Abschlussbericht Teil 1

Kurzbericht

DemoQuanDT

16KISQ071

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

Inhalt

1 Ziel des Projekts 3
2 Ablauf des Vorhabens 3
3 Wesentliche Ergebnisse 4
4 Zusammenarbeit mit anderen Forschungseinrichtungen 4

1 Ziel des Projekts

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.

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.

2 Ablauf des Vorhabens

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.

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.

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. Das führte auch zu einem deutlich geringeren Materialaufwand als im Antrag ursprünglich veranschlagt.

3 Wesentliche Ergebnisse

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. 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. Nähere Details zum Emulator finden sich in einer dedizierten Dokumentation, die allen Projektpartnern zur Verfügung steht.

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. Die Demonstration besteht 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.

4 Zusammenarbeit mit anderen Forschungseinrichtungen

Im Rahmen des Projekts erfolgte keine organisierte Zusammenarbeit mit anderen Forschungseinrichtungen, allerdings ist Adva wie viele andere Projektpartner auch an weiteren Forschungsprojekten auf diesem Gebiet in anderen Partnerkonstellationen beteiligt. Das führt zu einer gewissen Vernetzung über einzelne Projekte hinweg.