18th International Conference on Space Operations, Montreal, Canada, 26 - 30 May 2025.

SpaceOps-2025, ID # 270

MuQuaNet - Applying quantum-secure communications to space operations

Jan Pitann[a]*, Stephan Borek[a], Rossella Falcone[a], Andreas Spörl[a], Nikolas Pomplun[a], Swantje Kastrup[b], Fabian Farina[b]

[a] *German Space Operations Center (GSOC), Deutsches Zentrum für Luft- und Raumfahrt e.V. (DLR), Germany, jan.pitann@dlr.de*
[b] *University of the Bundeswehr, Germany*
* Corresponding Author

Abstract

The development towards fault tolerant quantum computers has accelerated in recent years. It is therefore, reasonable to posit that quantum computers will be able to solve numerical problems previously unsolvable in a reasonable amount of time. This is particularly relevant in the context of factoring large composite numbers and solving the discrete logarithm problem. These two mathematical problems form the foundation for the vast majority of asymmetric encryption systems and key exchange procedures (such as RSA, DH, ECDH, ECDSA, and so forth). It is anticipated that quantum computers with cryptographic capabilities will become available within the next one or two decades.

A significant number of high-security applications require the encryption of classified material beyond this timeframe. Consequently, the mitigation of the threats posed by quantum computers to classical encryption schemes has become a race against time, already. Currently two approaches are discussed to ensure quantum secure encryption and communications after the breakthrough of quantum computers.

The first approach is called Post-Quantum-Cryptography (PQC). Here, new encryption and signature schemes are implemented based on mathematical problems which are hard to crack classically and by quantum computers.

The second approach is based on a secure exchange of encryption keys and is referred to as Quantum Key Distribution (QKD). This approach utilizes the quantum mechanical properties of photons in a way that enables the sending and receiving parties to detect any attempts by an eavesdropper to record or alter the transmitted keys. If the successfully transferred keys are used only once for encryption unconditional security can be achieved in theory.

Nevertheless, quantum key distribution (QKD) requires either dedicated fiber-optic lines that are solely used for the key exchange, commonly referred to as a dark fiber network or free-space links, which utilize a laser terminal and a telescope as the sender and receiver, respectively. Free-space links can be employed for mobile applications that facilitate quantum-secured communication with minimal deployment times over distances of several kilometers. Moreover, free-space links are utilized to exchange quantum keys between optical ground stations (OGS) and QKD satellites. By leveraging the in-orbit deployment of quantum keys, QKD enables the establishment of secure long-distance connections.

DLR (Deutsches Luft- und Raumfahrtzentrum) is part of the Munich Quantum Network (MuQuaNet), which is a research dark fiber network situated in the metropolitan area of Munich. The project is spearheaded by the University of the Bundeswehr (Munich) and is operated in conjunction with a number of other research facilities and governmental institutions. The QKD network is comprised of multi-vendor QKD devices, including both prepare-and-measure and entanglement-based systems. DLR, in particular the German Space Operation Center (GSOC) assumed the task of demonstrating the use case of encrypting the ground segment for satellite operations employing QKD.

This presentation will provide an overview of the current status of our work, including a technical explanation of the implementation and a general description of the approach used to encrypt part of our TMTC data streams as part of this QKD experiment.

Keywords: DLR-GSOC, Quantum Key Distribution, Optical Quantum Communication, System Security, Cryptography, Ground segment

Acronyms/Abbreviations

Advanced Encryption Standard (AES), Command Link Control Word (CLCW), Custom of the shelf (COTS), Diffie-Hellman-Key-Exchange (DH), Discrete Logarithm Problem (DLP), Deutsches Zentrum für Luft- und Raumfahrt – German Aerospace Center (DLR), Elliptic-curve Diffie–Hellman key exchange (ECDH), German Space Operation Center (GSOC), Ground Station (G/S), Ground Station Network (GSN), Key management system (KMS), National Institute of Standards and Technology (NIST), Multipath Key Reinforcement (MKR), Optical Ground Station (OGS), Oberpfaffenhofen (OP), Post Quantum Cryptography (PQC), Quantum Communication Infrastructure (QCI), Quantum Key Distribution (QKD), Security Ascociation (SA), Space Craft (S/C), Telecommand (TC), Telemetry (TM), Virtual Private Network (VPN)

1. Introduction

In today's digital landscape, cryptography has become an indispensable component of both personal and professional communication. The use of encryption methods is no longer a luxury, but a necessity for safeguarding sensitive information in various aspects of life. In the context of satellite operations, data management is viewed through the lens of three primary concerns: Confidentiality, Integrity, and Availability. Satellite operators recognize that protecting data flow across the entire system, from the ground station network (GSN) to the spacecraft (S/C), is crucial. This entails ensuring secure transmission of sensitive telemetry (TM) and payload data, as well as safeguarding telecommands (TC) from interception or tampering.

Moreover, with the increasing reliance on internet-based applications for coordinating tasks across the ground segment, security has become a top priority. Applications (e.g. OpsWeb [1]) must be designed with robust security features to prevent unauthorized access and data breaches. In essence, safeguarding sensitive information in satellite operations requires a multi-layered approach that incorporates encryption methods, secure data transmission protocols, and robust cybersecurity measures. By adopting these best practices, satellite operators can ensure the confidentiality, integrity, and availability of their data, thereby maintaining the trust and reliability of their operations.

Classically, next to symmetric and asymmetric encryption, digital signatures and key exchange protocols are used for this purpose.

Symmetric encryption relies on a single secret key for both encryption and decryption processes. The Advanced Encryption Standard (AES) is one of the most widely used symmetric encryption algorithms, offering robust security and efficiency. Asymmetric encryption in contrast utilizes a pair of keys: a public key and a private key. This approach enables secure communication while maintaining confidentiality. RSA (Rivest-Shamir-Adleman), a prominent asymmetric encryption algorithm, relies on the difficulty of prime number factorization to ensure security.

Key exchange algorithms are employed to securely share a secret key between two parties without exchanging credentials. One such widely used algorithm is Diffie-Hellman (DH), which enables two parties to agree on a shared secret key over an insecure channel through repeated calculations and logarithmic arithmetic properties. Also known as the discrete logarithm problem (DLP). This method is very common to exchange for example temporary session keys for encrypted connections (e.g. SSH, TLS etc.). Digital signatures are another crucial application of asymmetric encryption, which allow for verification of identity and authenticity of data. By encrypting a message or dataset with their private key, senders create a unique signature that can be verified by recipients using the sender's public key.

The computational complexity of these cryptographic techniques lies in the difficulty of solving certain problems, such as prime number factorization and discrete logarithm problem. These challenges are largely due to their exponential nature, making them resistant to brute-force attacks or specialized algorithms.

However, this will change dramatically with the advent of quantum computer systems. A quantum computer is a type of computer that uses the principles of quantum mechanics to process information and perform calculations. Unlike classical computers, which use bits that can only be in one of two states (0 or 1), quantum computers use qubits that can exist in superposition of states simultaneously, allowing for much faster processing of complex data. Currently quantum computers are still restricted by relatively low number of qubits, short coherence times (the time before the quantum state of a qubit decays into a classical system) and noise/errors. But, the development in this area has gained considerable momentum over the last few years.

The so-called Shor algorithm in particular represents a future threat to the current asymmetric encryption schemes. This algorithm for execution on quantum computing systems is capable of solving both the prime number factorization and the solution of the DLP in polynomial time (i.e. in a foreseeable period of time). With the development of sufficiently powerful quantum computer systems, common methods such as RSA and DH will be broken. Asymmetric crypto methods that use elliptic curves are also vulnerable to the Shor algorithm [2]. The German government and the German Federal Office for Information Security (BSI) assume that cryptographically relevant quantum computer systems will be available in the early 2030s[1]. So, it can be concluded that all established asymmetrical encryption systems will be broken in the next one or two decades.

To secure communication networks against potential quantum threats, the development of post-quantum cryptography (PQC) and quantum key distribution (QKD) is a rapidly evolving field, with both significant advancements and recent setbacks. The selection of PQC algorithms by NIST has been a significant milestone in the development of quantum-resistant cryptography. The NIST PQC Competition, launched in 2016, aimed to identify algorithms that can withstand attacks from future quantum computers. While some algorithms have shown promise, recent developments highlight ongoing security concerns and limitations.[2]

One notable example is the Shortest Vector under Lattice Attack (SVLAD)-based algorithm SIKE, which made it to the fourth round of testing by NIST. However, in a recent demonstration, researchers were able to break SIKE, highlighting the need for continued research and improvement[3].Another lattice-based algorithm, Rainbow, has also been subject to attacks, with a team of researchers successfully breaking it during one weekend using a laptop [3]. Furthermore, a bug was discovered in a quantum algorithm for lattice-based cryptography, highlighting the importance of rigorous testing and validation[4]. These setbacks underscore the challenges of developing PQC algorithms that can effectively resist quantum attacks. To address these limitations, researchers are exploring hybrid approaches that combine traditional encryption methods with post-quantum cryptography techniques. This hybridization aims to enhance the resilience of PQC systems by leveraging the strengths of both classical and quantum-resistant cryptography.

QKD relies on the principles of quantum mechanics to secure key exchange between two parties over an insecure communication channel. Several approaches have been developed. On one hand, there so-called prepare and measure protocols. Here, single photons are prepared in a certain quantum state to carries the part of information of the transmitted key. For an eavesdropper it is impossible to measure and copy the quantum state without changing interfering with the quantum state of the original photo. So, an eavesdropper can be unveiled. On of the most widely used prepare-and-measure protocols is BB84 [4], which has become a standard in QKD due to its robustness against eavesdropping attacks.

Another set of protocols is based on the quantum-mechanical entanglement of photons, which poses an inherent source-intended security.

In terms of implementation, QKD can be deployed over various mediums, including standard fiber, free-space laser links, demonstrating recent advancements in feasibility for ground-based systems and dark fiber, which consists of dedicated single-mode fibers, is also being used for QKD applications due to their low noise and high security. While experimental setups already established fiber based twin-field QKD exchange over more than 830 km [5] typical QKD setups available on the open market only have a maximum range of a bit more than 100 km or much less, due to losses and attenuation in the locally available fiber connections. However, first examples of large-scale quantum networks are already in place using multiple trusted node. For example, South Korea established in 2022 a fiber based QKD network spanning over 800km in total, providing 27 individual QKD links between trusted nodes.[5]

More recently, space-based QKD has emerged as a promising area of research, with examples such as the Chinese satellite QKD missions [6] demonstrating its feasibility.

[1] https://dserver.bundestag.de/btd/19/252/1925208.pdf

[2] https://csrc.nist.gov/Projects/post-quantum-cryptography/selected-algorithms

[3] https://arstechnica.com/information-technology/2022/08/sike-once-a-post-quantum-encryption-contender-is-koed-in-nist-smackdown/

[4] https://sebastienrousseau.com/2024-04-22-bug-discovered-in-quantum-algorithm-for-lattice-based-crypto/index.html

[5] https://www.idquantique.com/quantum-safe-security/nation-wide-quantum-safe-key-distribution-network-in-south-korea/

Another notable initiative was recently launched by the European Commission. The EuroQCI initiative aims to strengthen Europe's digital sovereignty by deploying a highly secure quantum communications infrastructure (QCI) in the EU countries and the European overseas territories. The aim is to establish terrestrial, fiber-based QKD networks at national level. To establish cross-border links between the national terrestrial networks a space segment is planned. At first, the QKD-satellite Eagle-1 to be launched soon by ESA will take over the distribution of quantum keys from orbit. DLR Institute for Navigation and Communication (DLR-KN) in Oberpfaffenhofen is operating on of the optical ground stations for the IOT phase of Eagle-1 [7].

Overall, the development of PQC and QKD algorithms underscore the ongoing efforts to secure communication networks against potential quantum threats. While setbacks have occurred, continued research and innovation are essential to advancing the state of the art in these fields.

2. MuQuaNet

The MuQuaNet (Munich Quantum Network) is an EU-funded dtec.bw-project aiming to build a quantum communication infrastructure (QCI) for research and development in the larger Munich area. Under the University of the Bundeswehr[6] Munich (UniBw), various organizations from the public and private sectors collaborate, either through the provision of their expertise or through integration into the network orchestration. The research areas covered are as diverse as the partners involved, ranging from QKD hardware development to network integration, key management, data-intensive distributed applications and security analysis, to name but a few. The focus of this paper is on the potential of QKD integration into existing network and application architectures, which is also the focus of this section on MuQuaNet.

While the development of a free-space QKD system in collaboration with the Ludwig-Maximilians-Universität Munich (LMU) is a central part of the project, the vast majority of QKD systems are either off-the-shelf or custom built to be initially tested within the MuQuaNet project. The devices from manufacturers ID Quantique, HEQA Security (formerly QuantLR), KEEQuant, and Quantum Optics Jena (QOJ) were purchased to implement several different protocols. This QKD protocols implement either prepare-and-measure scheme or are entanglement-based. While this is certainly not the case for security analysis, when it comes to network integration, systems are treated as black boxes, providing only the interfaces intended by their developers.

Many other projects have already been concerned with multiplexing quantum channels with classical communication, as can be seen in a review by Bahrami from 2020 [8]. However, the commercially available products still need to mature more before they can be used stably in this environment. The QKD devices in the MuQuaNet use dedicated dark fiber links.

Those connect the sites of the following project partners:

- University of the Bundeswehr Munich (UniBw)
- Deutsches Zentrum für Luft- und Raumfahrt (DLR)
- Ludwigs-Maximilians-Universität Munich (LMU)
- Zentrale Stelle für Informationstechnik im Sicherheitsbereich (ZITiS), Central Office for Information Technology in the Security Sector – a federal agency of the German goverment
- BWI – privately structured but publicly owned IT service provider of the Bundeswehr
- Airbus – the largest aerospace company in Europe
- Bundeswehr barracks in the north of Munich – organizationally managed by the BAAINBw (Federal Office of Bundeswehr Equipment, Information Technology and In-Service Support)

[6] The Bundeswehr are the armed forces of the Federal Republic of Germany.

The UniBw connects its institutes INF (computer science), ETTI (electronics and technical computer science), EIT (electrical power systems and information technologies; in collaboration with the dtec.bw-project SeRANIS), the RZ (its data center), and the dtec.bw office, which are all located on the campus in Neubieberg (in the south of Munich). Among these UniBW's interconnected institutes is also FI CODE (Research Institute for Cyber Defence), located in Neuperlach within Munich. It has a direct QKD link with the INF institute. All the nodes are shown in Figure 1.

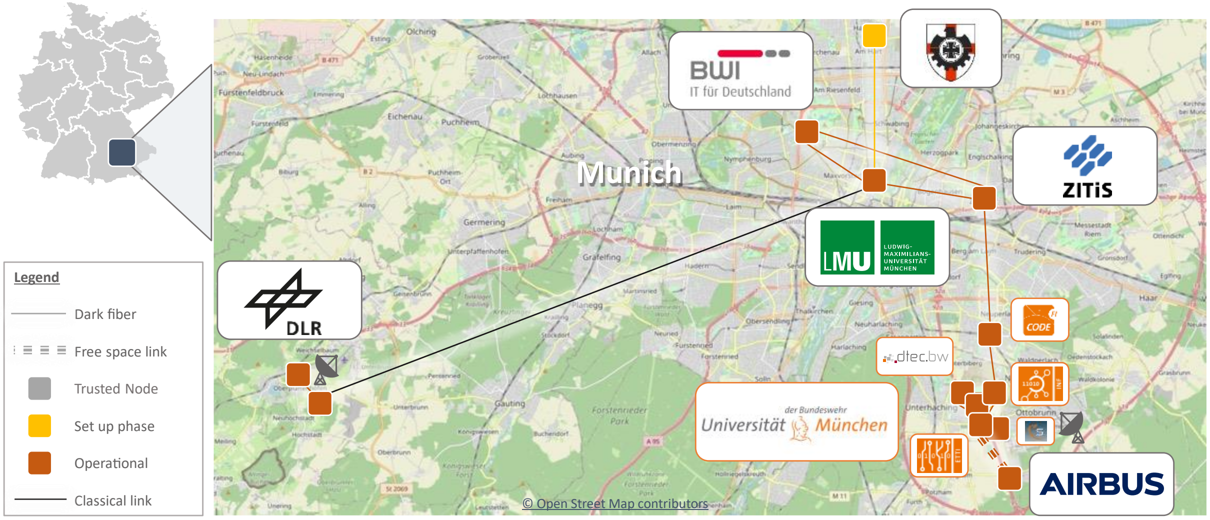


Figure 1 - QCI Topology of the MuQuaNet

A dark fiber connection between the LMU in Munich and the DLR campus in Oberpfaffenhofen is planned. The procurement is ongoing, but not available yet. Hence, we only have classical communication channels. Therefore, local dark fiber connections were set up at the DLR Campus OP. Beside the local setup at GSOC, we also tested dark fiber connections between GSOC and DLR-KN (round trip distance around 2km).

In order to deploy machines running the KMS and test distributed applications, most nodes of the network are equipped with a server for virtualization, and several additional components required for classical communication. While the network’s organization aims at a high degree of decentralized control mechanisms, the vast majority of systems get monitored and managed from the central hub located within the FI CODE.

3. Use of QKD in mission Operations

3.1 Encryption scenarios

Before examining the various encryption scenarios in satellite mission operations, it is necessary to consider the data flows between MCS, ground station and spacecraft. Both telemetry and telecommand data are transmitted in frames containing single or multiple data packets including metadata. This is described in more detail in the CCSDS standards [9,10,11,12]. Most of the missions operated at GSOC also use the PUS standard [13] at packet level. In addition to the data structure, services are defined which can be implemented in the space and ground segments.

Parts of the CCSDS standard are used at frame level and for network traffic in the ground segment. The nesting of packets in frames and other network protocols is shown in Figure 2 and Figure 3. Only CLTUs (Communications Link Transmission Unit) and TM transfer frames are processed on the satellite. All protocol layers further out are solely used for network traffic within the ground segment.

CLTUs are used to transmit telecommands from the ground to the satellite, while TM transfer frames are transmitted from the satellite to the ground segment.

Connections in the ground segment are established using the CCSDS Space Link Extension (SLE) standard, with all SLE connections having timeouts by default.

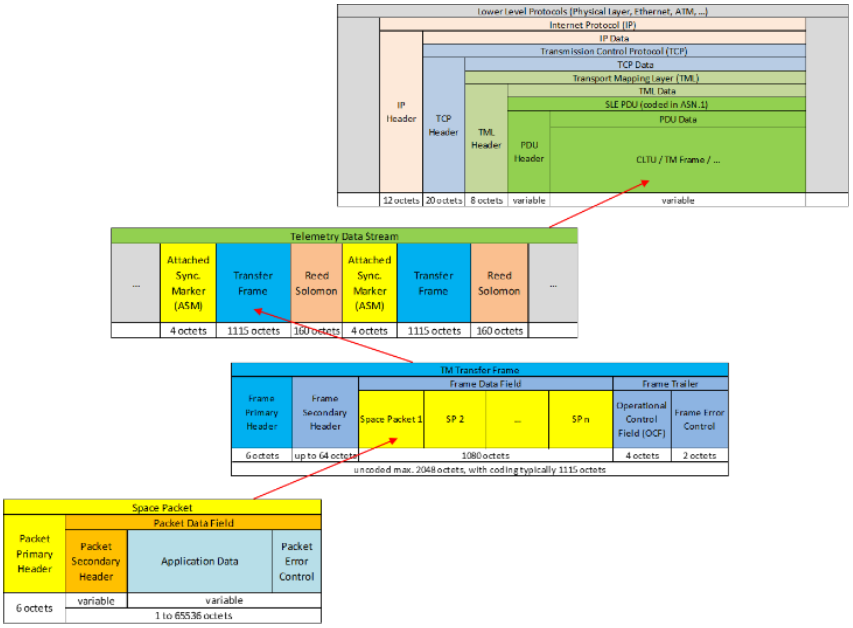


Figure 2 - Structure of TM frames and packets

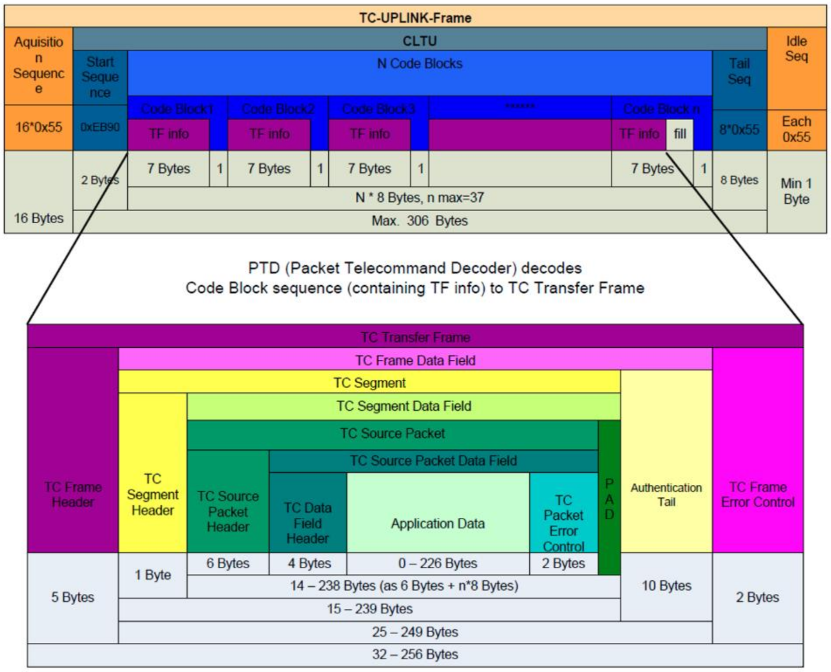


Figure 3 - Structure of TC packets/frames, embedding into CLTUs

SLE comes with its own "Internet SLE Protocol" (ISP) service [14] for establishing connections and transmitting data (Figure 4). CLTUs or TM transfer frames are embedded in Protocol Data Units (PDUs) and transmitted using Transport Mapping Layer Messages (TML).

To ensure end-to-end encryption from the MCS in the control center to the satellite, this must be done at frame or packet level. Connection-based methods (e.g. IPSec, MACsec), on the other hand, can only be used to encrypt the transmission in the ground segment, e.g. using SLE.

Encryption at frame or packet level has both advantages and disadvantages.

The encryption of entire frames is technically the easiest to implement, as it only requires encryption at the interface between MCS and SLE on the ground station site. On the satellite, the crypto module can be connected directly to the TC decoder and TM encoder without any additional logic. However, a failure of the encryption leads to considerable problems. On the one hand, no unencrypted HighPrio commands[7] can be sent to the satellite in an emergency. The CLCW cannot be transmitted unencrypted in the downlink, i.e. when the encryption malfunctioning, the ground segment cannot detect lost TC frames or monitor the status of the receiver. These are just some of the problems that occur.

These problems can be avoided by encrypting only the application data of the packets, for example. In this case, a risk analysis must be carried out during mission preparation to determine whether the unencrypted transmission of header information is safe. The technical implementation is also more complex as a plugin must be used to intervene directly in the MCS during TC packet generation and before embedding in the CLTU.

At present, we do not have a QKD-capable satellite available for GSOC, which is why research and testing of QKD is focused on the ground segment encryption. We have currently selected a single exemplary application for the ground segment to demonstrate a QKD-encrypted data transfer.

[7] HighPrio commands are always sent unencrypted, bypassing the on-board computer and triggering special on-board commands that are hardwired directly into the satellite bus. These commands are used to put the S/C into a stable state (SafeMode) in the event of a contigency.

The first focus was on the delivery of telemetry and the client-server connection of our SatMon TM display system was selected for demonstration purposes.

3.2 QKD encrypted TM transfer with SatMon

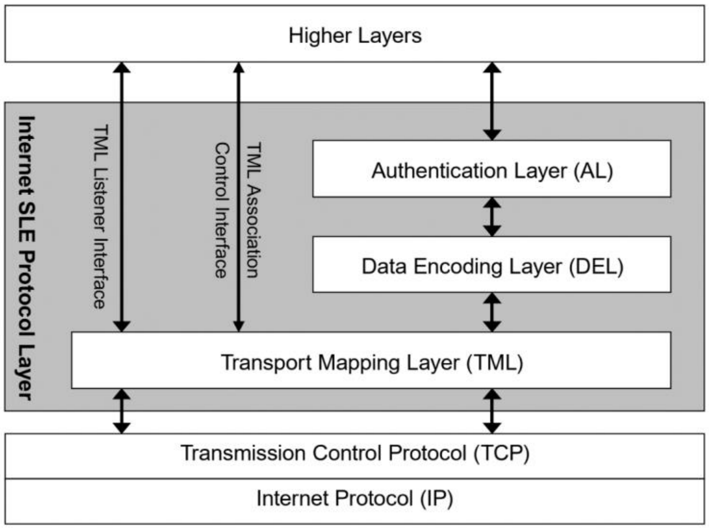
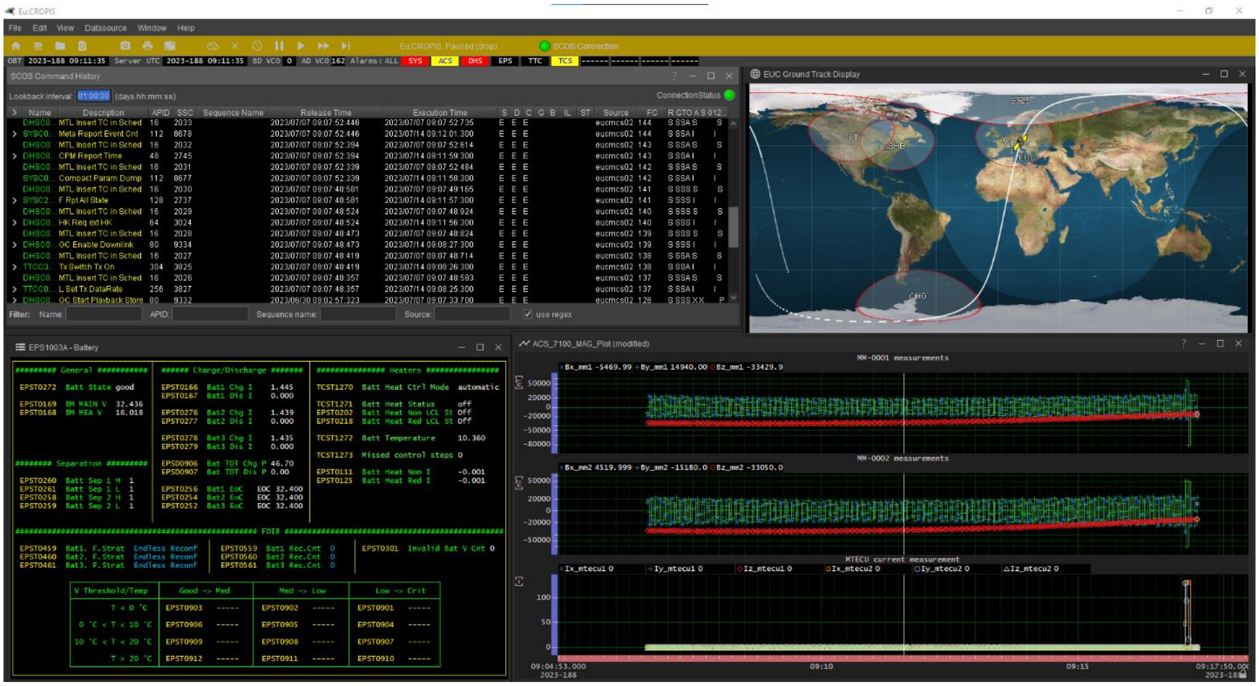

Higher Layers
Internet SLE Protocol Layer
TML Listener Interface
TML Association Control Interface
Authentication Layer (AL)
Data Encoding Layer (DEL)
Transport Mapping Layer (TML)
Transmission Control Protocol (TCP)
Internet Protocol (IP)

Figure 4 - Internet SLE Protocol from [14]

SatMon[8] is a comprehensive telemetry visualization software suite designed to monitor satellite activities in real-time. Its client-server architecture enables seamless data transfer between users and the system. Beside presenting the real-time telemetry, it provides fast access to archived and offline TM-data. The user interface offers a range of visualization options, including lists, parameter pages, overview dashboards, procedure guides, interactive plots, and reactive flow charts (an example is shown in Figure 5). As SatMon interfaces directly with the Monitoring and Control System (MCS, SCOS2K/GECCOS), it can display the command history and MCS-Events. Users can personalize their experience through an integrated editor, which allows them to create custom display pages for specific projects or tailor displays to suit individual needs. The server-site features include user authentication, encrypted connections, data flow control, a highly efficient telemetry database optimised for high storage density and low retrieval latency, and many admin tools for diagnostics and maintenance. For the MuQuaNet project at DLR we run a designated SatMon Server, which receives the telemetry stream from the MCS of a DLR EOL (end-of-life) mission. All packets containing the TM data are forwarded to the client using TCP socket connections.

The long-term goal is to encrypt the transmitted TM between DLR and the university using session keys derived from the transmitted QKD keys. The linear distance between the DLR campus in Oberpfaffenhofen and the next MuQuaNet QKD node in Munich is about 23 kilometers (see Figure 1).

[8] See our Software portfolio provide here: https://www.dlr.de/en/rb/about-us/departments/mission-technology-gsoc/mission-control-system


Eu:CROPIS
File Edit View Datasource Window Help
Eu:CROPIS Paused (drop)
SCOS Connection
OBT 2023-188 09:11:35 Server UTC 2023-188 09:11:35 BD VC0 0 AD VC0 162 Alarms: ALL SYS ACS DHS EPS TTC TCS
SCOS Command History
Lookback interval: 01:00:00 (days.hh:mm:ss)
ConnectionStatus
Filter: Name: APID: Sequence name: Source: use regex
EUC Ground Track Display
EPS1003A - Battery
ACS_7100_MAG_Plot (modified)
MM-0001 measurements
Bx_mm1 -5469.99 By_mm1 14940.00 Bz_mm1 -33429.9
MM-0002 measurements
Bx_mm2 4519.999 By_mm2 -15180.0 Bz_mm2 -33050.0
MTECU current measurement
Ix_mtecu1 0 Iy_mtecu1 0 Iz_mtecu1 0 Ix_mtecu2 0 Iy_mtecu2 0 Iz_mtecu2 0
50000
20000
0
-20000
-50000
-80000
100
50
0
09:04:53.000 2023-188
09:10
09:15
09:17:50.000 2023-188

	Name	Description	APID	SSC	Sequence Name	Release Time	Execution Time	S	D	C	G	B	IL	ST	Source	FC	R GTO A S 012...
	DHSC0...	MTL Insert TC in Sched	16	2033		2023/07/07 09:07:52.446	2023/07/07 09:07:52.735	E	E	E					eucmcs02	144	S SSA S S
>	SYSC0...	Meta Report Event Cnt	112	8678		2023/07/07 09:07:52.446	2023/07/14 09:12:01.300	E	E	E					eucmcs02	144	S SSA I I
	DHSC0...	MTL Insert TC in Sched	16	2032		2023/07/07 09:07:52.394	2023/07/07 09:07:52.614	E	E	E					eucmcs02	143	S SSA S S
>	DHSC0...	CPM Report Time	48	2745		2023/07/07 09:07:52.394	2023/07/14 09:11:59.300	E	E	E					eucmcs02	143	S SSA I I
	DHSC0...	MTL Insert TC in Sched	16	2031		2023/07/07 09:07:52.339	2023/07/07 09:07:52.484	E	E	E					eucmcs02	142	S SSA S S
	SYSC0...	Compact Param Dump	112	8677		2023/07/07 09:07:52.339	2023/07/14 09:11:58.300	E	E	E					eucmcs02	142	S SSA I I
	DHSC0...	MTL Insert TC in Sched	16	2030		2023/07/07 09:07:48.581	2023/07/07 09:07:49.165	E	E	E					eucmcs02	141	S SSS S S
>	SYSC2...	F Rpt All State	128	2737		2023/07/07 09:07:48.581	2023/07/14 09:11:57.300	E	E	E					eucmcs02	141	S SSS I I
	DHSC0...	MTL Insert TC in Sched	16	2029		2023/07/07 09:07:48.524	2023/07/07 09:07:48.924	E	E	E					eucmcs02	140	S SSS S S
>	DHSC0...	HK Req ext HK	64	3024		2023/07/07 09:07:48.524	2023/07/14 09:11:56.300	E	E	E					eucmcs02	140	S SSS I I
	DHSC0...	MTL Insert TC in Sched	16	2028		2023/07/07 09:07:48.473	2023/07/07 09:07:48.824	E	E	E					eucmcs02	139	S SSS S S
>	DHSC0...	GC Enable Downlink	80	9334		2023/07/07 09:07:48.473	2023/07/14 09:08:27.300	E	E	E					eucmcs02	139	S SSS I I
	DHSC0...	MTL Insert TC in Sched	16	2027		2023/07/07 09:07:48.419	2023/07/07 09:07:48.714	E	E	E					eucmcs02	138	S SSA S S
>	TTCC3...	Tx Switch Tx On	304	3825		2023/07/07 09:07:48.419	2023/07/14 09:08:26.300	E	E	E					eucmcs02	138	S SSA I I
	DHSC0...	MTL Insert TC in Sched	16	2026		2023/07/07 09:07:48.357	2023/07/07 09:07:48.593	E	E	E					eucmcs02	137	S SSA S S
>	TTCC0...	L Set Tx DataRate	256	3827		2023/07/07 09:07:48.357	2023/07/14 09:08:25.300	E	E	E					eucmcs02	137	S SSA I I
>	DHSC0...	GC Start Playback Store	80	9332		2023/06/30 09:02:57.323	2023/07/07 09:07:33.700	E	E	E					eucmcs02	126	S SSS X X P

```
######### General ###########   ###### Charge/Discharge #######   ############### Heaters ################

 EPST0272  Batt State good       EPST0166  Batt Chg I    1.445     TCST1270  Batt Heat Ctrl Mode  automatic
                                 EPST0167  Batt Dis I    0.000
 EPST0169  BM MAIN V  32.436                                       TCST1271  Batt Heat Status     off
 EPST0168  BM MEA V   16.018     EPST0276  Bat2 Chg I    1.439     EPST0202  Batt Heat Nom LCL St Off
                                 EPST0277  Bat2 Dis I    0.000     EPST0218  Batt Heat Red LCL St Off

                                 EPST0278  Bat3 Chg I    1.435     TCST1272  Batt Temperature     10.360
                                 EPST0279  Bat3 Dis I    0.000
                                                                   TCST1273  Missed control steps 0
######## Separation #########   EPSD0906  Bat TOT Chg P 46.70
                                 EPSD0907  Bat TOT Dis P 0.00      EPST0111  Batt Heat Nom I      -0.001
 EPST0260  Batt Sep 1 H  1                                         EPST0125  Batt Heat Red I      -0.001
 EPST0261  Batt Sep 1 L  1       EPST0256  Bat1 EoC    EOC 32.400
 EPST0258  Batt Sep 2 H  1       EPST0254  Bat2 EoC    EOC 32.400
 EPST0259  Batt Sep 2 L  1       EPST0252  Bat3 EoC    EOC 32.400

############################################ FDIR ############################################

 EPST0459  Bat1. F.Strat  Endless Reconf   EPST0559  Bat1 Rec.Cnt  0   EPST0301  Invalid Bat V Cnt 0
 EPST0460  Bat2. F.Strat  Endless Reconf   EPST0560  Bat2 Rec.Cnt  0
 EPST0461  Bat3. F.Strat  Endless Reconf   EPST0561  Bat3 Rec.Cnt  0
```

V Threshold/Temp	Good -> Med	Med -> Low	Low -> Crit
T < 0 'C	EPST0903 -----	EPST0902 -----	EPST0901 -----
0 'C < T < 10 'C	EPST0906 -----	EPST0905 -----	EPST0904 -----
10 'C < T < 20 'C	EPST0909 -----	EPST0908 -----	EPST0907 -----
T > 20 'C	EPST0912 -----	EPST0911 -----	EPST0910 -----

Figure 5 - The SatMon Display system in action

3.2.1 QKD-Encryption on DLR campus

Until a fiber connection between Munich and Oberpfaffenhofen is available, tests with QKD-based encryption are performed at the DLR site using the campus fiber network. The demonstrator for QKD encrypted telemetry transfer using SatMon, setup at DLR, is shown in Figure 6.

Both QKD devices used are manufactured by the Swiss company ID Quantique. The Clavis XG named model (see Figure 8) is utilizing a modified BB84 QKD protocol to deliver derived symmetric AES-256 keys. The fiber connection operates in O and C band. The delivery of the processed keys and the device management is provided by an RJ45 ethernet port. More details can be found on the vendors web site[9].

The assembly consists of two parts, the server site and the client site. The server-site setup includes the SatMon server, a classic network switch and the QKD (A) device. On the client site, there is also a network switch, as well as the second QKD (B) device and a computer with the installed SatMon client.

Both QKD devices are connected to each other by two designated dark fibers. One fiber, the so-called quantum channel, transmits the prepared photons that carry the information for the quantum key to be transmitted. The second fibre is used for time synchronization of the two QKD devices. The raw keys are generated on QKD (A) and on QKD (B), so this is a one-way transfer. The public part of the transfer is done via the Ethernet connection.

The telemetry stream from the SatMon server to the client is routed between the two computers through both network switches. Especially the route between these two switches can be consider as “insecure” (representative for a regular Internet connection). Both QKD device deliver the derived AES key to the server or the client, respectively.

The encryption of the SatMon telemetry is done with a software utilizing Linux tun-device driver (/dev/tun). On the server, the outgoing TCP socket connections are routed through this software and data embedded into the transmitted TCP segments are encrypted with the AES key from QKD (A). The client listens to the socket on its site. After receives the so encrypted telemetry data, it is decrypted with the vailid AES key forwarded by the QKD (B). The TM data received in this way is then displayed in the SatMon client. All the induviduell components of the setup were tested seperatly, such as the exchange of QKD keys, enryption & satmon client/server connection and found to be

[9] https://www.idquantique.com/quantum-safe-security/products/clavis-xg-qkd-system/

operational. Figure 7 show exemplary statistics of the QKD key exchange between both QKD devices. However, the demonstration of the whole setup is still ongoing as of now.

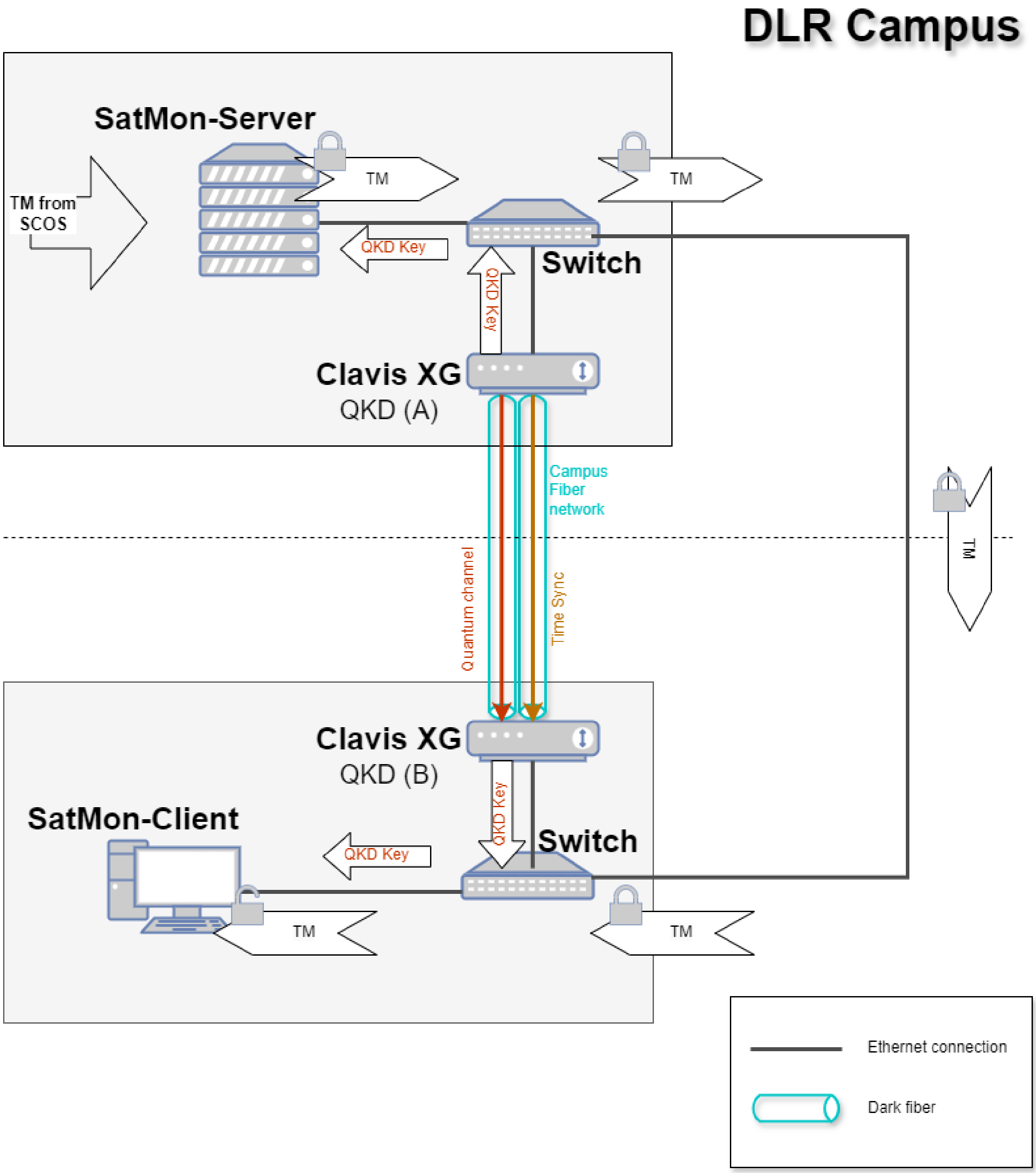


Figure 6 - QKD encrypted SatMon TM transfer at the DLR campus in Oberpfaffenhofen

3.2.2 Preparation for linking DLR-OP to the entire QKD network in MuQuaNet

To integrate GSOC and the DLR campus in Oberpfaffenhofen into the overall MQN network topology, the setup described in the previous section was extended. The central component here is a modified IPsec encryptor from the company Secunet, a "SINA L3 Box S 30M" (see Figure 8). It establishes a VPN with all other endpoints in the network also equipted with a SINA Box. A customized firmware extends the functionality of the SINA Box beyond the standard configuration. So the SINA box supports now different key exchange methods: the classical Diffie-Hellman using elliptic curves (ECDH), post quantum cryptographical key encapsulation mechanism (PQC-KEM) or QKD if available. If multiple paths from one endpoint to another are available, the SINA boxes support multipath key reinforcement (MKR). This means that the key material is split into separate chunks and transferred from one SINA box to another on disjoint routes. A potential adversary would have to compromise several security ascociation (SA) to obtain the complete key material. This ensures that endpoints that do not currently have a QKD connection can still be part of the VPN.

In this setup, there is only the SatMon server, the QKD device and the Sina Box is forseen at DLR. There is also a QKD device, an Sina box and the SatMon client on UniBW site. When the QKD dark fiber from Oberpfaffenhofen to Munich is available the SINA box can switch vom classical key exchange to QKD. The planned dark fiber link will transfer the QKD keys from Oberpfaffenhofe to the LMU. On every adjacent QKD connection from the LMU to the UnibW new QKD keys will be transferred. This managed by the KMS for MuQuaNet. The VPN set up in this way routes the telemetry from the SatMon-server at DLR to the SatMon-client on the UniBW site. Hence a secured TM transfer from DLR to the UniBW can be demonstrated. Currently, this is done using classic or PQC key exchange methodes. Once the dark fiber between Oberpfaffenhofen and Munich is established, we can seamlessly transition to QKD-based encryption.

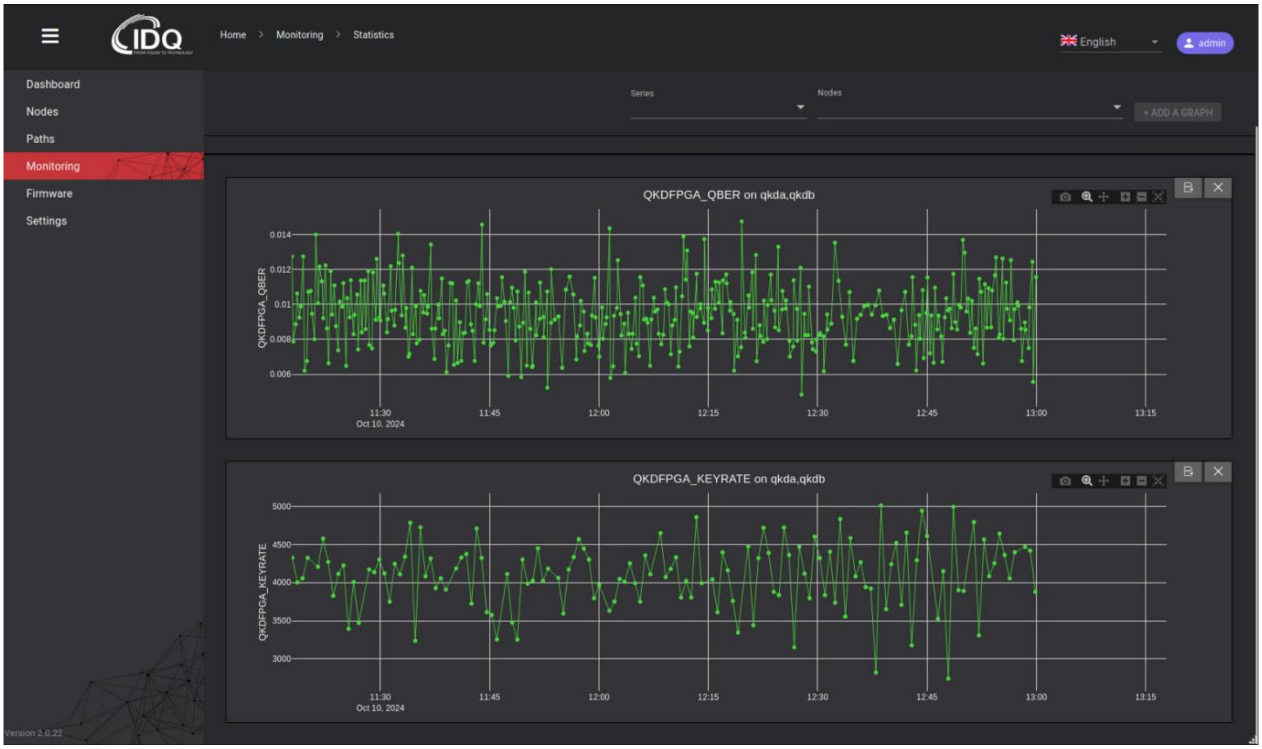


Figure 7 - Example QKD statistics, top: relativ error rates [0:1], bottom: key exchange rates in bit/s (avrg. ~4kbit/s)

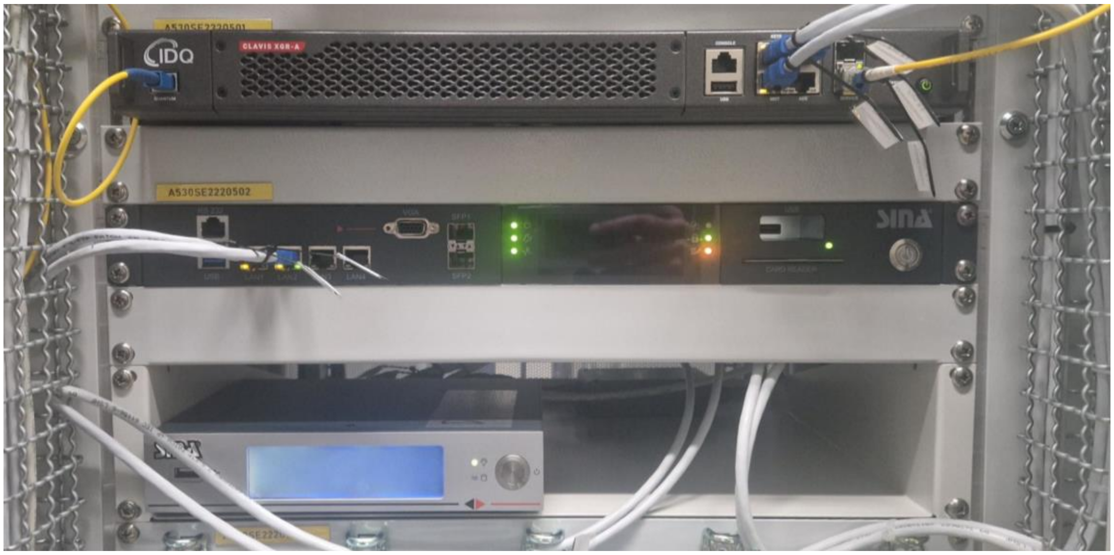


Figure 8 - shows the Clavis XG (QKD device, top) and the modified Sina 30M (grey box, bottom) in the rack

4. Roadmap for advancing GSOC's QKD capabilities

Several approaches are being pursued to strengthen GSOC's QKD capabilities within MuQuaNet and beyond. For example, we are planning to encrypt all data traffic in the ground segment with QKD. This will enable us to demonstrate the telecommunication capabilities of QKD-based encryption in addition to secure telemetry transfer. We want to use the V3C system for this purpose (see next section). We are also evaluating further options for expanding GSOC's dark fiber connections and are actively looking for opportunities to collaborate with other partners on the topic of QKD.

4.1 Full TMTC Encrytpion with V3C

V3C ("Verlegefähiges[10] Compact Control Center") is a highly mobile compact system for complete satellite command and control. The whole system runs self-sufficiently on a market-available SINA laptop approved for handling of classified information and is linked to an external antenna via a secured connection. It comprises mission and data-take planning, monitoring & control, flight dynamics and payload data processing. Objective of the V3C project is the provision of a quickly deployable, autonomous Mission Operations System as part of the German national capability for the "Responsive Space Cluster Competence Center"[11]. It shall allow secure and fully automated workflow-driven operations of special-purpose satellites by a single operator, e.g. earth observation using an optical instrument.

V3C is therefore the perfect tool for demonstrating data exchange, in particular telecommands with another ground station (real or simulated). The communication interface of V3C is based on the Internet SLE Protocol and therefore transparent for the QKD capable SINA *ipsec* encryptor. It is planned to use V3C in conjunction with the existing test setups to demonstrate the QKD encrypted TC transfer within the framework of MuQuaNet.

4.2 Further perspectives

The key to expanding GSOC's QKD capabilities is the expansion of connectivity to both ground-based QCI and satellite QKD systems. On the one hand, we are planning to connect partners in the immediate neighborhood of the DLR campus. In addition, it would be desirable in the long term to have a dark fiber connection between GSOC and DLR's central ground station in Weilheim (27 km linear distance). This would pave the way for the use of QKD encryption in the ground segment for future missions with elevated security requirements.

In order to strengthen our expertise in SatQKD, GSOC is leading a consortium with DLR-KN and other partners from Germany and Croatia which is submitting a proposal for the deployment and operation a QKD-capable optical ground station as part of the EU Commission's EuroQCI initiative. This OGS will be equipped with a QKD receiver for the EuoQCIs Space segment which will be ESA missions Eagle1. This allows to establish QKD cross-border links by connecting the pan-European QKD-OGSs with the national, terrestrial EuroQCI QKD networks.

DLR is also involved in networking initiatives to promote the advancement of QKD technology, such as SQUAD[12] and PETRUS[13].

[10] German expression for a system that is mobile in the sense that it can be deployed at different places.

[11] https://www.dlr.de/en/rs

[12] https://www.squad-germany.de/

[13] https://petrus-euroqci.eu/

Acknowledgements

This research paper is funded by dtec.bw -- Digitalization and Technology Research Center of the Bundeswehr. dtec.bw is funded by the European Union -- NextGenerationEU.

We appreciate the support of Stefan Gärtner for the preparation to integrate V3C into the framework. He is presenting V3C in his SpaceOps 2025 contribution #124: „V3C: Mobile Control Center for Autonomous Satellite Operations”. Our special thanks go to Michael Aschenbrenner, Enrique Knorr and Michael Szczuka from our IT department for their persistent and patient support during the QKD test setup at GSOC. We would also like to thank Florian Moll from DLR-KN for sharing his expertise on QKD and helping us to push the topic on the dark fiber connection to Munich. Above all, my thanks go to the whole MuQuaNet team for the great cooperation.

References

[1] Pitann et al., OPSWEB – A comprehensive management tool for mission operations, *Proceedings of the 17th International Conference on Space Operations, Dubai*, ID #374 GSE, 2023

[2] Roetteler, M., et al., Quantum resource estimates for computing elliptic curve discrete logarithms, Art. no. arXiv:1706.06752, 2017, https://arxiv.org/abs/1706.06752

[3] Beullens, W., Breaking Rainbow Takes a Weekend on a Laptop, *Proceedings of CRYPTO 2022 – Advances in Cryptology*, https://crypto.iacr.org/2022/papers/538804_1_En_16_Chapter_OnlinePDF.pdf, 2022

[4] Bennett, C. H., & Brassard, G., Quantum cryptography: Public key distribution and coin tossing. *Proceedings of IEEE International Conference on Computers, Systems and Signal Processing*, 175-179, 1984

[5] Wang, S., et al., Twin-field quantum key distribution over 830-km fibre. *Nat. Photon.* **16**, 154–161 (2022).

[6] Liao, SK., Cai, WQ., Liu, WY. *et al.*, Satellite-to-ground quantum key distribution. *Nature* **549**, 43–47, 2017

[7] Rivera, G.C., et al., Building Europe’s first space-based Quantum Key Distribution System – The German Aerospace Center’s role in the EAGLE-1 mission, *Proceedings of 75th International Astronautical Congress (IAC), Milan*, IAC–24–A.1.2.3, 2024

[8] Bahrami, A., Lord, A., & Spiller, T. (2020). Quantum key distribution integration with optical dense wavelength division multiplexing: a review. *IET Quantum Communication*, *1*(1), 9-15.

[9] CCSDS Recommended Standard, “TM Synchronization and channel coding”, CCSDS 131.0-B-4, September 2003, https://public.ccsds.org/Pubs/131x0b1s.pdf

[10] CCSDS Recommended Standard, “TM Space Data Link Protocol”, CCSDS 132.0-B-3, September 2003, https://public.ccsds.org/Pubs/132x0b1c1e1s.pdf

[11] CCSDS Recommended Standard, “Space Packet Protocol”, CCSDS 133.0-B-2, September 2003, https://public.ccsds.org/Pubs/133x0b1s.pdf

[12] CCSDS Recommended Standard, “TC Synchronization and Channel Coding”, CCSDS 910.4-B-2, July 2021, https://public.ccsds.org/Pubs/231x0b4e0.pdf

[13] ECSS Standard, ECSS-E-70-41A “Space engineering. Ground systems and operations - Telemetry and telecommand packet utilization”, January 2003

[14] CCSDS Recommended Standard, “Space Link Extension - Internet Protocol for Transfer Services,” CCSDS 913.1-B-1, September 2008, https://public.ccsds.org/Pubs/913x1b2.pdf