Network Architectures for Space-Optical Quantum Cryptography Services

Introduction of Quantum Communications in Satellite Communication Networks

Dominique Elser, Stefan Seel, Frank Heine
Division Laser Products
Tesat-Spacecom GmbH & Co. KG
Backnang, Germany
Dominique.Elser@tesat.de

Thomas Länger, Momtchil Peev
Safety & Security Department
AIT Austrian Institute of Technology GmbH
Vienna, Austria
Thomas.Laenger@ait.ac.at

Daniele Finocchiaro, Roberta Campo, Annamaria Recchia, Alessandro Le Pera
Development and Innovation Department
Eutelsat S.A.
Paris, France
dfinocchiaro@eutelsat.fr

Thomas Scheidl, Rupert Ursin
Institute for Quantum Optics and Quantum Information (IQOQI)
Austrian Academy of Sciences
Vienna, Austria
rupert.ursin@univie.ac.at

Zoran Sodnik
TEC-MMO
European Space Research and Technology Centre (ESTEC)
European Space Agency (ESA)
Noordwijk, The Netherlands
Zoran.Sodnik@esa.int

Abstract—**Quantum cryptography enables the distribution of 'information-theoretically' secure (ITS) keys, whose secrecy is guaranteed by the laws of quantum physics. Such a level of security is superior to conventional 'classical' cryptography whose security is at most 'computational', and even this lower security level is unverified in many cases. Fiber-based quantum key distribution (QKD) systems for link distances up to hundred kilometers are already available on the market since several years. However, there is no practical way to cover larger distances without employing a space-based relay. Therefore we propose here network architectures for space-optical quantum communication services. By a trade-off process between performance and cost, we have identified three scenarios that are capable to provide a large number of users on ground with ITS keys at affordable service fees. Here we detail the architectures of space, ground and control segment for operational space-based QKD services.**

Keywords - quantum communication; quantum cryptography; satellite communication; information security; optical communication; free space optics

I. INTRODUCTION

Applications and services based on Optical Quantum Communications could revolutionize information technology in the future. Quantum superposition and quantum entanglement constitute a novel type of resource, allowing the implementation of technological solutions which cannot be achieved with classical information technology alone. Examples are cryptographic quantum key distribution [1], [2] with an unprecedented level of security and the extension of information channel capacity beyond the theoretical maximum limit by quantum superdense coding [3]. Further potential applications are quantum state teleportation [4] in quantum repeaters and quantum computers [5].

In principle, due to the fact that quantum signals cannot be amplified, all of the aforementioned applications could benefit from a space-based infrastructure [6]. However, quantum state teleportation and quantum dense coding are currently too immature and impractical for real applications. Quantum key distribution (QKD), on the other hand, is technologically advanced enough for space applications. Therefore we focus here on the applicability of QKD to space-based telecommunication services, in order to protect user data channels on ground. In particular, we have performed a systematic trade-off of drivers, performance characteristics, merits and drawbacks, and specific constraints associated with deployment in the space environment. This allowed us to compile a list of the most promising services making essential use of Quantum Communication (for details of this trade-off process see [7]).

In this Paper, we first give an introduction in Quantum Key Distribution in chapter II. In chapter III, we present the selected

This work has been funded by the ARTES 1 Programme of the European Space Agency (ESA), Telecommunications and Integrated Applications Directorate (TIA) under contract number AO/1-6609/10/NL/NR, "Introduction of Quantum Communications (QC) In Satellite Communication Networks".

architectures of space-based quantum communication and the services that can be offered with these architectures. Chapter IV details the system components for space-based quantum communication and chapter V concludes.

II. QUANTUM KEY DISTRIBUTION

Quantum key distribution (QKD) [1], [2] is the process of establishing a secret shared key between two parties, traditionally named A (Alice) and B (Bob), see Figure 1. The security is based on the laws of quantum mechanics, in contrast to classical schemes, where security relies only on mathematical assumptions. Common public keys, for example, can be broken if an eavesdropper (E or Eve) disposes of an algorithm for efficient prime factorization. Although no such algorithm is known to exist in the public sphere, there is no proof that it cannot be developed. Another tool would be a quantum computer running Shor's algorithm [8] which already has been demonstrated for small numbers [9], [10]. Even without such an algorithm, the continuously increasing computational power of classical computers can be used to break currently used public keys, also retroactively.

The only encryption scheme which has been proven to be secure [11] is the one-time-pad [12], [13], where a key having the same length as the message is used only once. The issue of distributing large amounts of key material can be solved more efficiently by QKD than by human couriers. QKD guarantees the incorruptibility of the courier during its travel – a guarantee that classical information cannot offer [14].

In the last two decades, numerous QKD-protocols have been implemented by research groups. In recent years, QKD devices also have become commercially available, promoted by the start-ups ID Quantique in Geneva, MagiQ in Boston and New York, SmartQuantum in Lannion (Brittany-France), the Austrian Institute of Technology in Vienna, QASKY in Wuhu, China, qutools in Munich, QuintessenceLabs in Canberra, and SeQureNet in Paris. Bigger companies such as Siemens, NEC, HP and Mitsubishi are also active in the field [15]. Global telecommunication providers such as Thales and Toshiba hold QKD fiber-systems on standby in order to bring them on the market at the appropriate moment.

One of the bottlenecks of today's QKD systems is low key rate, typically about some kilobits per second. Thus only small data rates are possible using one-time-pad encryption. In order to increase data rate, e.g. for video transmission, QKD can be combined with classical algorithms. The keys for a classical block cipher, such as e.g. the Advanced Encryption Standard (AES), can be provided by QKD. The fiber-based QKD system Cerberis of ID Quantique, for example, can be operated in such a mode. Since the key is shorter than the message, unconditional security is not guaranteed. However, QKD allows for very frequent key exchange. An eavesdropper then has to break each new key separately, thus the complexity of this task is much higher than with purely classical methods.

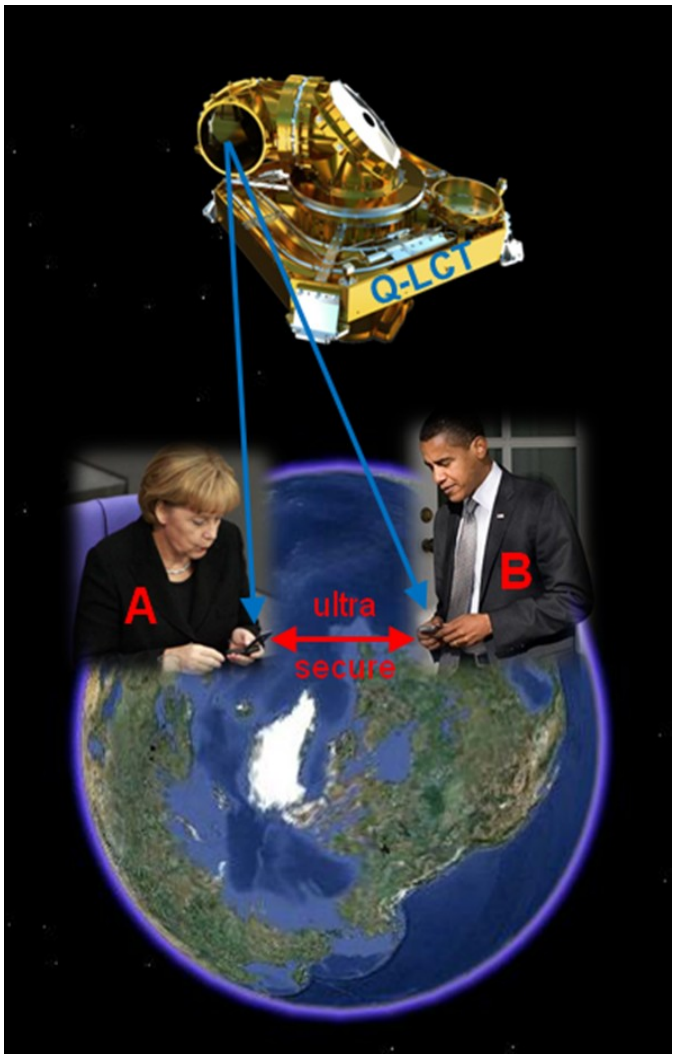

Figure 1. The users A and B on ground want to exchange confidential information. In order to do so, they use a quantum cryptographic key that is generated by means of the space-born Quantum Laser Communication Terminal (Q-LCT). (Picture of the Earth from Google Earth)

In the last few years, several demonstrations of QKD systems and networks were brought to the attention of the public, for example the DARPA/AFRL quantum network in Boston [16], a bank transfer in Vienna [17], QKD for the Swiss elections in Geneva [18], as well as operational QKD networks in Beijing [19], Vienna [20], Durban [21] and Tokyo [22]. With the exception of the Boston and Vienna networks, all QKD links were fiber-based. Free space QKD through the atmosphere, on the other hand, was already demonstrated in 1996 [23]. This first experiment used a prepare-and-measure scheme, meaning that Alice prepares quantum states and sends them to Bob, who performs measurements on the quantum states. A variety of prepare-and-measure implementations, using either single photons or coherent states as quantum signal, has been implemented since then [24], [25], [26], [27], [28], [29], [30]. Furthermore, entanglement-based [31] free space QKD has been implemented [32], [33], [34], [35], [36], [37], exploiting the non-classical coupling of photons that Einstein called “spooky action at a distance”.

III. ARCHITECTURES AND SERVICES OF SPACE-BASED QUANTUM COMMUNICATION

A. Architectures

In the trade-off process as described in [7], we have identified the two most promising architectures, one using a low earth orbiting satellite (LEO) and one using a geostationary earth orbiting satellite (GEO). These two architectures are capable to cover a significant range of QKD services (see below). Both architectures employ the existing TESAT Laser Communication Terminal (LCT) [38], [39], [40], see Figure 2 in the space segment to distribute the quantum signals to the ground. This configuration enables each ground station to establish a key with the satellite. The satellite carries a weak coherent pulse source because this part is usually less complex than the detecting end of the link. However, the satellite has to be equipped with key distillation (post processing) capability, as well as with storage for buffering the keys until they are handed over to the users on ground. Thus, the satellite can be considered as a moving node of a trusted repeater network, which enables two ground stations to sequentially establish a key with the satellite and to subsequently obtain a common key. The Quantum-LCT (Q-LCT) is effectively replacing the travelling human trusted (or potentially untrustworthy) couriers, which are nowadays still used to distribute keys for one-time pad encryption. In general, this scenario is an implementation of One-way QKD where one quantum state is sent at a time, but where the quantum satellite has to be trusted, similar to the mentioned human courier. In entanglement double-link systems, on the other hand, such trust in the satellite is not required. However, since in this case the satellite sends an entangled state simultaneously to two users on ground, the effective attenuation is the square of the single-link-attenuation. This is the main reason why entanglement double-link protocols lead to uneconomic costs for secure keys when not using a futuristic ground receiver, also leading to tremendous costs [7].

In general, the keys shared between grounds stations will be generated via the space segment during 'good weather conditions'. The keys can then be used at any time, independent of cloud coverage and visibility constraints. Thus weather conditions merely influence the key rate, but do not impede real-time communications.

The LEO based architecture allows secret key rates up to 13 megabits per day when used with a stationary ground terminal of 50 cm aperture. For mobile terminals for accommodation on trucks etc., we consider a 50 cm aperture too big and heavy, so we propose another configuration variant with a 25 cm aperture on ground. This configuration allows for secret key rates of about 3 megabits per day. For these two configurations, we have calculated the cost per megabit of user key with 77 €/Mbit and 312 €/Mbit, respectively. The GEO based architecture is able to achieve 39 megabits per day with a 200 cm aperture on ground, with cost per megabit of 615 €. The calculated costs are based on a return of investment period of 5 years. For further details of the calculation, please refer to [7].

B. QKD services

In the following, we present the QKD services that the selected three configurations are capable to provide:

1) One-way QKD by LEO Q-LCT with 13.5 cm aperture

a) Fixed ground terminals with 50 cm aperture

This configuration is capable to serve the needs of e.g.:

- Secure communication between Government seat and/or Ministry Headquarters
- Secure communication between command centers and operating centers, submarines and aircraft-carriers.

b) Mobile ground ground terminals with 25 cm aperture

This configuration is capable to serve the needs of e.g.:

- Database backups of banks, medium and large institutions and companies such as UBS, Citicorp, Oracle, Google, etc.
- Real-time stock exchange: Sensitive documents transmission and authentication of transfers (accountability).
- Supervisory Control and Data Acquisition (SCADA), such as the connections of oil/gas pipelines and nuclear power plants; QKD is used between the control center and the remote installations.

2) One-way QKD by GEO Q-LCT with 13.5 cm aperture and ground terminals with 200 cm aperture

This configuration is capable to serve the needs of e.g.:

- Secure communication between Foreign Ministry Headquarters and Embassies
- Inter-Governmental Organizations' (IGO) Head-quarters secure communication with their subsidiaries.
- Metropolitan Area QKD Network Interconnect: Fiber bound QKD networks (also including short ground-based free space links) are already today technically feasible and capable of high key distribution rates [19], [20], [21], [22]. These include trusted repeater networks with point-to-point quantum links between network nodes, as well as switched QKD networks, capable of providing direct optical connections between single network nodes by means of optical switching mechanisms and techniques. The size of such fiber bound QKD networks is however limited. For the latter case, the switched QKD networks, the maximum diameter of the network is limited by the maximum distance which can be achieved with one QKD link, which is about 100 kilometers. As the key generation rate decreases exponentially with distance, the maximum size of the network may even be smaller, depending on user behavior and requirements. For trusted repeater QKD networks,

Figure 2. TESAT Laser Communication Terminal (LCT) baselined for European Data Relay System (EDRS) and Global Monitoring for Environment and Security (GMES). The photo displays the LCT which has been integrated on the Alphasat GEO spacecraft.

there is no technological limitation of their maximum size, but larger distance means more nodes along the path which have to be trusted, which again confines the size of practical implementations to metropolitan area size. For intercontinental or long range communications, trusted repeater networks are clearly unfeasible. The idea of this use case is to interconnect some insular metropolitan area QKD networks by means of satellite QKD. One scenario could be to have a GEO satellite serving several QKD networks on a continental scale, e.g. metropolitan QKD networks in Europe.

IV. System Components of Space-based Quantum Communication

The space-based telecommunication network consists of several spatially distributed entities in three logical segments, the space, user, and control segments. The system architecture of the space-based telecommunication network identifies the components of the distributed entities and defines their relationship. The components shall be seen as 'logical components' and may in the final product become manifest in a different layout. An example would be several components implemented in software sharing the same computing platform, where the computing platform may be shared with another payload or functionality.

Both the LEO-based network with 25 cm and/or 50 cm ground terminals, as well as the GEO-based network with 200 cm ground terminals, are based on the same general architecture as defined in Figure 3.

The components of the system architecture are themselves composed of further components, potentially of different domains, like computer hardware, software, classical and quantum optics, sensors, actuators, and all kinds of interconnections and logic 'glue' between these components.

In the following, the components of the system architecture will be described in more detail, in order to facilitate and ease the definition of the system architecture requirements in chapter 4.

1) SCM – System control and management subsystem

The SCM controls the single components of the payload, being the Quantum Optical Subsystem (QOS/A or QOS/B), as well as the Quantum Laser Communication Terminal (LCT/A or LCT/B) and the QKD post-processing electronics (QPP), and the Key Database (QDB). Furthermore, it handles the access to the Classical Communication subsystem (CCS) and communicates with the Master Control and Accounting subsystem (MCA).

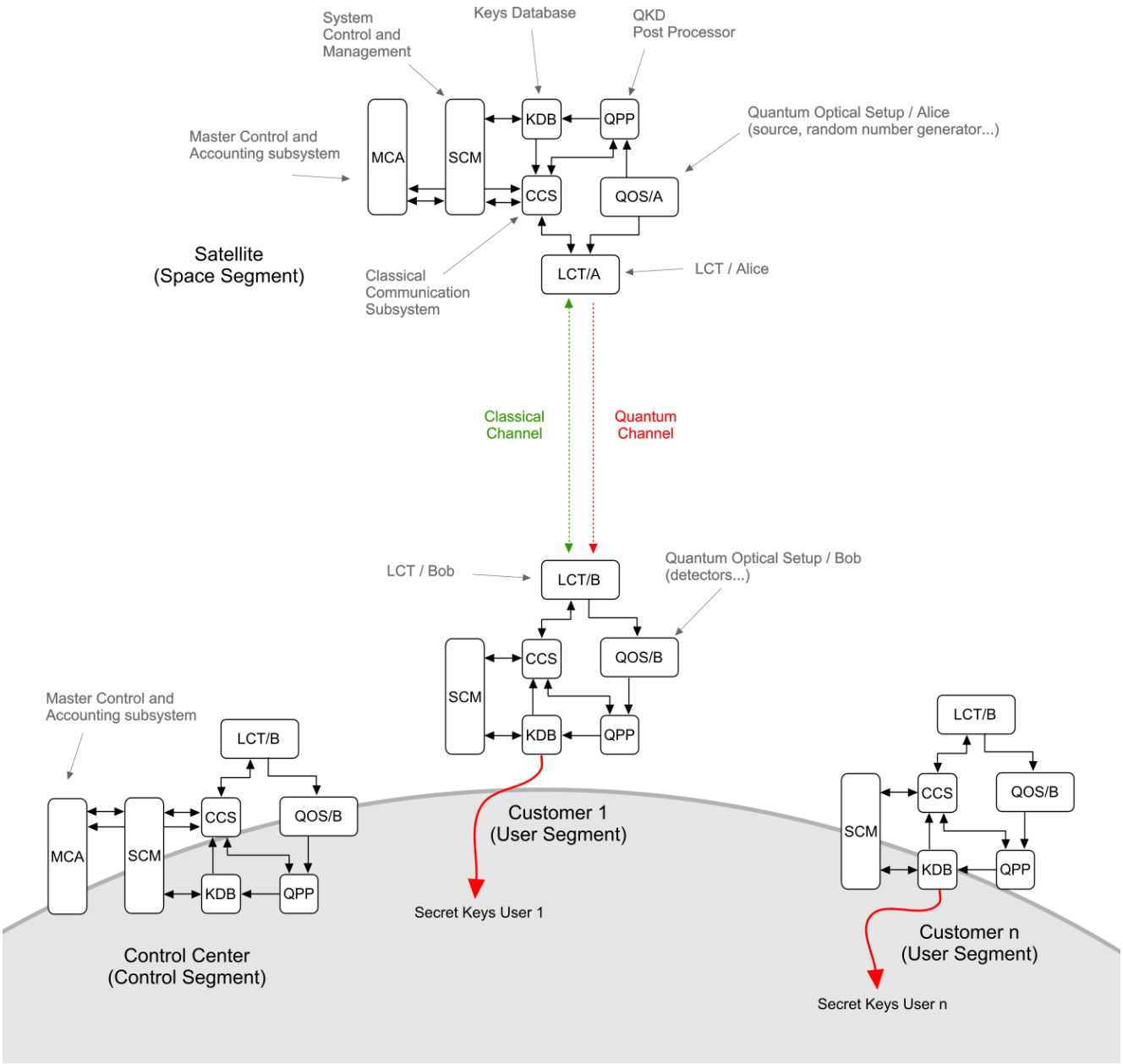

Figure 3. General architecture employed in LEO and GEO architectures.

The SCM consists of:

- a computing platform (CPU, memory, mass storage, operating system)
- the system control and management software

2) CCS – Classical communication subsystem

The CCS handles the classical communication between Alice and Bob.

The CCS consists of:

- a computing platform (CPU, memory, mass storage, operating system) which is shared with the SCM and KDB
- cryptographic algorithms providing information-theoretically secure (ITS) authentication and encryption/decryption functions. These algorithms might run on a computer shared with QPP.
- the classical communication channel subsystem: laser communication is proposed in order to establish the classical communication system. In any case, the quantum communication will need the classical communication functionality at least for spatial acquisition and tracking. The LCTs can be shared between classical and quantum communication by means of time or wavelength division multiplexing. Thus it is proposed to also use this classical channel for authentication and

key distillation functions (such as sifting, error correction and privacy amplification), for which the data are generated by the QPP.

3) KDB – Keys database

In the KDB, the QKD generated keys are temporarily stored on a mass storage until they are used (i.e. encrypted and subsequently distributed to customers, or used for authentication and encryption/decryption on the CCS).

The KDB consists of:

- a computing platform (CPU, memory, mass storage, operating system) which is shared with SCM and CCS
- the KDB management application running on the computer shared with the QPP
- mass storage for the QKD generated keys (optional, if not on the mass storage of the underlying computing platform). The mass memory might be shared with another payload of the spacecraft, e.g. an acquisition instrument of an earth observation satellite.

4) QPP – Quantum post processing subsystem

The QPP is the computing platform for the QKD post processing protocol stack. Here the different stages of the QKD key distillation protocol are executed to generate the final secret key from the raw key (i.e. sent and measured quantum signals).

The QPP consists of:

- a dedicated computing platform (CPU, memory, mass storage, operating system), shared with the KDB
- the post-processing protocol stack, consisting of several chained modules required for the used QKD protocol. In case of the BB84 protocol [41], for example, these steps are: sifting, error correction, privacy amplification. The computer for post-processing might be shared with the CSS.

5) QOS/A – Quantum optical setup Alice side (source, random number generator...), QOS/B – Quantum optical setup Bob side (detectors...)

For the quantum source, there are several design options, depending on the quantum protocol to be performed:

a) Entanglement Source

Up to the present, the most promising candidate of an entangled photon source in space is based on a crossed crystal scheme using two collinear type-0 phase matched PPKTP (periodically poled potassium titanyl phosphate) crystals [42]. This source was developed within ESA's Basic Technology Research Programme (TRP) in the project EQUO (Entangled Photon Source for Quantum Communications, Contract No. AO/1-5942/08/NL/EM). However, as stated before, entanglement protocols are currently not economically viable. Fundamental science missions [43], however, might justify the higher cost.

b) Polarization Prepare & Measure Source

The weak laser pulse source for the polarization decoy protocol was developed within the ESA-ARTES5 project PHT (Photonic Transceiver for Secure Space Communications, Contract No. 21460/08/NL/IA) [44] and relies on a single laser diode followed by four semiconductor optical amplifiers and thin film polarizers, connected through a fiber network.

c) Phase Prepare&Measure Source

The current TESAT LCT configuration is generating two coherent states with a phase difference of 180°. By attenuating these signals and possibly adding some further states, quantum communication can be enabled. In this case, no additional device would be required to turn an LCT into a Q-LCT. The modifications would rather be in on the level of optical parts than on device level.

Furthermore, Prepare&Measure protocols require true, non-deterministic random numbers. Quantum effects actually allow for readily building such a random number generator which delivers true random numbers. One possibility is to split single photons on a 50-50 beam splitter and to register their clicks on both outputs of the beam splitter. Another implementation consists in the homodyne measurement of vacuum noise inherent to coherent states ([45], [46]). It can be easily proven that random numbers from such measurements are non-deterministic. For example, the local oscillator laser used for homodyne detection in TESAT LCTs can be employed to generate the random numbers for quantum state transmission.

6) LCT/A – Quantum LCT space

The TESAT LCT [38], [39], [40], as shown in Figure 2, can be used as LCT/A.

7) LCT/B – Quantum LCT ground

In order to provide the QKD services from chapter III, ground LCTs with apertures of at least 25 cm, 50 cm or 200 cm are required. Here we give some examples of optical ground stations fulfilling these requirements on the aperture size:

- Optical Ground Stations developed by the Institute of Communications and Navigation of the German Aerospace Center (DLR-IKN). Aperture sizes are 40 cm in a fixed [47] and mobile [48] version and 60 cm in a mobile version [49].
- ESA Optical Ground Station (OGS) on Tenerife with 100 cm aperture diameter [50], [51], [52]. The ESA OGS, installed in the Teide observatory, 2400 m above the sea level was built for research of satellite optical communications.
- The Wendelstein Observatory, situated on a height of 1838 m in the Bavarian Alpesand, is operated by the Ludwig Maximilian University of Munich.

Currently, a 200 cm telescope is under construction by Kayser-Threde, Munich, and Astelco Systems, Martinsried [53]. It is assumed that this 200 cm telescope can be used for optical communication.

- MAGIC (Major Atmospheric Gamma-ray Imaging Cherenkov) Telescopes on Tenerife with a diameter of 17 m, consisting of 50 cm x 50 cm Aluminum individual reflectors [54].

8) MCA – Master control and accounting subsystem

The Master control and accounting subsystem (MCA) is distributed between the satellite (space segment) and the control centre (control segment) steering the entire telecommunication network with respects to service requests issued by customers. It schedules the single requests and possibly also optimizes their sequential execution order. It communicates with the system control and management (SCM) components of the single segments. The MCA is also responsible for accounting and billing of the customers.

The MCA consists of:

- a computing platform (CPU, memory, mass storage, operating system)
- the MCA software
- the flight operations team

A. Generic assumptions connected with the proposed architectures

- A similar architecture is employed for the LEO and the GEO variants.
- The quantum channel and the classical channel are multiplexed (time or frequency division) in one LCT.
- The control center is accessed by the satellite as any of the customers.
- The control center too, generates secret keys with the satellite and uses them to secure (authenticate, encrypt) its communication (command and control sequences, access lists for different customers). This communication can also use a radio frequency link and is thus not impacted by atmospheric conditions.
- For security, it is sufficient to authenticate the communication between control center and space segment. However, additionally encrypting this communication will strengthen anti-jamming capabilities since adversaries will not know a priori which stations are scheduled to exchange keys.
- For reasons of redundancy, and for more frequent access to the satellite, the architecture may be extended with additional control centers.
- The key database (KDB) of the satellite is large enough to store the keys until they are delivered to the legitimate customers.
- The KDB may store considerable amounts of cryptographic keys for specific customers as backup for anticipated system unavailability (e.g. due to seasonal weather conditions).

B. Service implementation

The customer books a service agreement at the control center. The service agreement defines an amount of keys which will be made available in the customer's key database during a certain interval of time (e.g. 1 megabit during one week), while the exact instant of time when keys will be arriving is not defined. The master control and accounting subsystem schedules the rendezvous between spacecraft and ground stations.

V. CONCLUSION

We have presented architectures for LEO and GEO based quantum cryptography services. A large variety of users on ground can be provided with keys for secure communication among each other. We highlight that the service fees for the users are very affordable for One-way QKD using Prepare & Measure protocols. We furthermore have detailed the system components required for such space-based quantum communication services. The existing, space-qualified TESAT LCT design can be used to transmit quantum signals from space to ground. In a next step, it has to be investigated which is the optimal way to extend the LCT to a Q-LCT.

[1] N. Gisin, G. Ribordy, W. Tittel, and H. Zbinden, "Quantum cryptography," Rev. Mod. Phys., vol. 74, pp. 145–195, January 2002.

[2] V. Scarani, H. Bechmann-Pasquinucci, N. J. Cerf, M. Dušek, N. Lütkenhaus, and M. Peev, "The security of practical quantum key distribution," Rev. of Mod. Phys., vol. 81, pp. 1301–1350, July–September 2009.

[3] C. Bennett and S. J. Wiesner, "Communication via one- and two-particle operators on Einstein-Podolsky-Rosen states," Phys. Rev. Lett., vol. 69, pp. 2881–2884, November 1992.

[4] C. H. Bennett, G. Brassard, C. Crépeau, R. Jozsa, A. Peres, and W. K. Wootters, "Teleporting an unknown quantum state via dual classical and Einstein-Podolsky-Rosen channels," Phys. Rev. Lett., vol. 70, 1895–1899, March 1993.

[5] M. Nielsen and I. Chuang, Quantum Computation and Quantum Information, Cambridge: Cambridge University Press, 2000.

[6] J. M. Perdigues Armengol, B. Furch, C. J. de Matos, O. Minster, L. Cacciapuoti, M. Pfennigbauer, M. Aspelmeyer, T. Jennewein, R. Ursin, T. Schmitt-Manderbach, G. Baister, J. Rarity, W. Leeb, C. Barbieri, H. Weinfurter, and A. Zeilinger, "Quantum communications at ESA: towards a space experiment on the ISS," Acta Astronaut., vol. 63, p. 165–178, July 2008.

[7] D. Finocchiaro, R. Campo, A. Recchia, A. Le Pera, Th. Länger, M. Peev, D. Elser, F. Heine, S. Seel, Th. Scheidl, R. Ursin, and Z. Sodnik, in preparation.

[8] P. W. Shor, "Algorithms for quantum computation: discrete logarithms and factoring," in Proc. 35th Annual Symposium on Foundations of Computer Science (FOCS), Santa Fe, pp. 124–134, IEEE Computer Society Press, November 1994.

[9] L. M. K. Vandersypen, M. Steffen, G. Breyta, C. S. Yannoni, M. H. Sherwood, and I. L. Chuang, "Experimental realization of Shor's quantum factoring algorithm using nuclear magnetic resonance," Nature, vol. 414, pp. 883–887, December 2001.

[10] A. Politi, J. C. F. Matthews, and J. L. O'Brien, "Shor's quantum factoring algorithm on a photonic chip," Science, vol. 325, p. 1221–1222, September 2009.

[11] C. E. Shannon, "Communication theory of secrecy systems," Bell Syst. Tech. J., vol. 28, pp. 656–715, October 1949.

[12] G. S. Vernam, "Secret signaling system." U. S. patent 1310719, July 1919.

[13] G. S. Vernam, "Cipher printing telegraph systems for secret wire and radio telegraphic communication," J. Am. Inst. Electr. Eng., vol. 45, p. 109–115, January 1926.

[14] V. Scarani and C. Kurtsiefer, "The black paper of quantum cryptography: real implementation problems," arXiv:0906.4547v2 [quant-ph], April 2012, in press.

[15] D. Graham-Rowe, "Photons protect privacy," Nat. Photonics, vol. 2, pp. 62–63, 2008.

[16] Ch. Elliott, A. Colvin, D. Pearson, O. Pikalo, J. Schlafer, and H. Yeh, "Current status of the DARPA quantum network," in Quantum Information and Computation III (E. J. Donkor, A. R. Pirich, and H. E. Brandt, eds.), SPIE Proceedings Vol. 5815, pp.138–393, May 2005.

[17] A. Poppe, A. Fedrizzi, R. Ursin, H. Böhm, T. Lörunser, O. Maurhardt, M. Peev, M. Suda, C. Kurtsiefer, H. Weinfurter, T. Jennewein, and A. Zeilinger, "Practical quantum key distribution with polarization entangled photons," Opt. Express, vol. 12, pp. 3865–3871, August 2004.

[18] P. Marks, "Quantum cryptography to protect Swiss election," NewScientist (15 October 2007).

[19] W. Chen, Zh.-F. Han, T. Zhang, H. Wen, Zh.-Q. Yin, F.-X. Xu, Q.-L. Wu, Y. Liu, Y. Zhang, X.-F. Mo, Y.-Zh. Gui, G. Wei, G.-C. Guo, "Field experiment on a 'star type' metropolitan quantum key distribution network," IEEE Phot. Techn. Lett., vol. 21, pp. 575–577, May 2009.

[20] M. Peev, C. Pacher, R. Alléaume, C. Barreiro, J. Bouda, W. Boxleitner, T. Debuisschert, E. Diamanti, M. Dianati, J. F. Dynes, S. Fasel, S. Fossier, M. Fürst, J.-D. Gautier, O. Gay, N. Gisin, P. Grangier, A. Happe, Y. Hasani, M. Hentschel, H. Hübel, G. Humer, T. Länger, M. Legré, R. Lieger, J. Lodewyck, T. Lorünser, N. Lütkenhaus, A. Marhold, T. Matyus, O. Maurhart, L. Monat, S. Nauerth, J.-B. Page, A. Poppe, E. Querasser, G. Ribordy, S. Robyr, L. Salvail, A. W. Sharpe, A. J. Shields, D. Stucki, M. Suda, C. Tamas, T. Themel, R. T. Thew, Y. Thoma, A. Treiber, P. Trinkler, R. Tualle-Brouri, F. Vannel, N. Walenta, H. Weier, H. Weinfurter, I. Wimberger, Z. L. Yuan, H. Zbinden, and A. Zeilinger, "The SECOQC quantum key distribution network in Vienna," New J. Phys., vol. 11, p. 075001, July 2009.

[21] A. Mirza and F. Petruccione, "Realizing long-term quantum cryptography," J. Opt. Soc. Am. B, vol. 27, pp. A185–A188, May 2010.

[22] M. Sasaki, M. Fujiwara, H. Ishizuka, W. Klaus, K. Wakui, M. Takeoka, A. Tanaka, K. Yoshino, Y. Nambu, S. Takahashi, A. Tajima, A. Tomita, T. Domeki, T. Hasegawa, Y. Sakai, H. Kobayashi, T. Asai, K. Shimizu, T. Tokura, T. Tsurumaru, M. Matsui, T. Honjo, K. Tamaki, H. Takesue, Y. Tokura, J. F. Dynes, A. R. Dixon, A. W. Sharpe, Z. L. Yuan, A. J. Shields, S. Uchikoga, M. Legré, S. Robyr, P. Trinkler, L. Monat, J.-B. Page, G. Ribordy, A. Poppe, A. Allacher, O. Maurhart, T. Länger, M. Peev, and A. Zeilinger, "Field test of quantum key distribution in the Tokyo QKD network," Opt. Express, vol. 19 , pp. 10387–10409, May 2011.

[23] B. C. Jacobs and J. D. Franson, "Quantum cryptography in free space," Opt. Lett., vol. 21, 1854–1856, November 1996.

[24] J. G. Rarity, P. R. Tapster, and P. M. Gorman, "Secure free-space key-exchange to 1.9 km and beyond," J. Mod. Opt., vol. 48, 1887–1901, November 2001.

[25] C. Kurtsiefer, P. Zarda, M. Halder, H. Weinfurter, P. M. Gorman, P. R. Tapster, and J. G. Rarity, "Quantum cryptography: a step towards global key distribution," Nature, vol. 419, p. 450, October 2002.

[26] R. J. Hughes, J. E. Nordholt, D. Derkacs, and Ch. G. Peterson, "Practical free-space quantum key distribution over 10 km in daylight and at night," New J. Phys., vol. 4, p. 43, July 2002.

[27] J. Bienfang, A. Gross, A. Mink, B. Hershman, A. Nakassis, X. Tang, R. Lu, D. Su, Ch. Clark, C. Williams, E. Hagley, and J. Wen, "Quantum key distribution with 1.25 Gbps clock synchronization," Opt. Express, vol. 12, pp. 2011–2016, May 2004.

[28] T. Schmitt-Manderbach, H. Weier, M. Fürst, R. Ursin, F. Tiefenbacher, T. Scheidl, J. Perdigues, Z. Sodnik, C. Kurtsiefer, J. G. Rarity, A. Zeilinger, and H. Weinfurter, "Experimental demonstration of free-space decoy-state quantum key distribution over 144 km," Phys. Rev. Lett., vol. 98, p. 010504, January 2007.

[29] P. Villoresi, T. Jennewein, F. Tamburini, M. Aspelmeyer, C. Bonato, R. Ursin, C. Pernechele, V. Luceri, G. Bianco, A. Zeilinger, and C. Barbieri, "Experimental verification of the feasibility of a quantum channel between space and earth," New J. Phys., vol. 10, p. 033038, March 2008.

[30] D. Elser, T. Bartley, B. Heim, C. Wittmann, D. Sych, and G. Leuchs, "Feasibility of free space quantum key distribution with coherent polarization states," New J. Phys., vol. 11, p. 045014, April 2009.

[31] A. K. Ekert, "Quantum cryptography based on Bell's theorem," Phys. Rev. Lett., vol. 67, pp. 661–663, August 1991.

[32] Ch.-Zh. Peng, T. Yang, X.-H. Bao, J. Zhang, X.-M. Jin, F.-Y. Feng, B. Yang, J. Yang, J. Yin, Q. Zhang, N. Li, B.-L. Tian, and J.-W. Pan, "Experimental free-space distribution of entangled photon pairs over 13 km: towards satellite-based global quantum communication," Phys. Rev. Lett., vol. 94, p. 150501, April 2005.

[33] R. Ursin, F. Tiefenbacher, T. Schmitt-Manderbach, H. Weier, T. Scheidl, M. Lindenthal, B. Blauensteiner, T. Jennewein, J. Perdigues, P. Trojek, B. Ömer, M. Fürst, M. Meyenburg, J. Rarity, Z. Sodnik, C. Barbieri, H. Weinfurter, and A. Zeilinger, "Entanglement-based quantum communication over 144 km," Nat. Phys., vol. 3, p. 481–486, June 2007.

[34] A. Ling, M. P. Peloso, I. Marcikic, V. Scarani, A. Lamas-Linares, and Ch. Kurtsiefer, "Experimental quantum key distribution based on a Bell test," Phys. Rev. A, vol. 78, p. 020301(R), August 2008.

[35] C. Erven, C. Couteau, R. Laflamme, and G. Weihs, "Entangled quantum key distribution over two free-space optical links," Opt. Express, vol. 16, pp. 16840–16853, October 2008.

[36] A. Fedrizzi, R. Ursin, T. Herbst, M. Nespoli, R. Prevedel, T. Scheidl, F. Tiefenbacher, T. Jennewein, and A. Zeilinger, "High-fidelity transmission of entanglement over a high-loss free-space channel," Nat. Phys., vol. 5, p. 389–392, May 2009.

[37] T. Scheidl, R. Ursin, A. Fedrizzi, S. Ramelow, X.-S. Ma, T. Herbst, R. Prevedel, L. Ratschbacher, J. Kofler, T. Jennewein, and A. Zeilinger, "Feasibility of 300 km quantum key distribution with entangled states," New J. Phys., vol. 11, p. 085002, August 2009.

[38] M. Gregory, F. Heine, H. Kämpfner, R. Lange, M. Lutzer, and R. Meyer, "Commercial optical inter-satellite communication at high data rates," Opt. Eng., vol. 51, p. 031202, March 2012.

[39] R. Fields, D. Kozlowski, H. Yura, R. Wong, J. Wicker, C. Lunde, M. Gregory, B. Wandernoth, and F. Heine, "5.625 Gbps bidirectional laser communications measurements between the NFIRE satellite and an Optical Ground Station," International Conference on Space Optical Systems and Applications (ICSOS) , pp. 44–53, May 2011.

[40] F. Heine, H. Kämpfner, P. Greulich, S. Seel, "Coherent detection of low light level pulses," International Conference on Space Optical Systems and Applications (ICSOS), pp. 288–291, May 2011.

[41] C. H. Bennett and G. Brassard, "Quantum cryptography: public key distribution and coin tossing", in Proceedings of the IEEE International Conference on Computers, Systems, and Signal Processing, Bangalore, pp. 175–179, December 1984.

[42] F. Steinlechner, P. Trojek, M. Jofre, H. Weier, D. Perez, Th. Jennewein, R. Ursin, J. Rarity, M. W. Mitchell, J. P. Torres, H. Weinfurter, and V. Pruneri, "A high-brightness source of polarization-entangled photons optimized for applications in free space," Opt. Express, vol. 20, pp. 9640–9649, April 2012.

[43] R. Ursin, T. Jennewein, J. Kofler, J. M. Perdigues, L. Cacciapuoti, C. J. de Matos, M. Aspelmeyer, A. Valencia, T. Scheidl, A. Acín, C. Barbieri, G. Bianco, C. Brukner, J. Capmany, S. Cova, D. Giggenbach, W. Leeb, R. H. Hadfield, R. Laflamme, N. Lütkenhaus, G. Milburn, M. Peev, T. Ralph, J. Rarity, R. Renner, E. Samain, N. Solomos, W. Tittel, J. P. Torres, M. Toyoshima, A. Ortigosa-Blanch, V. Pruneri, P. Villoresi, I. Walmsley, G. Weihs, H. Weinfurter, M. Zukowski, A. Zeilinger, "Space-quest, experiments with quantum entanglement in space", Europhysics News, vol. 40, pp. 26–29, June 2009.

[44] M. Jofre, A. Gardelein, G. Anzolin, W. Amaya, J. Capmany, R. Ursin, L. Penate, D. Lopez, J. L. San Juan, J. A. Carrasco, F. Garcia,

F. J. Torcal-Milla, L. M. Sanchez-Brea, E. Bernabeu, J. M. Perdigues, T. Jennewein, J. P. Torres, M. W. Mitchell, and V. Pruneri , "Fast optical source for quantum key distribution based on semiconductor optical amplifiers," Opt. Express, vol. 19, pp. 3825–3834, February 2011.

[45] Ch. Gabriel, Ch. Wittmann, D. Sych, R.-F. Dong, W. Mauerer, U. L. Andersen, Ch. Marquardt, and G. Leuchs, "A generator for unique quantum random numbers based on vacuum states," Nat. Photonics, vol. 4, pp. 711–715, August 2010.

[46] T. Symul, S. M. Assad, and P. K. Lam, "Real time demonstration of high bitrate quantum random number generation with coherent laser light," Appl. Phys. Lett., vol. 98, p. 231103, June 2011.

[47] N. Perlot, M. Knapek, D. Giggenbach, J. Horwath, M. Brechtelsbauer, Y. Takayama, J. Yoshihisa, and T. Jono, "Results of the optical downlink experiment KIODO from OICETS satellite to optical ground station Oberpfaffenhofen (OGS-OP)," Proc. SPIE, vol. 6457, p. 645704, February 2007.

[48] J. Horwath, and Ch. Fuchs, "Aircraft to ground unidirectional laser-comm. terminal for high resolution sensors," Proc. SPIE, vol. 7199, p. 719909, January 2009.

[49] Ch. Fuchs, D. Giggenbach, and M. Brechtelsbauer, "Verification of ground station diversity for direct optical TTC-downlinks from LEO satellites by means of an experimental laser source," 5th ESA Workshop on Tracking, Telemetry and Command Systems for Space Applications, Nordwijk, The Netherlands, 21.-23. September 2010.

[50] M. Pfennigbauer, W. Leeb, G. Neckamm, M. Aspelmeyer, Th. Jennewein, F. Tiefenbacher, A. Zeilinger, G. Baister, H. J. Egli, K. Kudielka, Th. Dreischer, and H. Weinfurter, "Accomodation of a Quantum Communication Transceiver in an Optical Terminal ('ACCOM')," Executive Summary Report prepared for the European Space Agency under ESTEC/Contract No. 17766/03/NL/PM, ESTEC Technical Management: J. M. Perdigues (TOS-MMO), January 2005. http://esamultimedia.esa.int/docs/gsp/completed/C17766ExS.pdf

[51] H. Weinfurter, T. Schmitt-Manderbach, H. Weier, M. Fürst, P. Trojek, A. Zeilinger, M. Aspelmeyer, R. Ursin, Th. Jennewein, F. Tiefenbacher, Th. Scheidl, A. Fedrizzi, J. Rarity, D. Benton, P. Gorman, D. Taylor, P. Tapster, C. Barbieri, F. Tamburini, P. Villoresi, I. Capraro, T. Occhipinti, G. Bianco, F. Heine, G. Baister, and G. P. Guizzo, "Quantum Information and Quantum Physics in Space: Experimental Evaluation ('QIPS'), Executive Summary prepared for the European Space Agency under ESTEC/Contract No.18805/04/NL/HE, ESA Study Manager: J. M. Perdigués Armengol (TEC-MMO) October 2007. http://esamultimedia.esa.int/docs/gsp/completed/C18805ExS.pdf

[52] Th. Berkefeld, D. Soltau, R. Czichy, E. Fischer, B. Wandernoth, and Z. Sonik, "Adaptive optics for satellite-to-ground laser communication at the 1 m telescope of the ESA optical ground station, Tenerife, Spain," Proc. SPIE, vol. 7736, p. 77364C, June 2010.

[53] http://www.wendelstein-observatorium.de:8002/wst_en.html

[54] J. Albert et al. (MAGIC Collaboration), "Very-high-energy gamma rays from a distant quasar: How transparent is the universe?", Science, vol. 320, pp. 1752–1754, June 2008.