Abschlussbericht Teil 2

Eingehende Darstellung

DemoQuanDT

16KISQ071

Dr.-Ing. Helmut Grießer
Tel. +49 (0)175 4365653
helmut.griesser@advasecurity.com

Inhalt

1 Einleitung 3

2 Arbeitspakete und erreichte Ziele 3

2.1 AP1 Projektmanagement 3

2.2 AP2 Architektur & Design 4

2.3 AP3 Software Defined Networking 7

2.4 AP4 Referenzlabor 8

2.5 AP5 Demonstrator 9

3 Erläuterung der wesentlichen Kostenpunkte 9

4 Notwendigkeit und Angemessenheit der geleisteten Projektarbeiten 10

5 Voraussichtlicher Nutzen, insbesondere die Verwertbarkeit des Ergebnisses – auch konkrete Planungen für die nähere Zukunft - im Sinne des fortgeschriebenen Verwertungsplans 10

6 Der während der Durchführung des Vorhabens dem Zuwendungsempfänger bekannt gewordene Fortschritt auf dem Gebiet des Vorhabens bei anderen Stellen 10

7 Erfolgte oder geplante Veröffentlichungen des Ergebnisses nach Nr. 5 der NKBF/NABF 11

1 Einleitung

Dieser Bericht beschreibt die Beiträge von Adva für das Forschungsprojekt DemoQuanDT.

In DemoQuanDT wurde eine vollständige QKD-Strecke im Netz der Deutschen Telekom aufgebaut mit dem Ziel, einen wirknetznahen Testbetrieb zu ermöglichen, der alle operativen Aspekte eines zukünftigen Wirkeinsatzes abdeckt. Der Quantenlayer selbst stand dabei nicht im Fokus. Vielmehr wurden Netzintegration und Netzmanagement sowie das Zusammenspiel aller notwendigen Komponenten, Systeme und Prozesse für einen reibungsfreien Netzbetrieb betrachtet. Zunächst wurde eine QKD-Testumgebung bereitgestellt um die Geräte für den Demonstrationslink auf ihre Tauglichkeit zu testen und zu konfigurieren. Anschließend wurde die QKD-Demonstratorstrecke unter Berücksichtigung aller grundlegenden Eigenschaften einer späteren Produktivumgebung, aufgebaut.

Adva hat im Projekt vor allem mit Ethernet-Verschlüsselern mit Quantenschlüsselinterface und einem Emulator für QKD-Geräte beigetragen.

Weiterhin werden für Adva die aufgelaufenen Kosten im Vergleich zur Projektplanung sowie insbesondere die voraussichtliche Verwertung der Ergebnisse diskutiert.

NB: Im Oktober 2022 wurde im Zuge der Ausgliederung der Adva Network Security GmbH aus der ADVA Optical Networking SE auch das entsprechende Teilprojekt in DemoQuanDT auf Adva Network Security übertragen. Da auch die im Projekt beteiligten Mitarbeiter nun bei Adva Network Security arbeiten und die Unterstützung von administrativer Seite bei beiden Firmen Hand in Hand läuft, ist der Übergang relativ reibungslos von statten gegangen. Adva steht deshalb im Folgenden kurz für Adva Network Security GmbH, nicht der ursprüngliche Projektpartner ADVA Optical Networking SE, der großteils in der fusionierten Adtran aufgegangen ist.

2 Arbeitspakete und erreichte Ziele

Adva war verantwortlich für Teilaufgabe 2.6 Standardisierung & Wissenschaftskommunikation in AP2 und Teilaufgabe 3.4 QKD-Emulator in AP3. Weiterhin wirkte Adva an vielen anderen Teilaufgaben mit und brachte seine Expertise in der Entwicklung und dem Betrieb von sicheren, zertifizierten Kommunikationssystemen ein. Schwerpunkte waren insbesondere Anforderungen und Architektur von sicheren Kommunikationssystemen, Knoten- und Netzsteuerung, sowie die Unterstützung von Labor- und Feldtests.

2.1 AP1 Projektmanagement

Adva hat sehr zeitig im Projekt zwei L1-Verschlüsseler (5TCE-AES10G) mit QKD-Schnittstelle (ETSI-014) für das Testlabor zur Verfügung gestellt, um zunächst gelieferte QKD-Geräte und später KMS-Implementierungen zu testen. Der QKD-Emulator wurde im engen Austausch mit der Deutschen Telekom erstellt und intensiv für Labortests und außerdem auf der Teststrecke für das virtuelle Rerouting sowie bei Ausfall eines physischen QKD-Gerätes eingesetzt. Im dritten Projektjahr haben wir dann die Verschlüsseler für die Datenverbindung (XG118pro CSH, Ethernet, L2) mit einer Demoversion der ETSI-014-Schnittstelle verfügbar gemacht. Leider konnte das Paar aus zeitlichen Gründen nicht mehr vollständig auf der Teststrecke in Betrieb genommen werden.

Um Verzögerungen vor allem bei der Lieferung der QKD-Geräte für den Projektpartner Deutsche Telekom auszugleichen, wurde das Projekt um drei Monate verlängert.

2.2 AP2 Architektur & Design

Adva hat zusammen mit den Projektpartnern die Anwendungsszenarien und die Anforderungen an die Adva-Verschlüsseler sowie den QKD-Emulator diskutiert und definiert.

Die Demonstratorstrecke zwischen Berlin und Bonn verfügt zwar über eine dedizierte Faserverbindung, die nicht für andere Zwecke genutzt wird (*dark fiber*), die Datenübertragung erfolgt jedoch über eine konfigurierbare Ethernetverbindung im bestehenden Transportnetz der Telekom. Deshalb haben wir für die Datenübertragung ein Ethernet-Gerät vorgesehen, das eine Datenrate von 10GbE oder 1GbE per AES mit dem Quantenschlüssel verschlüsseln kann. Für die Demonstration ist somit das Ethernet-Gerät mit einer QKD-Schlüsselschnittstelle nach ETSI-014 auszustatten. Neben den funktionalen Elementen zur Anforderung und dem Abgleich des Quantenschlüssels an den beiden Enden der verschlüsselten Verbindung, ist insbesondere die Authentifizierung zwischen QKD-Gerät und Verschlüsseler bzw. Schlüsselmanager mit Hilfe von Zertifikaten sicherheitsrelevant.

Der **QKD-Emulator** soll lediglich das generische Verhalten einer QKD-Strecke am Schlüsselinterface nachbilden. Es wird weder der Quantenkanal noch die klassische Prozessierung und Kommunikation zur Generierung von Quantenschlüsseln emuliert. Das ist aufgrund der Unterschiede und der Komplexität der QKD-Systeme kaum effektiv und vor allem nicht notwendig. Die Emulation stellt vielmehr generisch eine von den Streckendämpfung und parametrisierbaren zeitlichen Variationen (aufgrund von Temperaturschwankungen, Regelprozessen in den QKD-Geräten, etc.) beeinflusste Schlüsselrate bereit. Es werden Schlüssel mit einer festen Länge von 256 bits erzeugt und in einem Speicher mit konfigurierbarer Tiefe zwischengespeichert. Der QKD-Emulator soll neben der Schlüsselschnittstelle (ETSI-014) auch über eine Managementschnittstelle (SNMP) verfügen, die verschiedene (gegebenenfalls fingierte) Parameter zurückliefert, um auch das Monitoring der QKD-Geräte emulieren zu können.

Im Rahmen von AP2 haben wir auch die relevanten Standardisierungsaktivitäten verfolgt. Mit ITU-T, ETSI, CEN-CENELEC, ISO/IEC und IRTF sind zahlreichen Standardisierungsgremien im Bereich QKD oder allgemeiner Quantenkommunikation aktiv.

Im Rahmen der ITU-T Standardisierung werden Standards in den sogenannten *Study Groups* SG11, SG13 und SG17 erstellt. Die Bilder 1 bis 4 zeigen einen Überblick über die zahlreichen Standards zu QKD, die zu einem großen Teil bereits abgeschlossen und teils noch in Bearbeitung sind (letzteres wird durch einen orangen Rahmen angezeigt). Abgeschlossene Standards sind frei verfügbar, *drafts* nur für Mitglieder bei der ITU-T zugänglich. Relevant für die Projektaktivitäten sind wohl insbesondere die Standards Y.3802 QKDN – Functional architecture, Y.3803 QKDN – Key management, Y.3804 QKDN – Control & Management und Y.3805 SDN control. Generell sind die Standards der ITU-T bislang eher konzeptionell und abstrakt, es werden z.B. keine Protokolle auf der Bitebene spezifiziert.

Für die ETSI QKD Industry Standardization Group ist es dagegen Ziel, konkrete Schnittstellen präzise zu definieren, um die Interoperabilität zwischen Geräten verschiedener Hersteller zu erreichen. Relevant für das Projekt sind hier offensichtlich die Standards zu verschiedenen Schnittstellen, insbesondere die Schlüsselschnittstellen ETSI-004 und ETSI-014 sowie die derzeit diskutierten Änderungen, ETSI-015 (SDN control) und ETSI-020 (inter-KMS-Schnittstelle).

CEN/CENELEC hat nach dem Abschluss der Fokusgruppe Quantentechnologien ein sog. Joint Technical Committee CEN/CLC/JTC 22 - Quantum Technologies gestartet auch um dort Standardisierungsaktivitäten im Bereich Quantenkommunikation in Europa zu bündeln.

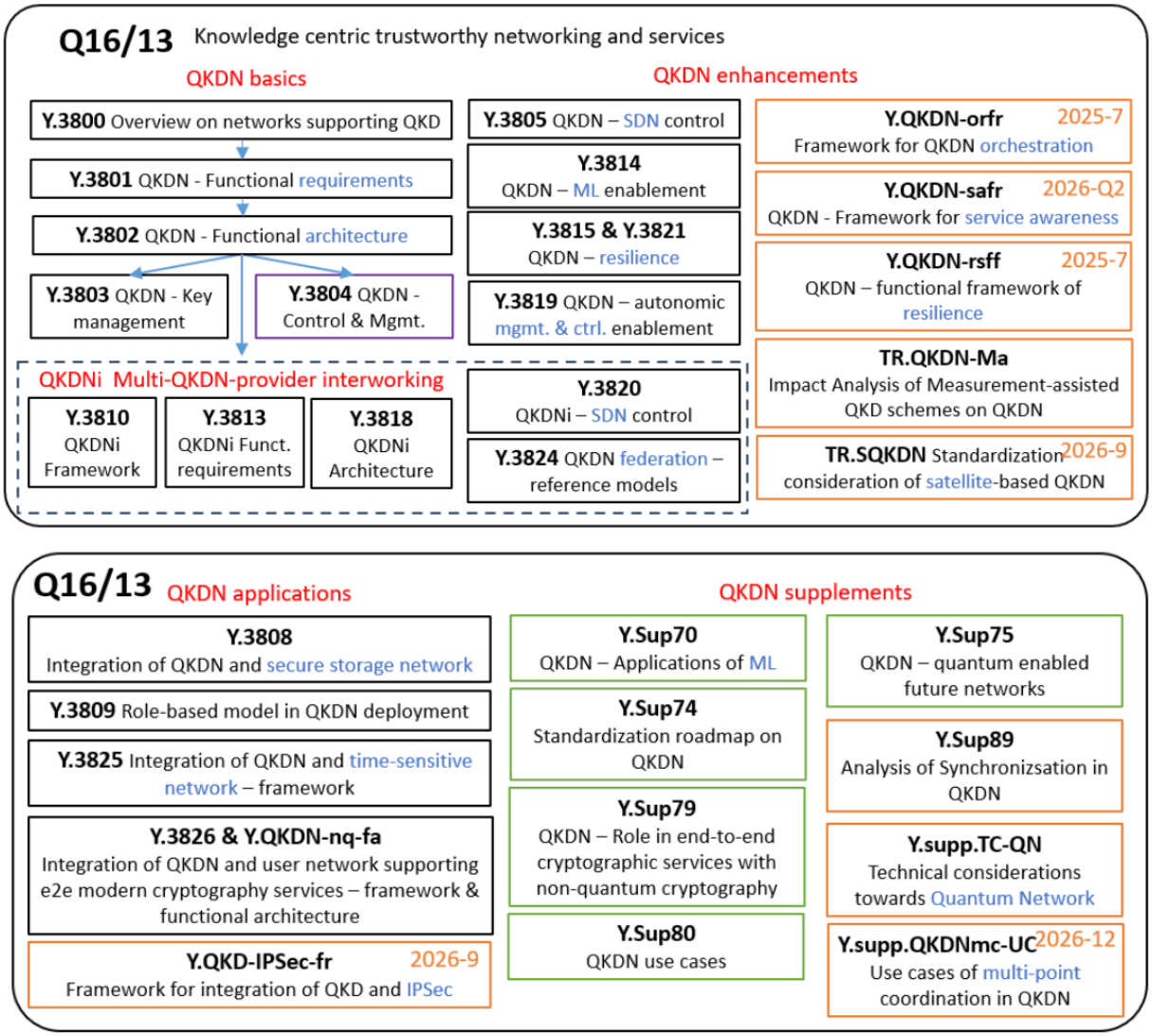

Bild 1. ITU-T Standards in *Study Group* 13, *Question* 16. Ein Datum weist auf den geplanten Genehmigungszeitpunkt von *draft* Dokumenten hin.

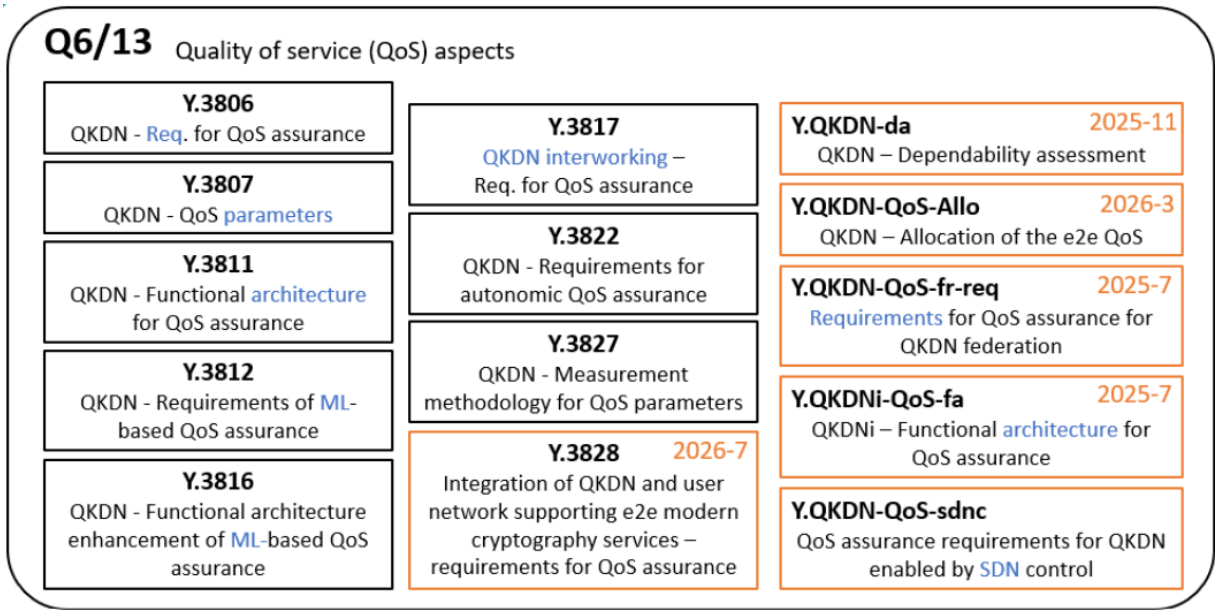

Bild 2. ITU-T Standards in *Study Group* 13, *Question* 6.

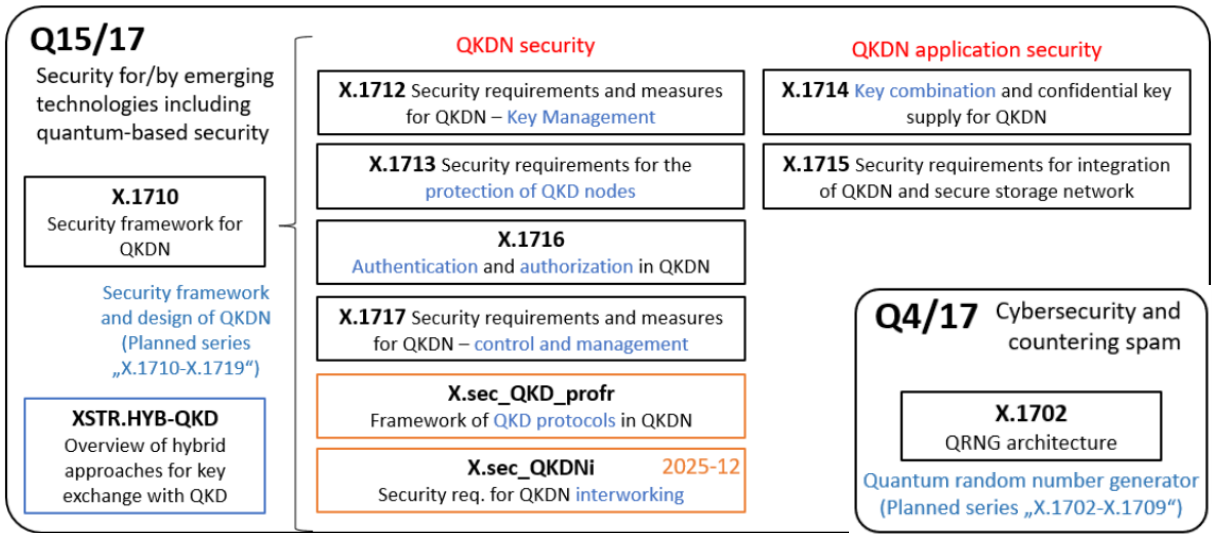

Bild 3. ITU-T Standards in *Study Group* 17, *Question* 15 und 4.

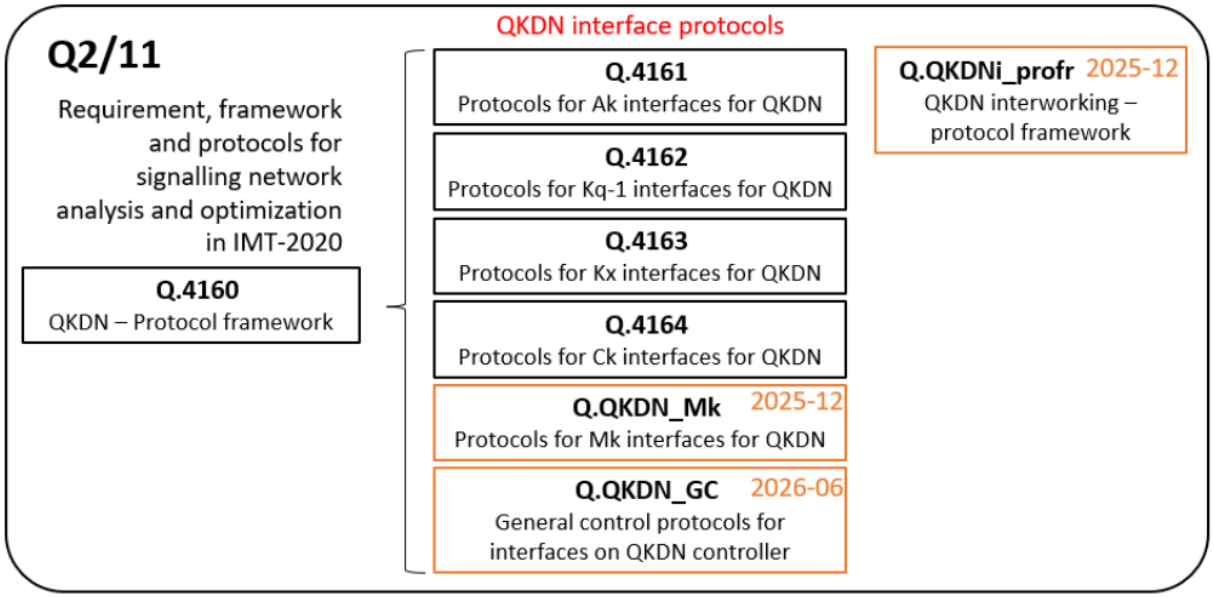

Bild 4. ITU-T Standards in *Study Group* 11, *Question* 2.

Ein gemeinsames Paper[1] des Konsortiums beschreibt die Architektur des *carrier-grade* QKD-Netzes wie im Projekt erarbeitet. Mit der Veröffentlichung dieses Projektergebnisses soll eine Referenz für eine Architektur etabliert werden, die auf einen Service-Provider zugeschnitten ist.

[1] P. Horoschenkoff et al., "DemoQuanDT: a carrier-grade QKD network," *Journal of Optical Communications and Networking*, vol. 17, no. 9, pp. 743–756, Sep. 2025, doi: 10.1364/JOCN.563470.

2.3 AP3 Software Defined Networking

Die Arbeiten von Adva in AP3 fokussierten sich auf einen QKD-Emulator und die Unterstützung von externen Quantenschlüsseln für die Verschlüsselungsfunktion des Ethernet-Gerätes XG118PRO CSH. Ein experimentelles Schlüsselinterface nach ETSI wurde implementiert und für einen Punkt-zu-Punkt Datenstrom getestet.

Adva hat im Projektverlauf in enger Abstimmung mit der Telekom und weiteren Projektpartnern einen **Softwareemulator für QKD-Systeme** entwickelt. Der QKD-Emulator bildet das generische Verhalten einer QKD-Strecke für das Schlüsselinterface (ETSI GS QKD 014) und das Interface für das QKD-Gerätemanagement (SNMP) nach. Im Vorhaben dient der Emulator vor allem der Demonstration eines erweiterten QKD-Netzes, dem Ersatz von physischen QKD-Geräten und ggf. auch der Emulation von zeitlichen Variationen der Streckenqualität und damit der resultierenden Schlüsselrate.
Unter Berücksichtigung der in AP2 definierten Anforderungen des QKD-Emulators und der Schlüsselschnittstelle wurde eine Lösung erarbeitet, die auf *docker containern* basiert. Für die SNMP-Schnittstelle kommt Net-SNMP, eine *open-source* Bibliothek mit BSD-Lizenz zum Einsatz. Der QKD-Emulator wurde zunächst im Telekom-Testlabor in Nürnberg installiert und später auf der Demonstratorstrecke zwischen Berlin und Bonn für das virtuelle Rerouting und temporäre Überbrückung von Ausfällen bei QKD-Systemen genutzt. Bild 5 zeigt die Softwarearchitektur des Emulators mit jeweils einem docker container für die Schlüsselerzeugung und -schnittstelle, sowie einem weiteren für die snmp-Funktionalität. Nähere Details zum Emulator finden sich in einer dedizierten Dokumentation, die allen Projektpartnern zur Verfügung steht.

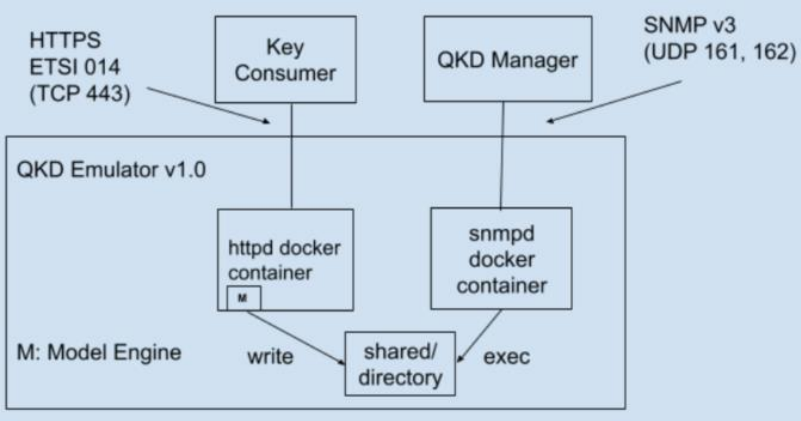

Bild 5. Softwarearchitektur des QKD-Emulators.

In einer weiteren Aktivität wurde zu Demonstrationszwecken eine **QKD-Schnittstelle für das Ethernet-Gerät XG118Pro CSH** implementiert. Das Gerät erlaubt die Verschlüsselung und den klassischen Schlüsselabgleich von Ethernet-Verbindungen nach dem MACsec-Standard. Es verfügt über eine AES-Verschlüsselung und ein Cryptomodul (CSM), das für MACsec mit der Gegenstelle eine herkömmliche MKA-Schlüsseleinigung durchführt. Für die Berücksichtigung des Quantenschlüssels muss zunächst ein Tunnel von der entsprechenden Geräteschnittstelle zum CSM aufgebaut werden um das verschlüsselerseitige Ende des Schlüsselprotokolls (hier ETSI GS QKD 014, Version 1.1.1) direkt im CSM durchzuführen. Der erfolgreich übertragene Quantenschlüssel wird dann im CSM mit dem klassisch ausgetauschten Schlüssel zum neuen AES-Sitzungsschlüssel hybridisiert und für die MACsec-

Verschlüsselung eingesetzt. Das Schlüsselinterface im Ethernet-Gerät ist in Python implementiert und besteht aus der eigentlichen *key-handler* Anwendung und einem Konfigurationsfile.

Zur **Verifikation der Implementierung der QKD-Schnittstelle im Ethernet-Gerät** wurde ein Testaufbau für einen einzelnen verschlüsselten Ethernet-Datenstrom genutzt. Bild 6 zeigt die Demonstration bestehend aus zwei Adtran FSP 150-XG118Pro (CSH) Layer 2-Geräten mit acht 1/10GbE (SFP/SFP+)-Ports mit MACsec-Fähigkeiten, einer FPGA-Implementierung von AES-GCM-256 für die Verschlüsselung des Datenverkehrs mit einem Durchsatz bis zu 10Gb/s und einem integrierten Cryptomodul (CSM) für die Verarbeitung des klassischen Schlüsselaustauschs (Diffie-Hellman der Länge 4096) und die sichere Kombination mit importierten QKD-Schlüsseln zur Ableitung hybrider Sitzungsschlüssel. Die QKD-Geräte müssen Schlüssel gemäß dem ETSI-014-Standard, Version 1.1.1, liefern. In der Demonstration haben wir statt echter QKD-Geräte hilfsweise den zuvor im Projekt erstellten QKD-Emulator eingesetzt.

Für die Demonstration muss jedes QKD-Gerät über TCP-Port 443 an das jeweils lokale Ethernet-Gerät angebunden sein. Statische Zertifikate sind in den Geräten zu setzen, um die Authentifizierung des Schlüsselinterfaces zu gewährleisten. Danach kann die key-handler-Anwendung gestartet werden. Für Test- bzw. Debugzwecke können alle erfolgten Schlüsselübergaben in einem log-file dokumentiert werden.

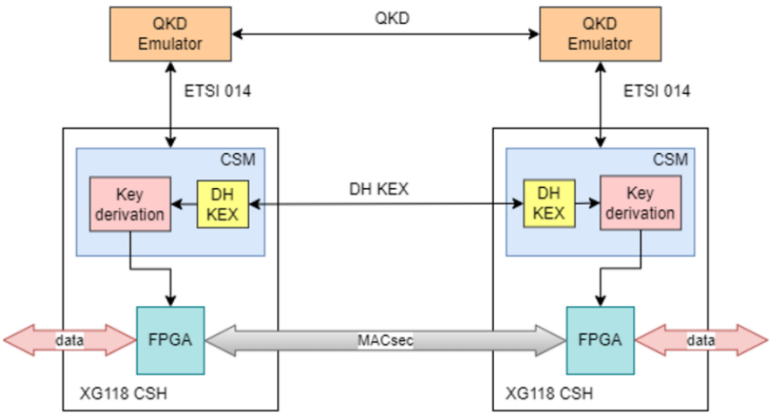

Bild 6. Testaufbau für einen quantenverschlüsselten Ethernet-Datenstrom.

Die im Projektplan vorgesehenen eigenen Arbeiten für ein Schlüsselmanagementsystem (KMS) wurden nicht durchgeführt. Im Projekt haben drei weitere Partner an einem KMS gearbeitet, die Anforderungen hierfür sind auf ein Konzept zugeschnitten, das Quantenschlüssel als Service zur Verfügung stellt und zwischen einem Kernbereich des KMS unter Kontrolle des Providers, sowie einem Access-Link unterscheidet. Das passte nur bedingt zu unseren anderen Aktivitäten im Bereich KMS, die sich stark auf ein dezentrales, verteiltes KMS konzentrierten. Ein weiteres zentrales KMS für DemoQuanDT hätte aus unserer Sicht aber keinen großen Mehrwert für das Projekt bedeutet.

2.4 AP4 Referenzlabor

Adva hat quasi als Überbrückung zunächst zwei L1-Verschlüsseler (5TCE-AES10G) mit QKD-Schnittstelle (ETSI-014) für das Testlabor zur Verfügung gestellt, um gelieferte QKD-Geräte und KMS-Implementierungen zu testen. Die QKD-Schnittstelle ist bei den L1-Geräten seit vielen Jahren ein offizielles Feature und in zahlreichen Konfigurationen erprobt. Allerdings konnten die L1-Geräte nicht im Demonstratorlink eingesetzt werden, da es sich bei der Datenverbindung um einen Ethernet-Kanal handelt. Deshalb haben wir im dritten

Projektjahr entsprechende L2-Verschlüsseler (XG118pro CSH, Ethernet) mit einer Demoversion der ETSI-014-Schnittstelle verfügbar gemacht. Sowohl für das L1- als auch das L2-Equipment haben wir für Konfiguration und Inbetriebnahme im Referenzlabor Unterstützung geboten und insbesondere das L1-Equipment wurde intensiv für Tests genutzt.

Der QKD-Emulator wurde im engen Austausch mit der Deutschen Telekom erstellt und im Referenzlabor mit unserer Unterstützung getestet.

2.5 AP5 Demonstrator

Adva war über die gesamte Projektlaufzeit in die Diskussion zu möglichen und sinnvollen Tests und Showcases für den Demonstrator-Link eingebunden. Der QKD-Emulator wurde auf der Teststrecke für das virtuelle Rerouting sowie bei Ausfall eines physischen QKD-Gerätes eingesetzt. Es wurde mit unserer Unterstützung auch getestet ob das steuerbare Dämpfungselement von Adva (FSP3000 VOA-Karte) geeignet ist, um in der Demonstration variable Übertragungsbedingungen für den Quantenkanal zu erzeugen.

Weiterhin haben wir die Deutsche Telekom bei der Installation und Konfiguration der Ethernet-Verschlüsseler in Berlin und Bonn unterstützt. Ein Konfigurations-Guide wurde erstellt, der die Installation der Ethernet-Geräte mit dem experimentellen QKD-Interface beschreibt. Leider konnte das Paar aus zeitlichen Gründen nicht mehr vollständig auf der Teststrecke in Betrieb genommen werden. Die Hardware ist aktuell noch vor Ort und steht (ggf. nach einem Softwareupdate) für die finale Inbetriebnahme und weitere Tests auf dem Link zwischen Berlin und Bonn zur Verfügung.

3 Erläuterung der wesentlichen Kostenpunkte

Der ganz überwiegende Anteil der Kosten im Projekt entfiel auf **Personal- und zugehörige Verwaltungskosten**. Dabei liegen die angefallenen Kosten ca. 25% unter dem veranschlagten Wert im Projektantrag. Dies liegt im Wesentlichen an den in AP3 vorgesehenen eigenen Arbeiten für ein Schlüsselmanagementsystem (KMS), die tatsächlich nicht durchgeführt wurden. Grund hierfür waren einerseits, dass bereits drei andere Partner ebenfalls ein KMS für das Projekt entwickelt haben, ein weiteres KMS hier also nur einen bedingten Mehrwert beigetragen hätte. Andererseits passte das spezielle Serviceproviderkonzept der Deutschen Telekom nicht zu unseren anderen Forschungsaktivitäten im Bereich KMS und hätte einen Mehraufwand bedeutet, den wir im vorliegenden Projekt nicht abgedeckt haben.

Der Betrag für **Material** war deutlich geringer war als ursprünglich engeschätzt. Dies hängt hauptsächlich an den Arbeiten für ein KMS, die entfallen sind. Für das KMS hatten wir im Material optional Ethernet-Geräte in allen Knoten vorgesehen, die dann folglich nicht benötigt wurden.

Der Betrag für **Reisen** liegt ebenfalls deutlich unter den ursprünglich veranschlagten Kosten. Dies lag zum einen daran, dass weniger persönliche Projekttreffen stattfanden als geplant, viele Meetings wurden auch nach der Covid19-Pandemie virtuell durchgeführt, was sich als sehr effizient herausgestellt hat. Daneben sind wir nicht zu den Standardisierungsmeetings der ETSI angereist, da die Aktivitäten der QKD-Gruppe in der Projektlaufzeit nicht sehr relevant für unsere Arbeiten im Projekt waren.

Unter **sonstige unmittelbare Vorhabenskosten** waren Gebühren für Veröffentlichungen vorgesehen, es sind im Projekt für Adva allerdings keine derartigen Kosten angefallen (die Kosten für das Architekturpaper hat der Einfachheit halber der Erstautor komplett übernommen).

Um Verzögerungen vor allem bei der Lieferung der QKD-Geräte für den Projektpartner Deutsche Telekom auszugleichen, wurde eine Projektverlängerung um drei Monate beantragt und gewährt. Die Verlängerung war kostenneutral möglich, da noch ausreichend Personalmittel verfügbar waren.

4 Notwendigkeit und Angemessenheit der geleisteten Projektarbeiten

Auch wenn der Schwerpunkt der Arbeiten von Adva mit dem L2-Verschlüsseler und dem QKD-Emulator nicht im Zentrum der Aktivitäten standen haben wir durchaus wichtige Beiträge zum Gesamterfolg des Förderprojekts geleistet. Auch eine andauernde Begleitung bei den langen Diskussionen zur Architektur, Management, Schnittstellen, Protokollen, etc. wäre ohne die Förderung nicht möglich gewesen.

5 Voraussichtlicher Nutzen, insbesondere die Verwertbarkeit des Ergebnisses – auch konkrete Planungen für die nähere Zukunft - im Sinne des fortgeschriebenen Verwertungsplans

Adva bietet seit vielen Jahren ein QKD-Interface für Verschlüsselungslösungen für 10GbE und 100GbE auf Layer 1 (OTN-Ebene) an. Auf Layer 2 (Ethernet) gab es bislang kein Gerät mit QKD-Interface, obwohl Kunden das durchaus nachgefragt haben. Es ist geplant das QKD-Interface für das Ethernet-Gerät FSP 150 XG118Pro CSH zum Produktfeature weiterzuentwickeln kommerziell anzubieten. Damit erweitern wir unser Angebot an Verschlüsselungslösungen mit QKD-Support auf eine zweite Geräteklasse. Wir planen auch in Zukunft das Portfolio von Verschlüsselern mit QKD-Schnittstelle regelmäßig zu erneuern, um auch weiterhin aktuelle Produkte mit QKD einsetzen zu können. Dabei werden die Verschlüsseler bereits einen hybriden Schlüsselaustauschmechanismus aus klassischer und post-quantum Schlüsseleinigung haben; der Quantenschlüssel kommt als dritte Komponente dazu und wird mit den anderen beiden Schlüsseln in einem sicheren Algorithmus kombiniert.

6 Der während der Durchführung des Vorhabens dem Zuwendungsempfänger bekannt gewordene Fortschritt auf dem Gebiet des Vorhabens bei anderen Stellen

Während des Vorhabens wurde in nationalem, europäischem und internationalem Umfeld vielfach an weiteren Teststrecken und Netzen für QKD gearbeitet. Soweit wir wissen, wurde in keinem anderen Projekt jedoch die anwendungsnahe Demonstration eines Quantenkommunikationsnetzes über alle für den praktischen Betrieb notwendigen Komponenten, Systemen und Prozessen hinweg angestrebt. Mit der Veröffentlichung der Architektur eines *carrier grade* QKD-Netzes wurde eine wichtige Referenz etabliert, auf die weitere Arbeiten verweisen und aufbauen können.

Adva Network Security verfolgt auch die aktuellen Entwicklungen in den Themenbereichen Quanteninformation und QKD. Der Fokus liegt hier vor allem auf den aktuellen Standardisierungsaktivitäten (u.a. ETSI, ITU-T). Aktuell ist eine neue Version der ETSI GS QKD 014 in der Diskussion, sie war allerdings noch nicht ausgereift genug, um sie im Projekt schon zu berücksichtigen. Adva war und ist auch Partner in den QuNET+-Projekten QuNET+ML, ISQKMS und Lorelay, zudem ist der Austausch mit weiteren QuNET+-Projekten über das

QuNET-Kernprojekt gewährleistet. Außerdem sind wir über weitere nationale und Europäische Aktivitäten über das Schirmprojekt des Innovationshubs für Quantenkommunikation (SQuaD) und die Industrieverbände DIVQSec und QuIC informiert.

Die Entwicklungen haben nicht dazu geführt, dass Änderungen im Projekt vorgenommen werden müssen.

7 Erfolgte oder geplante Veröffentlichungen des Ergebnisses nach Nr. 5 der NKBF/NABF

Ein gemeinsames Paper[2] des Konsortiums beschreibt die Architektur des *carrier-grade* QKD-Netzes wie im Projekt erarbeitet.

Daneben haben der Konsortialführer Deutsche Telekom, andere Projektpartner und auch Adva das Projekt und Ergebnisse auf zahlreichen Veranstaltungen vorgestellt. Präsentationen von Adva waren z.B.:

- ONDM 2023, invited, 'Quantum-safe optical transport'
- World of Quantum 2023, Panel on 'Quantum communication applications'
- OFC 2023/24, ShortCourse 'Secure Optical Communications'
- ECOC 2024, Workshop ‚Has the time come for quantum-secure optical networks?'

[2] P. Horoschenkoff et al., "DemoQuanDT: a carrier-grade QKD network," *Journal of Optical Communications and Networking*, vol. 17, no. 9, pp. 743–756, Sep. 2025, doi: 10.1364/JOCN.563470.