplikation gestartet.
- Die Applikationsserver A und B stellen dabei die Verbindungen her und leiten die Kommunikation.
- Über die QKD-KMS-A1 und QKD-KMS-B1 beziehen nun die Usergeräte Schlüssel und verschlüsseln und authentifizieren die Kommunikation.
- Die Kommunikation wird als Chiffrat über die Applikation-Server ausgetauscht.

Bei diesem Verfahren müssen die Applikationen auf den Clientrechner die lokale Schlüsselverwaltung übernehmen und die kryptographischen Prozesse durchführen. Die QKD-Schlüssel werden von den KMS an die Clientrechner geliefert und scheiden dann aus dem Netzwerk aus.

2.4.2 Service-to-Service

Dem gegenüber steht der Service-to-Service-Ansatz. Hierbei wird das Schlüsselmaterial nicht an die Clientrechner übertragen, sondern an die Applikationsserver, welche die Daten verarbeiten. Die Clientapplikationen müssen dabei nicht gleichzeitig online und aktiv sein. Darüber hinaus müssen diese Anwendungen nicht mit QKD relevanten Funktionen ergänzt werden.

Abbildung 6 Service-to-Service QKD-Key-Konsumation



Beispiel: verschlüsselte Email.

- Alice auf dem Gerät „User A1“ möchte QKD-verschlüsselte Emails an „Bob“ senden.
- Sie bedient ihren Emailclient in gewohnter Weise, ohne QKD relevante Ergänzungen.
- Der Applikationsserver A (Emailserver) erkennt (bsp. auf Basis der Zieladresse „bob@qkd.networkB“), dass diese Nachricht zu verschlüsseln ist.
- Applikationsserver A verbindet sich mit Applikationsserver B und beide einigen sich auf entsprechendes Schlüsselmaterial, welches sie aus ihren jeweiligen lokalen Netzen von QKD-KMS A1 und QKD-KMS B1 beziehen.
- Applikationsserver A verschlüsselt die Email und sendet sie an Applikationsserver B.
- Applikationsserver B speichert die Nachricht und den Schlüssel für Bob.
- Zeitversetzt später meldet sich Bob auf Client B2 an und fragt seine Emails ab. Dabei erkennt der Applikationsserver B die neue Email, entschlüsselt diese und händigt diese Bob aus.

Dieses Muster ist geprägt durch das Behalten und Speichern des Schlüssels nachdem er zur Anwendung kam. D. h. die Applikationsserver verknüpfen Schlüssel aus den QKD-KMS mit konkreten Userdaten und halten das Chiffrat sowie die Schlüssel auf Anfrage bereit[3]. Ein weiteres Beispiel für diesen Anwendungsfall sind Datacenter oder QKD-Cloud Lösungen.

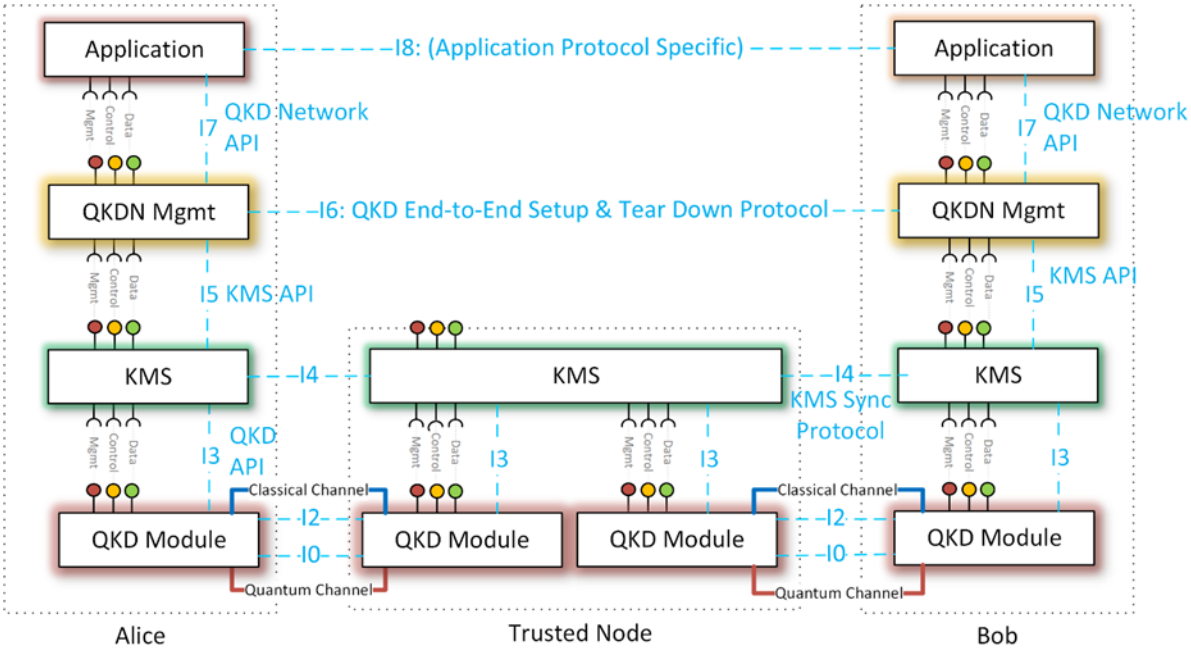
[3] Dabei empfiehlt sich ausdrücklich die physikalische Trennung von Daten und Schlüsselmaterial im System.

Auch werden die Daten zwischen den Clientrechnern und den Applikationsserver im Klartext übertragen, was Einfluss auf den zu definierenden und einzuhaltenden Security-Perimeter hat.

2.5 KMS-Interfaces

Abb. 7 stellt die verschiedenen Schnittstellen im Kontext einer QKD-KMS-Diskussion dar. Diese Abbildung orientiert sich dabei an dem Schichtenmodell von Netzwerkstrukturen (bsp. ISO/OSI Layer), verweist aber auch auf den Plane Ansatz beim Inkludieren einzelner Schnittstellen der Data-, Control- und Managementplane.

Abbildung 7 KMS Interfaces



Die Menge an Interfaces kann dabei in horizontale und vertikale Schnittstellen eingeteilt werden. Horizontale Schnittstellen werden dabei als Kommunikationsprotokolle zweier gleichberechtigter Partner:innen auf der gleichen Ebene umgesetzt, von KMS zu KMS oder Applikation zu Applikation. Die Schnittstellen in den vertikalen Achsen stellen APIs dar, welche von den oberen Entitäten benutzt werden, um Funktionen oder Services der darunterliegenden Objekte aufzurufen.

Abgesehen von ETSI GS QKD 004 und ETSI GS QKD 014, welche zum Teil die Schnittstelle I3 bzw. I5 adressieren, gibt es für alle anderen Schnittstellen zur Zeit keine Standards. Hersteller von QKD-Geräten und QKD-Lösungen setzen hier auf Eigenentwicklungen. In der Vergangenheit wurden ebenfalls auf verschiedenen Ebenen Protokolle und APIs im Rahmen von EU-Projekten erstellt und veröffentlicht bsp. Q3P als Beispiel für I4 im SECOQC Projekt.

2.5.1 Protokolle

Im QKD-KMS-Schichtenmodell lassen sich grob folgende Protokolle identifizieren (jede dieser Protokollebenen besteht tatsächlich aus einer Reihe von Unterprotokollen):

I0

Dieses Protokoll läuft auf dem Quantenkanal und stellt somit das QLCP (Quantum Level Communication Protocol) dar. Hier werden Korrelationen bzw. QuBits ausgetauscht oder übertragen und entsprechende Messungen durchgeführt.

I2

Darüber liegt das QKD-Post-Processing-Protokoll, welches die Schritte Sifting, Error Estimation, Error Correction, Confirmation und Privacy Amplification durchführt. Ein vollständig durchgeführtes QKD-Post-Processing liefert den eigentlichen Quantenschlüssel: den Shared-Secret-Key.

I4

Haben die unteren Schichten entsprechende Schlüssel erzeugt, findet auf dieser Ebene die Synchronisation der Schlüsselspeicher sowie die Verteilung von Schlüsselmaterial an verschiedenen Punkten im Netzwerk statt. Auch findet auf dieser Ebene der Data Relay statt: das Weiterleiten von Anwendungsschlüssel bzw. Daten im generellen Sinn. Hier gibt es eine Reihe von proprietären Protokollen seitens der QKD-Gerätehersteller, als auch öffentlich bekannte Vorschläge wie z. B. Q3P (Quantum Point-to-Point Protocol) aus dem SECOQC Projekt.

I6

Ziel dieses Protokollansatzes ist eine Ende-zu-Ende-Verbindung zwischen möglicherweise nicht benachbarten KMS herzustellen, um die Anforderung von darüberliegenden Applikationen zu erfüllen. Kernaufgaben sind dabei eine (optimale) Route durch das Netzwerk sowie eventuelle Garantiezusagen. Auch hier gibt es im Bereich der Data Plane kein standardisiertes Protokoll.

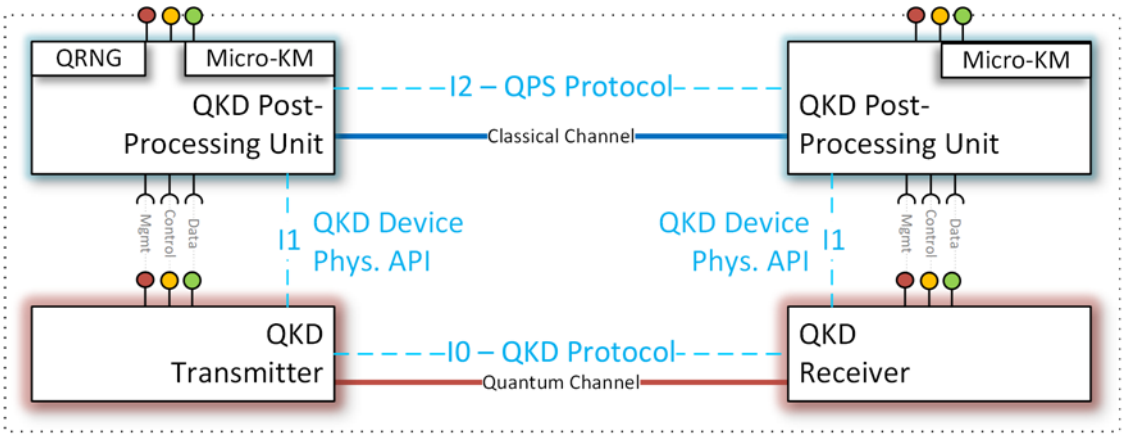
I8

Das ist das applikationspezifische Protokoll, welches im Auftrag eines Users Schlüssel aus der darunterliegenden Schicht entgegennimmt und damit einen Benefit erzeugt.

2.5.2 APIs

In der Betrachtung der Schnittstellen auf der vertikalen Achse durch die Ebenen der Netzwerkschichten, lassen sich die folgenden APIs identifizieren. Auch hier gilt, dass es sich dabei meist nicht um ein einziges bestimmtes, umfangreiches API handelt, sondern um eine Menge an gebündelten Funktionen, welche thematisch oder logisch gruppiert sein können. Beispielsweise kann die Anfrage ans Schlüsselmaterial in der Verwaltung von QKD-Geräten kombiniert und getrennt sein.

Abbildung 8 KMS-Interfaces auf den untersten Ebenen einesbQKD-Moduls: QKD-Post-Processing-Unit + QKD-Transmitter/QKD-Receiver



I1

Abbildung 8 ist ein Ausschnitt aus den KMS-Interfaces und stellt die untersten APIs und Protokolle nochmals dar. Hier ist auch I1 sichtbar, welches den Übergang zwischen der eigentlichen QKD-Hardware (Single Photon Source, SPAD etc.) und der klassischen Post-Processing-Einheit markiert. In I1 werden die Ergebnisse von Messungen (bsp. Time Tags) abgefragt, welche Korrelationen induzieren.

I3

Dieses API liefert das Schlüsselmaterial an die darüberliegenden KMS.

I5

Die Funktionen dieser Schnittstelle liefern ebenfalls Schlüsselmaterial. Darüber hinaus werden Ende-zu-Ende-Schlüsselverbindungen hergestellt bzw. abgebaut.

I7

Dieses API befasst sich mit der Herstellung bzw. dem Abbau von Ende-zu-Ende-Applikationsverbindungen durch das Netzwerk.

2.6 Allgemeine Anforderungen

Auf oberster Ebene, unberücksichtigt ob es sich um ein Einmalschlüsselsystem oder ein Schlüsselstromsystem handelt, gibt es eine Reihe an Anforderungen, welche eine QKD-KMS-Lösung abdecken bzw. ansprechen muss.

2.6.1 Key-Material-Verhandlung

Key-Material-Verhandlung umfasst den Akt der Initiierung einer Kommunikation, die durch Quantenschlüssel unterstützt werden soll. Das ist das erste Themenfeld, wenn Applikationen Ende-zu-Ende-Schlüssel anfordern. Das umfasst:

- Identifizierung der Benutzer:innen
- Identifizierung von Routen
- Formulierung der Schlüsselmaterialanforderung mit Qualitätsmerkmalen, sofern das System einen Schlüsselstrom anbietet. Beispiele für Qualitätsmerkmalen sind Bitrate pro Sekunde, maximal tolerierte ε-Sicherheit und maximale Anzahl von vertrauenswürdigen Knoten

Im konventionellen, bisherigen Aufbau von QKD sind bisher Punkt-zu-Punkt-Verbindungen vorherrschend, bei dem Routen, Benutzer:in und andere Elemente in diesem Bereich eher fix sind oder eine sehr begrenzte Variationsbreite haben.

Geht man jedoch über eine begrenzte Punkt-zu-Punkt-Netzwerkstruktur hinaus, stellt sich die Frage, wer sich mit wem verbindet und wie er angesprochen werden muss. Dies hat Auswirkungen auf Protokolle und APIs in diesem Bereich wie:

- Wo sollen Informationen über Entitäten und Eigenschaften gespeichert werden?
- Wie fügt man Benutzer:innen oder Knoten zum System hinzu und identifiziert sie darin?
- Wie kann man Pfade zwischen Benutzer:innen erkennen bzw. definieren? Sind Pfade dynamisch oder statisch bzw. sowohl als auch?
- Gibt es verschiedene Arten von Schlüsseln, Qualität, Verwendungszweck und Lebensdauer?

2.6.2 Key-Material-Herstellung

Wenn ein Bedarf an Schlüsselmaterial über einen Pfad erkannt wurde, müssen die QKD-Geräte entlang dieses Pfades angewiesen werden, Schlüsselmaterial zu produzieren.

Da dies potenziell mehr als ein einzelnes Gerätepaar umfassen kann, wenn ein Pfad sich über mehrere Knoten in einem Netzwerk erstreckt, ist ein Standardverfahren zur Anweisung zur Schlüsselproduktion über alle Geräte hinweg entlang dieses Pfades zu definieren. Das bedeutet, dass ein KMS-System eine allgemein bekannte Pfadangabe oder Beschreibung entgegennehmen muss, um die internen Ressourcen entsprechend des formulierten Bedarfs zu budgetieren, wie Schlüsselspeicher oder Routing für Schlüsselrelay.

Das KMS fungiert dabei als Adapter, indem nach oben bzw. extern eine homogene Schnittstelle bereitgestellt wird, obwohl die QKD-Geräte und -Techniken darunter unterschiedliche Schnittstellen und Paradigmen verfolgen können.

2.6.3 Key-Material-Charakterisierung

Quantenschlüssel haben unterschiedliche Qualitätswerte oder Eigenschaften, wie beispielsweise:

- Eigenschaften, die von den Benutzer:innen oder der Anwendung gewählt werden:
  - Länge des Schlüssels
  - Ursprungspaar, teilnehmende QKD-Geräte
  - ε-Sicherheit des Schlüssels
  - Berechtigte Klassifizierungsstufe
- Vom Netzwerk definierte oder berechnete Merkmale:
  - Anzahl der benötigten Hops (Trusted Nodes)
  - Zeitpunkt der Erzeugung des ersten/letzten Bits
  - Geeignete kryptografische Algorithmen

Um eine Ende-zu-Ende-Schlüsselverteilung zu gewährleisten, müssen sich die KMS-Systeme auf die Menge dieser Schlüsseleigenschaften einigen und eine gemeinsame Strategie entwickeln, diese Werte zu identifizieren und zu adressieren.

2.6.4 Key-Material-Verteilung

Bei der Key-Material-Verteilung wurde ein Bedarf an Quantenschlüsseln ausgehandelt und identifiziert, dann wird entlang des Pfades eines Multi-Hop-QKD-Netzwerks jedes Paar von Quantengeräten angewiesen, Schlüssel zu erzeugen. Qualitätsparameter, die in der Anforderung angegeben sind, können sich auf Segmente des Pfades auswirken, z. B. Anhebung oder Absenken des ε-Parameters.

Die Key-Material-Verteilung befasst sich mit dem Aspekt, den optimalen Weg zu finden, um die Anforderung zu erfüllen. Dies kann den Pfad über Raumsegmente oder Multi-Hop-Vertrauensknoten über verschiedene Domänen hinweg beinhalten. Dazu kommen auch die Prioritätslevel, die den Benutzer:innen gemäß dem von ihnen abonnierten SLA gewährt werden und dann greifen, wenn die momentanen Kapazitäten des Schlüsselnetzwerks nicht für alle Anfragen ausreicht.

In einem einzelnen Punkt-zu-Punkt-Szenario sind Key-Material-Herstellung und Key-Material-Zuweisung synonym. Erweitert man dieses Prinzip jedoch auf ein Ende-zu-Ende-Beziehung, die mindestens einen Zwischenknoten einschließt, führt dies zusätzliche Komplexität ein.

2.6.5 Key-Material-Speicherung

Das Schlüsselmaterial wird möglicherweise nicht bei Bedarf erstellt, sondern im Voraus gepuffert. Wenn dies der Fall ist, dann darf sensibles Schlüsselmaterial nicht einfach auf einer Festplatte gespeichert werden. Stattdessen muss jedes KMS über eine standardisierte, manipulationssichere Art der Speicherung für eine große Menge stark fluktuierender Schlüsseldaten verfügen.

2.6.6 Key-Material-Zuteilung

Wenn das Schlüsselmaterial unabhängig von der tatsächlichen Nachfrage der Benutzer:innen erstellt wurde (z. B. durch vorheriges Puffern), dies aber in Bursts, müssen Strategien zur Verteilung des verfügbaren Schlüsselmaterials auf parallel existierende Benutzer:innen definiert werden. Idealerweise können Protokolle und APIs dies mit einem Minimum an Interaktion und Neuverhandlung erreichen. Auch die Themen QoS und Fair-Use-Policies werden hier angesprochen, wenn das verfügbare Schlüsselmaterial geringer ist als der aktuell bekannte Bedarf.

2.6.7 Key-Material-Buchhaltung

Wenn einer Benutzer:in ein Schlüssel zugewiesen wurde, müssen entsprechende Abrechnungsaktionen stattfinden. Audits spielen eine wichtige Rolle bei der Zertifizierung von kryptographischen Implementierungen, und daher sind solche Abrechnungs- und Buchhaltungsschritte unbedingt notwendig.

3 Konzept für ein transnationales Key-Management-System

Die Zusammenführung von zwei kooperierenden Key-Management-Systemen zu einem QKD-Netzwerk stellt das zentrale Thema für den Aufbau eines grenzüberschreiten Netzwerks mit gleichberechtigten Kommunikationspartner:innen (Member State Government to Member State Government) dar. Die im weiteren genannten Akteure wie z. B. Deutsche Telekom, A1, Deutsche Bank sind nicht als Präjudiz für künftige Netzwerk gedacht, sondern wurden zur leichteren Veranschaulichung gewählt.

3.1 Interdomain-Key-Verteilung

Die grenzüberschreitende Verteilung von Schlüsselmaterial stellt einen Spezialfall der Interdomain-Key-Verteilung dar. Die Interdomain-Key-Verteilung definiert wie zwischen Netzwerken unterschiedlicher Domains Quantenschlüssel verteilt werden.

Einige zentralen Fragen dabei sind:

- Wie werden Knoten domainübergreifend identifiziert und adressiert? Gibt es zentrale KMS-Instanzen für Subnetze?
- Wie werden die Routen für die Schlüsselverteilung hergestellt?
- Wer darf die Verbindungen auf- und abbauen? Wie erfolgt die Verrechnung und/oder Ressourcenbudgetierung?
- Logisch: Welche Entitäten, Rollen und Positionen gibt es in einer Interdomain-Key-Verteilung? Welche Aufgaben gibt es dabei?
- Technisch: Wo und wie werden zentrale und/oder dezentrale Aufgaben dabei realisiert bzw. implementiert?
- Organisatorisch: wer verwaltet diese Einheiten? Gibt es eine Schlichtungsstelle?

Es gibt zurzeit in verschiedenen Standards Hinweise, welche o. a. Fragen aufgreifen und besonders im Kontext der QKD-Schlüsselverteilung hier Vorgehensweisen aufzeigen.

Abbildung 9 Interdomain-QKD-KMS

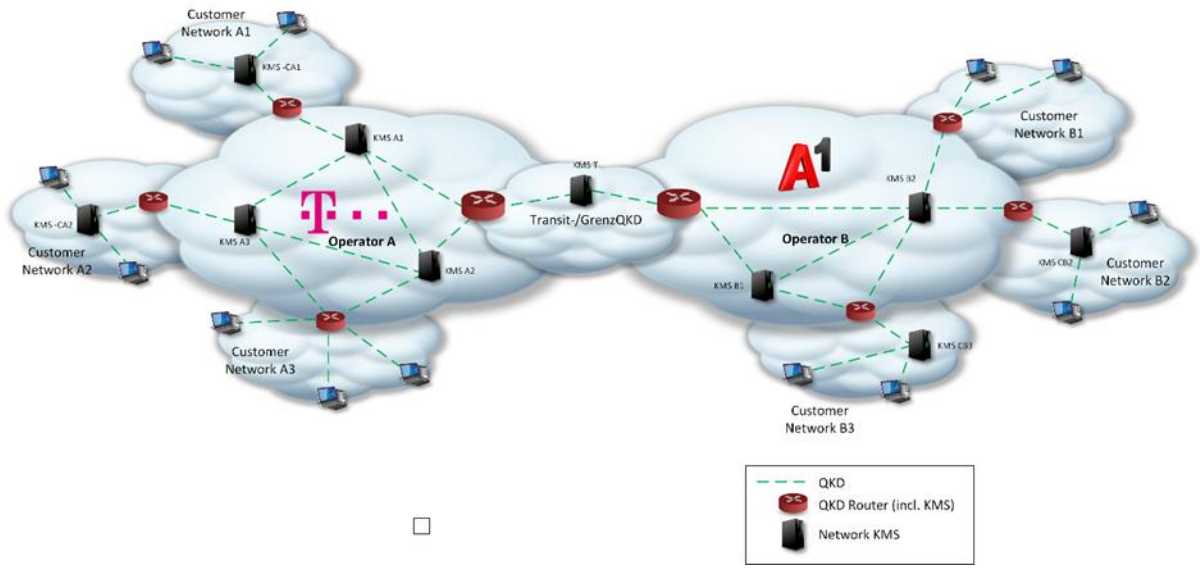


Abb. 9 zeigt eine Interdomain-QKD-KMS Situation inklusive grenzüberschreitender QKD-Schlüsselverteilung. Dabei sind die QKD-Router (rot eingezeichnet) gleichzeitig KMS und Gateway-Knoten in andere Netze. Interne Netzwerk-KMS (schwarz) dienen dabei zur Überbrückung der Distanzlimitation von QKD-Netzen.

Auch können dabei mehrere Customernetze gleichen Organisationen zugeordnet werden, wodurch ein QKD enhanced transnationales VPN entsteht. Es könnten in Abb. 9 die Customer Network A2 und Customer Network B3 Netze des gleichen Unternehmens (bsp. Deutsche Bank) sein.

Die beiden QKD-Router des Transit- bzw. Grenz-QKD in der Mitte können auch zusammenfallen wodurch das Grenz-QKD-Netz sich zu einem einzelnen Grenz-Knoten auflöst. In jedem Fall hat ein Transit Gateway QKD-Router in seinem physikalischen Setup min. zwei QKD-Geräte, welche nicht in das gleiche Netzwerk greifen.

In den jeweiligen Netzwerken der einzelnen Operatoren (in Abb. 9 sind das Deutsche Telekom und A1) befinden sich lediglich Operator-KMS. D. h. die Router und Intermediate-KMS dienen nur der Weiterleitung von Userdaten (Userschlüssel) über das QKD-Netzwerk. Die Service-KMS, also diejenigen KMS, welche tatsächliche über QRNG einen Userschlüssel (Userdaten) zur Verfügung stellen und diese über die Operator-KMS Ende-zu-Ende verteilen, befinden sich nur in den Customer-Netzwerken.

3.1.1 Beispiele

Beispiel 1

Das Customer Netzwerk A2 in Abb. 9 und das Customer Netzwerk B3 sind beides Netzwerke eines einzigen Unternehmens. Customer Netzwerk A2 ist in Frankfurt bei der Deutschen Telekom angebunden, während das Customer Netzwerk B3 in Wien an die Betreiberin A1 angebunden ist. In Frankfurt hat das Unternehmen QKD-Geräte der Deutschen Telekom angemietet während in Wien die Geräte von A1 stammen. Durch Subunternehmen des jeweiligen Betreibers werden diese Geräte serviciert. Das Service-KMS in Frankfurt baut eine Ende-zu-Ende-Verbindung mit dem Service-KMS in Wien auf. Es wird nun ein Router durch die jeweiligen Netze derart ausgestaltet:

- Frankfurt Kunde – DT Ingress Frankfurt: 1 Hop
- DT Ingress Frankfurt – Grenzknoten Ö (DT intern, DT Operator-KMS): x Hops
- Grenzknoten D-seitig – Grenzknoten Ö-seitig (Grenznetz Betreiber:in; mögl. 0 Hop wenn es sich dabei um einen Einzelknoten handelt): y Hop(s).
- Grenzknoten Ö – A1 Egress Wien (A1 intern; A1 Operator-KMS): z Hops
- A1 Egress Wien – Wien Kunde: 1 Hop

Sollte es innerhalb des Operators ebenfalls Service-KMS für den Zugriff auf einzelne Subnetze und Komponenten geben, dann sind dies ebenfalls in diesem Sinne Customer-Netzwerk, allerdings der gleichen Organisation.

Beispiel 2

Eine Administrator:in in Berlin greift über das KMS-Netzwerk auf eine Netzwerkgerät in Nürnberg zu, um den SDN-Controller dort zu konfigurieren. Der Zugriffsknoten im QKD-Netzwerk ist ein Service-KMS, als auch das KMS am SDN-Controller in Nürnberg. Beide bilden zwei Customer Netzwerke: „Berlin“ und „Nürnberg“, selbst dann, wenn die jeweiligen Netzwerke nur aus einem einzigen Knoten bestehen. Über den Pfad der Operator-KMS (Berlin, Magdeburg, Leipzig, Jena, Hof, Bayreuth und Nürnberg) wird der Schlüssel für diese Sitzung in Berlin und Nürnberg an den Service-KMS ausgegeben.

Eine besondere Rolle nehmen die Ingress- und Egress-Router-KMS der Netzwerke ein. Aus Sicht der Operator sind alle Netzwerke hinter den Border-Router-KMS synonym mit den Knoten selbst. Das heißt: In Abb. 9 sieht die Deutsche Telekom operativ nicht einzelne

User und Geräte in den Customer-Netzwerken A1, A2 und A3 und keinen Knoten jenseits des Transits bzw. Grenz-KMS-Router-Gateways. Alle Anfragen aus dem A1-Operator-Netz oder dahinter liegender Customer-Netwerke werden durch diesen Grenz-QKD-Router subsumiert. Das gleiche ist aus Sicht der Betreiberin A1 vice versa an deren Transit- bzw. Grenz-QKD-Knoten für die Geräte, Knoten und Router des Netzes der Deutschen Telekom gültig.

Das heißt nicht, dass die jenseitigen Elemente nicht adressierbar sind. Die operative Verantwortung erlischt aber an diesen Grenzen. Alle Verträge und Zusagen (bsp. QoS) werden mit der Betreiber:in der direkten Gegenstelle vereinbart.

Die Gesamtsicherheit des Systems setzt sich somit kumulativ aus den Einzelsicherheiten der betrachteten Netzwerke zusammen.

Aus dieser Ausführung ist es zwingend, dass herstellerunabhängige Protokolle für eine Ende-zu-Ende-Verbindung zwischen Service-KMS (Protokoll I6 in Kapitel 2.5.1) und Datentransfer (User Schlüssel; I4 in Kapitel 2.5.1) zu standardisieren sind.

3.1.2 Conclusio

Diese Protokolle sind nach wie vor weder voll spezifiziert, noch entwickelt oder standardisiert.

3.2 QKD-Device-Ownerhsip und -integration

QKD-Geräte werden paarweise installiert. Dies bedeutet, dass an dem Router-KMS ein QKD-Gerät integriert wird, welches mit einem QKD-Gerät verlinkt ist, das an der Gegenstelle in einem unternehmensfremden Router eingebaut wird.

Abgesehen von den organisatorischen Herausforderungen stellt sich die technische Frage, wie diese Geräte am fremden Router interagieren. Eine Empfehlung dabei ist, die QKD-Geräte physisch als Einheit zu trennen (eventuell jeweils ein eignes 19“ Gerät für die beteiligten QKD-Geräte und das KMS).

Darüber hinaus ist die Schnittstelle zwischen dem QKD-Gerät und dem KMS (API I3 im Kapitel 2.5.2) ebenfalls herstellerunabhängig zu spezifizieren und zu standardisieren. Mit

ETSI QKD GS 004 und ETSI QKD GS 014 gibt es hier zwei Kandidaten, welche neben I5 auch bei I3 zum Einsatz kommen könnten. Beide Protokolle sind jedoch pullbasiert, d. h. Schlüsselmaterial muss ausdrücklich von der hierarchisch übergeordneten Instanz angefordert werden. Dies widerspricht einem Separation of Concerns Paradigma, denn das QKD-Gerät müsste dabei neben der Schlüsselproduktion ein „Mikro“-KMS implementieren und auf Schlüsselanforderungen warten. Bei einem Pushansatz würde das QKD-Gerät im Gegenzug einen Schlüssel aktiv von sich aus an das übergeordnete KMS liefern, sobald jener fertig destilliert wurde.

3.2.1 Conclusio

Die pushbasierte Schlüsselweitergabe ist bisher auf keinem kaufbaren QKD-Gerät implementiert.

4 Evaluierung möglicher optischer Faserstrecken vom Testbed in Wien zur Grenze nach Bayern

Nachfolgend wurde eine mögliche Glasfaserverbindungen zwischen Wien und der Landesgrenze zu Deutschland sowie potentielle Standorte für Trusted Nodes identifiziert. Partner:innen für die Anmietung von Glasfasern zwischen Wien und beispielsweise Salzburg können A1, ÖBB, Asfinag oder für Teilstrecken auch die Energieversorger sein.

4.1 Knotenpunkte

Um eine QKD-Verbindung über lange Strecken aufzubauen, ist es aufgrund der aktuellen technischen Einschränkungen notwendig, alle etwa 24 dB Dämpfung der Glasfaser einen Trusted Node Standort zu betreiben. 24 dB Dämpfung entsprechen etwa 100 km Singlemode Faserlänge. Aus diesem Grund ist es notwendig für die Strecke von Wien bis an die Landesgrenze zu Deutschland etwa 5 bis 7 QKD-Links zu betreiben. Mithilfe eines KMS ist es möglich, für diese Verbindung QKD-Systeme unterschiedlicher Hersteller zu benutzen.

Abbildung 10 Glasfaserverbindung
(Quelle: Image Landsat/Copernicus, GeoBasis-DE/BKG, Google)

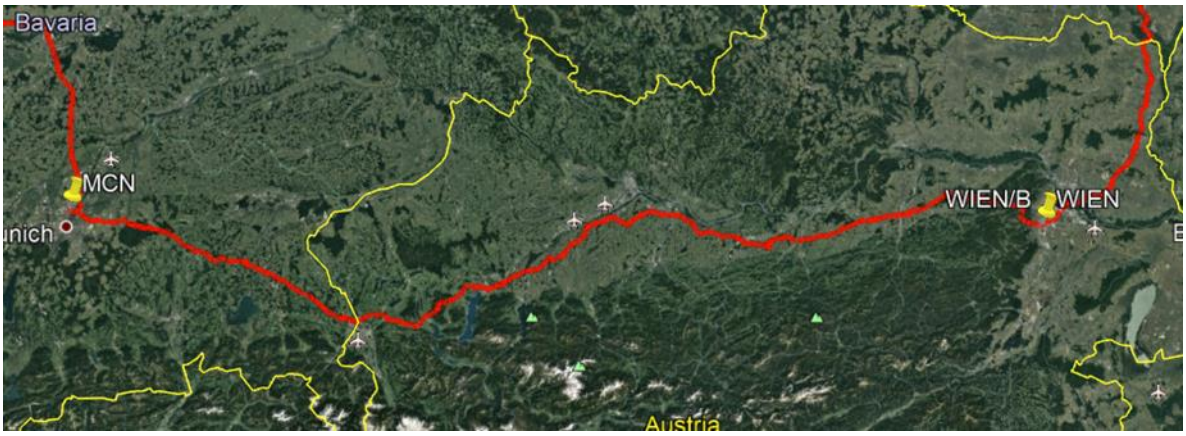
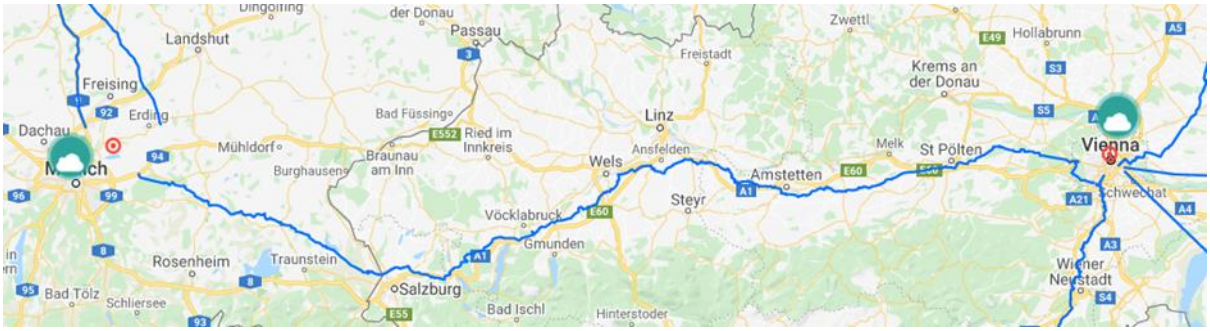


Abbildung 11 Glasfasernetz der Colt Technology Services Group Limited
(Quelle: © 2021 Colt Technology Services Group Limited)



4.2 Verbindung Wien bis Landesgrenze

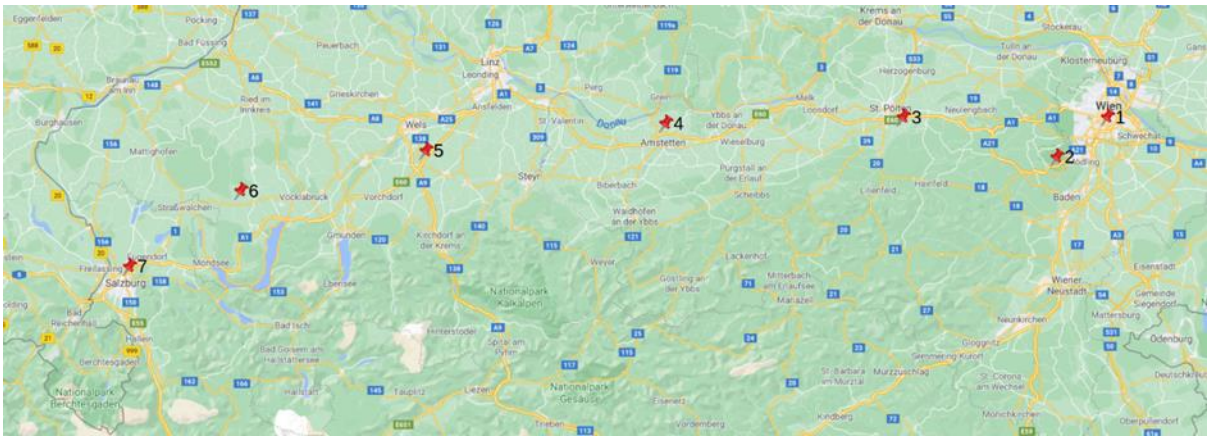
Eine mögliche Faserstrecke inklusive der Standorte für Trusted Nodes verläuft von Wien über Sankt Pölten bis an die Grenze nach Deutschland in Salzburg.

Hier ist eine Beschreibung dieses Links anhand der Nodes und der Eigenschaften der Fasern zwischen ihnen, inklusive der grafischen Darstellung der Nodes auf einer Karte:

1. Vienna Internet Exchange
   a) Länge: 45 km
   b) Dämpfung: 10 dB
2. 2393 Sittendorf, Am Marbach 197
   a) Länge: 68 km
   b) Dämpfung: 13 dB
3. Pyhra/St. Pölten, Getzersdorf 19
   a) Länge: 80 km
   b) Dämpfung: 16 dB
4. 3300 Ardagger/ Amstetten, Betriebsgebiet Nord 24
   a) Länge: 76 km
   b) Dämpfung: 15 dB
5. 4642 Sattledt, Gewerbestrasse 9
   a) Länge: 68 km
   b) Dämpfung: 14 dB
6. 4890 Frankenmarkt, Fornacher Strasse 46
   a) Länge: 53 km
   b) Dämpfung: 11 dB

7. 5020 Salzburg, Jakob Haringer Strasse 1

Abbildung 12 Liste der Nodes in Österreich
(Quelle: Google Maps, Nodes nach eigener Darstellung)



4.3 Wiener Behördennetzwerk

Das Wiener Behördennetzwerk, welches im Zuge des Horizen2020 EU Projekt OpenQKD initialisiert wurde, besteht aus fünf Knotenpunkten.

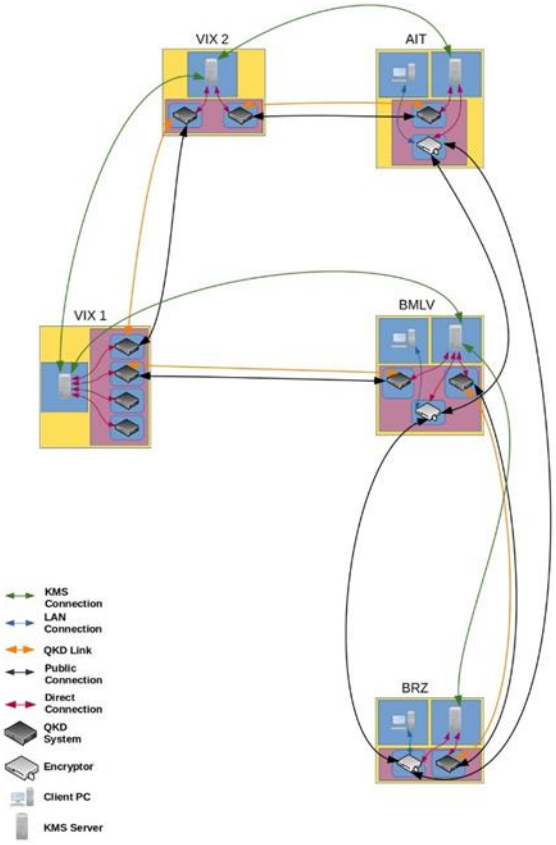
- AIT
- Vienna Internet Exchange 1
- Vienna Internet Exchange 2
- BMLV
- BRZ

Diese Standorte werden mit ein bis zwei Glasfaserpaaren miteinander verbunden. Über die Glasfaser wird sowohl das Quantensignal als auch der klassische Verkehr für das Post Processing übertragen. Die verschlüsselten Daten können wahlweise über die Fasern direkt oder über das Internet übertragen werden.

Die QKD-Systeme und Encryptoren werden von IDQuantique, Infiniquant, Toshiba UK, ADVA sowie Rhode und Schwarz zur Verfügung gestellt.

Zusätzlich wird es auch eine Langstreckendirektverbindung von Wien aus bis nach Budapest geben, welche mit Hilfe des OEAW QKD-Systems realisiert wird.

Abbildung 13 Schematische Darstellung des Wiener OpenQKD Testbeds



4.3.1 Conclusio

Für die Zusammenführung von zwei nationalen Sicherheitsnetzwerken stellt sich auf österreichischer Seite die Frage der Streckenführung insbesondere innerhalb Wiens.

Insbesondere muss festgelegt werden, ob der Vienna Internet Exchange als zentraler Knotenpunkt für Glasfaserverbindungen oder z. B. das BRZ, als zentraler Knotenpunkt der Kommunikation zwischen den Bundesministerien als intermediäre Trusted-Repeater-Standorte gewählt werden sollen.

5 Evaluierung möglicher optischer Faserstrecken von München zur Grenze nach Österreich

In diesem Abschnitt wird ein möglicher Streckenverlauf einer QKD-Verbindung von München an die österreichische Grenze untersucht. Wichtig ist dabei das Ausnutzen bereits verlegter Glasfaserverbindungen. Mit Hilfe der Deutschen Telekom Technik wurde ein Referenznetzwerk geplant, das diese Bedingungen erfüllt und als Beispiel dienen soll. In diesem Referenznetzwerk existieren bereits „dunkle“ Glasfasern, die exklusiv für Quantenverbindungen genutzt werden könnten.

Abbildung 14 Streckenverlauf von München nach Salzburg mit Knotenpunkten entlang der Strecke (Grundlage: google maps).

Die Referenzplanung von München nach Salzburg enthält drei Knotenpunkte, um den Verlust der einzelnen Glasfaserverbindungen deutlich unter 20 dB Dämpfung zu halten. Dies ermöglicht zukünftige Tests von Quantenkommunikationstechnologien und

Erweiterungen, die geringere Verluste benötigen (z. B. Quantenschlüsselverteilung mit hoher Schlüsselrate oder zukünfige Quantenrepeatertechnologien). Die angegebenen Knotenpunkte sind zusätzlich mittlere Aggregationsknoten im Netz der Deutschen Telekom. Damit wären auch baulich schon Voraussetzungen gegeben, um nötige Quantenschlüsselverteilungssysteme und Managementsysteme in den lokalen Räumlichkeiten unterzubringen, die mit der nötigen Technologie und Schutz ausgestattet sind. Falls es nötig wäre die Verluste der einzelnen Teilstrecken noch weiter zu verringern, existieren auch alternative Streckenplanungen, bei denen die Einzelverluste stets unter 13 dB gehalten werden können. Die Knotenpunkte wären dabei allerdings teilweise bei kleineren Betriebsstellen verortet, deren bauliche Ausstattung zu prüfen wäre.

Für einen Betrieb von Trusted Nodes wäre die präsentierte Möglichkeit auch hinsichtlich des Schutzes der Knoten in den Rechenzentren der Aggregationsknoten zu bevorzugen.

Streckenverlauf und Parameter der Referenzplanung:

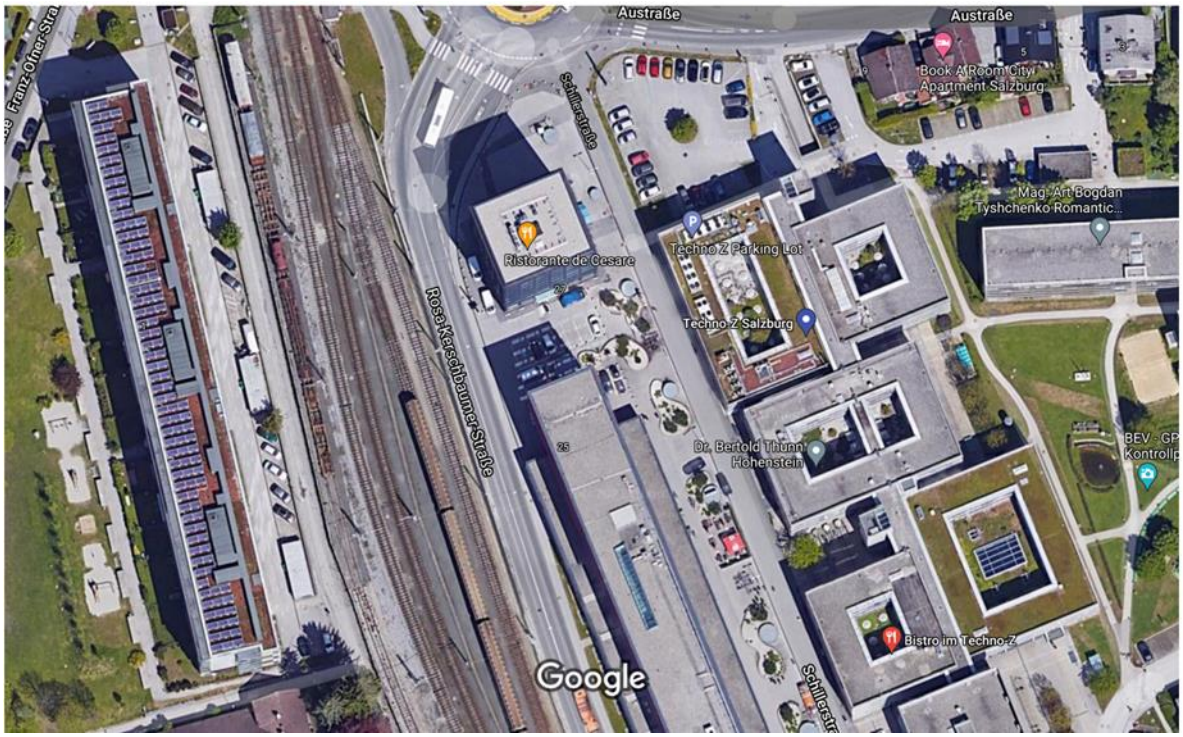
1. München
    a) Länge: 40 km
    b) Dämpfung: 10 dB
2. Höhenkirchen
    a) Länge: 70 km
    b) Dämpfung: 17,5 dB
3. Prien
    a) Länge: 40 km
    b) Dämpfung: 10 dB
4. Traunstein
    a) Länge: 35 km
    b) Dämpfung: 8,8 dB
5. Salzburg

Für den Betrieb der Strecke würden vier QKD-Links benötigt.

Der geeignetste Übergabepunkt für eine Strecke zwischen Bayern und Österreich liegt in Salzburg. Dort können die Netze aus Österreich und Bayern am Techno-Z in Salzburg zusammengeführt werden.

Das Techno-Z ist ein Technologiezentrum mit starker Anbindung an Firmen und Universität. Am Techno-Z bestehen sowohl von der A1 Telekom als auch von der Magenta Telekom (100 % Tochter der Deutschen Telekom) Standorte, von denen neben den klassischen Netzen auch zukünftige Quantennetze zusammengeführt werden könnten.

Abbildung 15 Umgebung des Übergabepunkts am Techno-Z in Salzburg (google maps 2021).



In München können verschiedene Standorte von einem zentralen Aggregationspunkt aus angeschlossen werden. Insbesondere wäre diese Planung kompatibel zu den Überlegungen der Machbarkeitsstudie des bayerischen Wirtschaftsministerium „QuKomm“. Die Verbindung nach Österreich könnte so ein Bestandteil eines bayerischen Testnetzwerkes für Quantenkommunikation werden, das durch Verbindungen nach Thüringen und Sachsen und weiteren Verbindungen nach Westen und Norden in einem europäisches Quantennetzwerk zentral integriert werden kann.

5.1 Conclusio

Für die Zusammenführung der Strecken aus Bayern und Österreich hat sich Salzburg als geeigneter Übergabepunkt herausgestellt. Auf bayerischer Seite existieren bereits Glasfaserverbindungen und baulich geeignete Knotenpunkte auf dem Streckenverlauf.

Ein zentraler Knotenpunkt in München ist geeignet für die Anbindung von lokalen Standorten und die Einbettung in ein bayerisches Quantennetzwerk (QuKomm) sowie zukünftige Einbettungen in deutsche und europäische Quantennetzwerke.

6 Conclusio und Darstellung der perspektivischen Weiterentwicklung

Grundsätzlich sind für die Errichtung eines nationalen QKD-Testnetzwerke im Rahmen von QCI die folgenden Fragen zu beantworten:

- Wer kann/soll das nationale QCI-Testnetzwerk betreiben?
- Wie sehen die Betriebsprozesse für das Testnetzwerk aus?
- Welche Standorte sollen am QCI-Testnetzwerk beteiligt werden?
- Wie soll die Streckenführung zwischen den Standorten erfolgen und wo sind Trusted Repeater Standorte notwendig?
- Welche Lieferanten kommen für die einzelnen QKD-Links in Frage?
- Wie soll das QKD-Key-Management-System für das gesamte QKD-Testnetzwerk (nationale und transnationale Komponente) aussehen?
- Wird das nationale QKD-Testnetzwerk mit anderen QCI-Testnetzwerken an der Grenze verbunden?
- Welche Funktionalitäten müssen dann die QKD-Key-Management-Systeme in den beteiligten QCI-Testnetzwerken implementiert haben?

Auf Basis der vorliegenden Studie lassen sich einige der vorliegenden Fragen beantworten. Andere Fragen sollten im Rahmen künftiger Projekte zu QCI-Testnetzwerken beantwortet werden.

Für den Betrieb eines österreichischen QCI-Testnetzwerks kommt prinzipiell ein Telekommunikationsunternehmen in Frage. Solange das QCI-Netzwerk noch ein Testnetzwerk ist, könnte es auch von einer Forschungseinrichtung betrieben werden.

Die Testnetzwerke in Bayern und Deutschland sind dabei auch im Kontext des BMBF QuNet-Projektes zu sehen.

Die im Rahmen des Projekts aufgezeigten Prozessthemen

- Prozesse für die Planung neuer QKD-Verbindungen einschließlich der Bewertung neuer Standorte, Leitungen und QKD-Systeme,
- Prozesse für die Abnahme neuer Standorte, die Messung und Abnahme neuer Leitungen sowie Abnahmeprozesse für die Installation und Inbetriebnahme neuer QKD-Geräte,
- Prozesse im Bereich der Qualitätssicherung der QKD-Netzwerke im Bereich der Überwachung, Fernwartung, SW Updates, sowie Entstörung,

existieren aktuell noch nicht und sollten in künftigen Projekten für QKD-Testnetzwerke entwickelt werden.

Für den Zusammenschluss von zwei nationalen QKD-Netzwerken für einen oder mehrere Kunden sind ergänzend noch Fragen der Synchronisation und Transparenz in den Prozessen sowie der Haftung gegenüber den Endkunden abzuklären.

Die konkreten Standorte künftiger QCI-Testnetzwerke hängen von den Use-Cases ab, die jeweils demonstriert werden sollen. Die Identifikation möglicher Streckenführungen und allenfalls notwendiger Trusted-Repeater-Standorte muss aufgrund der Rahmenbedingungen der QKD-Link-Systeme bezüglich der maximal erlaubten Dämpfungswerte sorgfältig geplant werden. Allerdings stellt dieses Thema für Planungsmitarbeiter:innen von Telekommunikationsunternehmen keine besondere Herausforderung dar.

Nachdem es aktuell keine QKD-Link-Produkte auf TRL9 Ebene gibt, die von EU Unternehmen angeboten werden, sollte man voraussichtlich unterschiedliche Prototypen aus der EU und Produkte von IdQuantique oder Toshiba in künftigen QCI-Testnetzwerken kombinieren.

Aktuell unterscheiden die QKD-Lieferanten nicht zwischen Plattform-, Operator- und Service-KMS. Dadurch ergibt sich im Wesentlichen eine Lieferantensituation mit Vendor-Lock-in. Es sind bisher keine QKD-Netzwerke mit unterschiedlichen QKD-Link-Lieferanten mit einem gemeinsamen KMS bekannt.

Darüber hinaus gibt es bisher kein QKD-Gesamtnetzwerk, in dem zwei QKD-Teilnetzwerke mit unterschiedlichen Operator-KM-Systemen zu einem gesamten Netzwerk zusammengeschalten wurden.

Die Spezifikation und Implementierung der Key-Management-Systeme in den benachbarten Staaten sind jedoch notwendige Voraussetzung für das Zusammenschalten von zwei QKD-Testnetzwerken im Rahmen von QCI. Für dieses Thema existieren bisher weder Spezifikationen noch Standards.

Daher sollte im Rahmen künftiger nationaler QCI-Testnetzwerke dieses Thema enthalten sein und erstmalig implementiert werden, um erste Erfahrungen zu sammeln und das Thema im Weiteren auch in die europäische Standardisierung einbringen zu können.

Ein transnationaler QKD-Netzaufbau könnte zeitlich so umgesetzt werden:

1. 2022–2024: Aufbau und Inbetriebnahme erster nationaler Testbeds mit Faserstrecken in Richtung der Nachbarländer und Knoten in Grenznähe im Rahmen des DEP Programms.
   Zentrale Themen könnten die oben aufgezeigten Prozessthemen und die Weiterentwicklung des QKD-KMS mit einer Spezifikation und Trennung der Plattform-, Operator- und Service Anteile im KMS sein.

2. 2023–2025: Aufbau transnationaler QCI-Testbeds im Rahmen des CEF Programms.
   Zentrale Themen könnten die Zusammenführung mehrerer nationaler QKD-Netzwerke mit unterschiedlichen Operator KM Systemen zu einem gesamten Netzwerk sein. Darüber hinaus müssten Fragen zur transnationalen Synchronisation und Transparenz der Prozesse sowie zur transnationalen Produktspezifikation für das QoS sowie der Haftung gegenüber den Endkunden evaluiert werden.

Anhang 1 QKD-Standards

Weltweit befassen sich mehrere SDOs mit verschiedenen Aspekten und Themen auf dem Feld der Quantentechnologie. Besonders im Bereich der Quantenkryptographie haben sich bereits mehrere Gruppen mit verschiedenen Standards etabliert bzw. arbeiten daran.

Unter den SDOs, welche sich ausdrücklich mit Quantentechnologien beschäftigen sind:

- ETSI (European Telecommunications Standards Institute). Das ETSI hat eine Industry Specification Group (ISG) nur zum Thema QKD eingerichtet: ETSI ISG-QKD. Diese arbeitet an und veröffentlichte bisher einige Standards (Group Specification – GS).
- ITU-T (International Telecommunication Union Telecommunication). Die ITU-T hat zwei Study Groups (SG) und eine Focus Group etabliert, welche sich (auch) mit QKD befassen. ITU-T SG13 „Future networks“, ITU-T SG16 „Security“ sowie ITU-T FG-QIT4N “Focus Group on Quantum Information Technology for Networks”.
- ISO (International Organization for Standardization) befasst sich ebenfalls im Rahmen von ISO/IEC JTC 1/SC 27 „IT Security techniques“ mit QKD. Dort ist QKD im WG3 (Working Group 3) angesiedelt.
- Die IETF (Internet Engineering Task Force). Die QIRG (Quantum Internet Research Group) der IETF hat nicht nur QKD sondern generell ein Quantum Internet im Fokus.
- IEEE (Institute of Electrical and Electronics Engineers) hat mit der IEEE SA Quantum-Comm ebenfalls eine Einheit eingerichtet, welche sich mit Software-Defined Quantum Communication beschäftigt.

Obschon es weltweit zahlreiche Aktivitäten gibt, sind speziell zum Thema QKD-KMS wenig bis kaum Standards verfügbar. Eine Auswahl, welche bei der Umsetzung eines transnationalen QKD-KMS in Betracht gezogen werden muss, ist:

Tabelle 2 Auswahl an für QKD-KMS relevante weltweite Standards

SDO	Standard	Titel	Beschreibung	Version
ETSI	GS QKD 003	Components and Internal Interfaces	Generelle Beschreibung von QKD-Systemen und QKD Modulen	V2.1.1
ETSI	GS QKD 004	Application Interface	Generelles API zur Key-Ausgabe im Schlüsselstrom Verfahren.	V2.1.1
ETSI	GS QKD 014	Protocol and data format of REST-based key delivery API	API zur Key-Ausgabe im Einmalschlüssel-Verfahren als REST-based Web Service.	V1.1.1
ETSI	GS QKD 015	Quantum Key Distribution Control Interface for Software Defined Networks	Anbindung von QKD-Systemen an SDN inkl. KMS Funktionalität an einem QKD Knoten (Control & Management).	Draft (noch nicht öffentlich verfügbar)
ETSI	GS QKD 016	Common Criteria Protection Profile for QKD	Zertifizierungsgrundlage nach Common Criteria für QKD Devices.	Draft (noch nicht öffentlich verfügbar)
ETSI	GS QKD 017	QKD Network Architectures	Allgemeine Definition von grundlegenden Funktionen eine QKD-Netzwerks.	Draft (noch nicht öffentlich verfügbar)
ETSI	GS QKD 018	Orchestration Interface for Software Defined Networks	Konfiguration und Management von QKD-Netzwerken via SDN (Control & Management).	Draft (noch nicht öffentlich verfügbar)
ITU-T SG 13	Y.3800	Overview on networks supporting quantum key distribution	Empfehlung für den prinzipiellen Aufbau eines QKD-Netzes; allgemeine Struktur und Elemente eines QKD-Netzwerks.	1.0
ITU-T	TR.sec_qkd	Technical report on security framework for Quantum key distribution in telecom network		

SDO	Standard	Titel	Beschreibung	Version
ITU-T	X.cf-QKDN	Use of cryptographic functions on a key generated in Quantum Key Distribution networks		
ITU-T	X.sec-QKDN-km	Security requirements for quantum key distribution networks - Key management		
ITU-T	X.sec-QKDN-ov	Security requirements for quantum key distribution networks - Overview		
ITU-T	X.sec-QKDN-tn	Security requirements for quantum key distribution networks - Trusted node		
ITU-T	Y.QKDN_Arch	Functional architecture of the Quantum Key Distribution network		
ITU-T	Y.QKDN_BM	Business role-based models in Quantum Key Distribution Network		
ITU-T	Y.QKDN_KM	Key management for Quantum Key Distribution network		
ITU-T	Y.QKDN_CM	Control and Management for Quantum Key Distribution Networks		
ITU-T	Y.QKDN-req	Functional requirements for quantum key distribution network		
ITU-T	Y.QKDN_SDNC	Software Defined Network Control for Quantum Key Distribution Networks		
ITU-T	Y.QKDN-qos-gen	General Aspects of QoS on the Quantum Key Distribution Network		

Tab. 2 listet Standards auf, welche beim Bau von QKD-KMS-Netzwerken in Betracht gezogen werden müssen. Auffällig dabei ist, neben einer Dominanz von ETSI und ITU-T Veröffentlichungen, dass es keinen umfassenden homogenen Standard zu QKD-KMS gibt. Vielmehr gibt es eine Sammlung miteinander kompatibler Veröffentlichungen einer SDO.

Auch existieren Lücken im Gesamtentwurf und werden zum Teil erst diskutiert. Es fehlt ebenfalls ein standardisiertes Key-Synchronisations- und Data-Relay-Protocol, um KMS unterschiedlicher Anbieter in einem Netzwerk zu integrieren.

Bei dem Entwurf eines transnationalen QKD-KMS ist jedenfalls die Liste der Standards in Tab. 2 der Zielimplementierung gegenüber zu stellen und etwaige Lücken (bsp. I4 und I6 in 2.5.1 Protokolle) selbst im abgeleiteten Sinne der angeführten Standards zu schließen.

Tabellenverzeichnis

Abbildungsverzeichnis

Abkürzungen

AAA	Authentication, Authorization and Accounting
AIT	Austrian Institute of Technology
API	application programming interface
ASHRAE	American Society of Heating, Refrigerating and Air-Conditioning Engineers
BMLV	Bundesministerium für Landesverteidigung
BRZ	Bundesrechenzentrum
DIN	Deutsche Institut für Normung
EN	European Norms
ETSI	European Telecommunications Standards Institute
EuroQCI	European Quantum Communication Infrastructure
FG-QIT4N	Focus Group on Quantum Information Technology for Networks
GS	Group Specification
ISG	Industry Specification Group
ISO	International Organization for Standardization
ITU-T	International Telecommunication Union
KMS	Key Management System
NISG	Netz- und Informationssystemsicherheitsgesetz
OEAW	Österreichische Akademie der Wissenschaften
OIB RL	Österreichisches Institut für Bautechnik Richtlinie
OSI	Open Systems Interconnection
ÖVE	Österreichischer Verband für Elektrotechnik
QCI	Quantum Communication Infrastructure
QFP	Quantum Flux Parametron
QKD	Quantum Key Distribution
QLCP	Quantum Level Communication Protocol
QoS	Quality of Service
QRNG	Quantum Random Number Generator
QuBits	Quantum Bits

REST	Representational State Transfer
SDN	Software-defined Networking
SDO	Standard Developing Organisation
SLA	Service Level Agreements
SPAD	Single-Photon Avalanche Diode
SW	Software
TRL	Technology Readiness Level
TRNG	True Random Number Generator
USV	Unterbrechungsfreie Stromversorgung
VdS	Schadenverhütung GmbH
VPN	Virtual Private Network
XOR	Exclusive oder

Bundesministerium für Klimaschutz, Umwelt, Energie, Mobilität, Innovation und Technologie
Radetzkystraße 2, 1030 Wien
+43 (0) 800 21 53 59
servicebuero@bmk.gv.at
bmk.gv.at