DISCRETION: Quantum Secure Communications for European Defence

Catarina Bastos
Deimos Engenharia,
Av. Columbano Bordalo Pinheiro, N. 75, Piso 9 A1, 1070-061, Lisboa
PORTUGAL

catarina.bastos@deimos.com.pt

ABSTRACT

In a military context, information and communications services are of central importance in a variety of operational and strategic scenarios. These services rely on secure, reliable, often heterogeneous, and segregated infrastructure. Clearly, vulnerabilities in the cryptosystem or the communication channel supporting them can compromise the entire network and at all levels, causing large institutional and material losses. The advent of quantum technologies, and more particularly quantum computing, has raised new security threats that can potentially affect most of the existing security cryptosystems. In this context, Quantum Key Distribution (QKD), which is based on the fundamental laws of physics, appears as a credible solution to face the threat of quantum computers. Indeed, QKD is an example of what is known as an Information Theoretic Secure primitive, immune to any computational attack, no matter the power of the adversary. However, QKD is fairly limited in range and flexibility, usually relying on point-to-point connections, rigid physical infrastructures and often even requiring dedicated fibres. It also requires specialized photonic components, different from those used in traditional optical networks.

The integration of QKD technologies in a network becomes easier when considering a Software Defined Networking (SDN) paradigm. SDN allows for increased network scalability, flexibility, agility, and manageability. These properties are very desirable in dynamic environments, and SDN can extend its benefits to interface with Software Defined Radio (SDR) networks. In addition, the software-defined nature of SDN enables the vital permanent evolution of mechanisms that guarantee network resilience and robustness. The adoption of SDN technology opens the possibility to a flexible QKD network, where QKD provides a very secure way to distribute cryptographic keys to different points. SDN and QKD thus provide mutual benefits in a symbiotic approach: SDN enables a flexible QKD network, with control and monitoring capabilities, and QKD enables highly secure communications within the SDN.

DISCRETION shall develop an SDN solution that integrates QKD capabilities to support optical secure communications, in a way that European Defence can benefit from the security and resilience that these technologies bring to the networks, not only for network situational awareness but also for cyber situational awareness. The challenge of DISCRETION is to implement and integrate these disruptive technologies into military and Defence communication infrastructure, considering the red-black separation architecture of military networks. Encryption of information between red and black blocks of the network shall be done using cipher machines prepared to use keys generated with QKD systems integrated with SDN and a key management service (KMS) developed in DISCRETION. DISCRETION explores the use of Continuous-Variables (CV) QKD technology, which is currently regarded as one of the main building blocks for a large-scale deployment of quantum cryptography, as it facilitates coexistence with traditional optical networks, using classical photonics platforms. It presents a set of features, like flexibility, higher key rates, and software controllable, showing the feasibility of more seamless integration into DISCRETION's SDN. For tactical scenarios, SDR solutions shall be analyzed and integrated into the SDN solution to cover radio network segments and support secure communication services.

1.0 INTRODUCTION

Currently, a technological revolution is emerging, that is changing the field of cryptography. All over the world, companies and governments are heavily investing resources into Quantum Computing. Quantum Computers use a different logic than classical computers, which enables them to solve some traditionally hard computational problems in a reasonable timeframe. These include the mathematical problems which are the foundation for currently used Asymmetric Cryptography and established protocols, such as TLS. Some of the quantum algorithms that address this have been known for nearly 30 years, such as the Shor algorithm [1]. Specific methods and approaches dedicated to breaking encryption algorithms have also been studied and optimized over the years, and it is expected that quantum computers will be capable of breaking current asymmetric encryption standards within the next 15 years [2]. Another threat is the attacker scheme commonly known as ***store now, decrypt later*** or ***harvest attacks,*** where an attacker collects encrypted data to decrypt it in the future, when technological breakthroughs allow it. While most of it should be reasonably protected by current standards, it could still be decrypted later, when the technology allows it. It could compromise the secrecy of information even in areas where data remains sensitive for long periods of time, such as military, government and genetics. Thus, for the Post-Quantum Era, it is necessary to adopt alternative cryptographic tools which are not susceptible to being attacked with either Classical or Quantum Computers in the future. There are two main branches of new cryptographic algorithms and protocols: *Classical Post-Quantum Cryptography [3]*, that is based on the same type of mathematical hard assumptions of Classical Cryptography, but uses computational problems believed to be hard to solve even by a large Quantum Computer, and *Quantum Cryptography* [4], [5], [6], that takes advantage of quantum mechanics and laws of physics to ensure information security independently of an adversary's computational power. On one hand, classical Post-Quantum Cryptography is easier and cheaper to deploy, and may be the best solution for some cases, particularly for small and mobile devices, but the newly proposed algorithms will require continuous evaluation, updates and replacements as time goes by. On the other hand, Quantum Key Distribution (QKD) protocols provide stronger and long-lived security assurances, but need dedicated systems with physical limitations, being more useful for applications in critical sectors that require strong and lasting security, such as military, or government infrastructures.

DISCRETION aims at integrating and combining SDN and QKD technologies on top of legacy optical networks to build a highly secure, scalable, and resilient network control architecture for defence networks and advanced tactical operation services. This SDN shall have a highly available centralized control, and the security of the network should increase through the integration with QKD technologies. Current QKD devices suffer from a series of limitations regarding management, control, scalability, and interoperability. Although there is a plethora of experimental devices based on different design principles, technologies, and using different key delivery interfaces, the final objective is the same: delivering a key in a distributed way over a path of nodes, using quantum technologies for key generation in each hop's link. This is done using secure key forwarding techniques in the KMS layer where this forwarding must not use any algorithm that compromises the Information Theoretical Security (ITS) of the quantum forwarded key. The flexibility of SDN opens the possibility of integrating into the network potentially disruptive technologies like Quantum Key Distribution (QKD). SDN relies on simple key ideas: separation of control and data plane, centralization of network policies and programmability of the networks. They are more agile, flexible, and easier to manage, meaning that new services and general devices can be deployed much faster than with the old networks. **DISCRETION proposes a quantum-enabled SDN architecture and will demonstrate that it unites under the same management the quantum and classical communications, enabling network optimization to better use all resources**.

2.0 RATIONALE

DISCRETION solution is based on the **mutual beneficial relationship between QKD and SDN**. On the one hand, QKD provides a continuous flow of keys whose security cannot be compromised by computationally breaking an algorithm. This provides a physical security plane to the SDN network that can benefit from the QKD keys to protect its control as well as data flows. Not only are the user's communications protected, but also the network itself can be made more robust by using QKD together with carefully chosen architectures. On the other hand, the SDN network allows with its flexibility the integration of QKD technologies in a network, a feature much more complex and costly with past networking paradigms. Early testing of these ideas has been already performed and deployed in production facilities to demonstrate how to harden the telecommunications network as a critical infrastructure and how to provide new, high security services, like in MadridQCI [7].

Some of these concepts were already used in European projects like CIVIQ [8] that showed the flexibility of SDN integrating quantum communication technologies, and in particular Continuous-Variable QKD (CV-QKD), into emerging optical telecommunication networks. However, DISCRETION must consider the Red–Black network separation paradigm [9] typical of defence networks, with the different trade-offs between programmability and reconfigurability; any required exchange of information between red and black network control systems has a potential implication in terms of security, including security requirements of the different interfaces between network planes. Isolation mechanisms will be provided to the SDN applications in the service plane that enable a sufficient degree of programmability while preserving required security for the red network management system. ALTO protocol [10] or unidirectional communication gateways are potential alternatives to achieve this goal. Finally, the Cipher Machines (CMs), developed in the project, are the components responsible for assuring data segregation between red-black networks in DISCRETION, serving as an interface between user plane overlay (red network) and underlying non-secure infrastructure (black network). It will provide real-time data encryption and decryption, and using embedded pre-shared keys provide quantum key distribution authentication. The data encryption is performed using both classical symmetrical keys, distributed identically to existing NATO key distribution approaches, and the proposed quantum distributed keys, when available.

3.0 DESCRIPTION:

DISCRETION offers a **multiplane SDN enabled QKD-based solution that is unified, secure, resilient, robust, and scalable** (see Figure 1). For the full solution it is required not only the integration of each software components but also the integration of specific hardware developed inside the project, such as the QKD Devices and CMs, in a unified ecosystem specifically designed for military environments. Radio communications have also special relevancy due to the inherent mobility of vehicles and military troops. Thus, DISCRETION SDN solution will support the control of the radio network segment as well, integrating with SDR equipment and extending the SDN control scope to programmable radio resource management.

The protocol proposed for the QKD nodes being developed in the DISCRETION project is a CV-QKD Prepare-and-Measure Discrete Modulation protocol. It envisions the usage of quantum states prepared according to a finite-sized constellation. CV-QKD allows using homodyne or heterodyne detection. These detectors are usually cheaper, available off-the-shelf and able to produce faster output rates than the single-photon counters commonly used in DV-QKD systems. In addition, the produced quantum states for CV-QKD protocols do not need to be single-photons, but rather weak coherent laser pulses, which are much easier to produce. These systems are usually able to achieve high secret key rates over distances of a few tens of kilometres, being more suitable for deployments in metropolitan networks. To extend the range of those single links and allow multiple points to communicate, multiple QKD links are connected to form a QKD network. The quantum key management layer above the QKD layer then distributes the generated keys in the network with the help of the SDN layer.

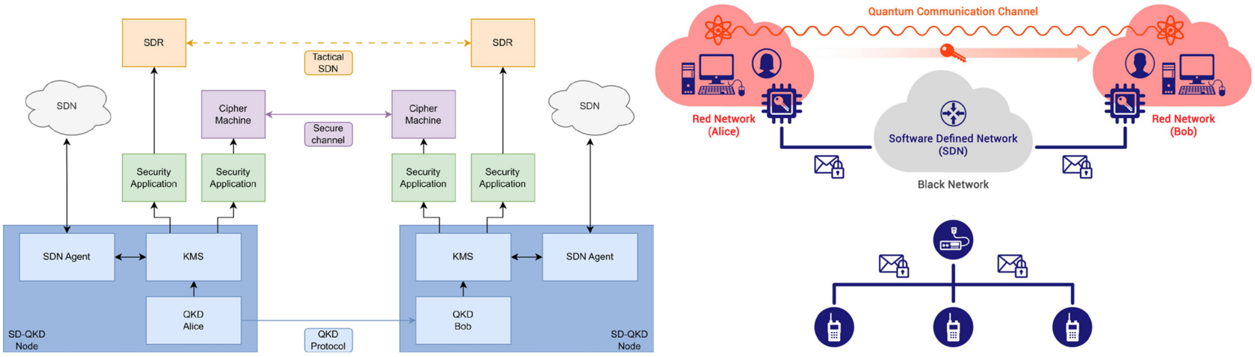

Figure 1: Block Diagram of all DISCRETION elements and high-level architecture.

A Software Defined QKD (SD-QKD) Node shall be assembled by a set of hardware and software components that cooperate to establish ITS communications. The SDN agent shall connect to the QKD modules through the southbound interfaces. The northbound interface will connect to the SDN controller following the most convenient structure to ensure robust and resilient communication. The SDN agent shall also communicate with the key management to adjust the parameters of the QKD module to the key requests required by the applications. Between the SD-QKD Node and the CMs, there will be a security application that is responsible to manage the loading of both quantum keys and classical keys into the CMs. Due to the design of the CM as a passive component, it cannot actively pull the keys. As such, this application interacts with the KMS at each endpoint of the communication to obtain keys and with the applications at the other communications endpoints to get classical keys.

Finally, a crucial step on the integration of all the technology developed under DISCRETION is the correct selection of robust protocols and well-defined standards and interfaces. That will define how the components communicate each other, intra-node, and extra-node. In this regard, the standards proposed by the European Telecommunications Standards Institute (ETSI) play a crucial role in the DISCRETION project, adopting the proposal defined by ETSI GS QKD 015 as Control Interface for Software Defined Networks. Another crucial standard will be the ETSI GS QKD 004, an Application Interface for the key delivery process, that will be used not only to deliver keys to the application layer but also to feed the Cipher Machine to protect all the DISCRETION infrastructure. Furthermore, the study of standards for further security certification of the different components was already started and the goal in this case is to identify the necessary requirements to allow the technology to be compliant with military grade networks.

3.1 Use Cases and Scenarios

DISCRETION is based on different scenarios which range from securing the connection between important static locations, to tactical situations where the proposed technologies can enhance communication security and network capabilities. First, it considers that the connections between national governmental sites and military buildings are of strategic importance, as well as their connections with Information services data centres. They are usually connected by classical networks, which often use redundant topologies. DISCRETION' SDN will increase robustness against failures, disasters, and cyber-attacks. The addition of QKD to the network under the SDN control helps securing these connections and the SDN itself. DISCRETION also considers the operational level data centres since they are the point of contact for mobile tactical networks, enabling tactical access to low latency computing functions and processing of heavy volumes of data. As Operational Data Centres make the connection with tactical contexts, the SDN enabled QKD-based solution can provide new advantages in network control and distribution of pre-shared keys. Moreover, DISCRETION, also addresses tactical communications in mobile and dynamic environments, exploring the possibility of using an SDN approach to interface with Software Defined Radio. While QKD is not yet mature enough to be reliably deployed in these dynamic environments, communication security between tactical units is ensured by previously orchestrating the delivery of pre-shared keys. Finally, DISCRETION proposes the extension of encrypted communications to international level domains, by extending national networks to support increased geographical coverage, including synergies with traditional encryption algorithms.

These scenarios helped defining the possible use cases with the participation of the member states, constraints, and requirements, providing a clearer picture of target objectives in terms of functionality and necessary conditions. This was the main objective of the 1st phase of the project, during 2022. The three use cases defined to demonstrate the capabilities of DISCRETION are the following:

- Use Case A, where two users want to create a secure encrypted connection between them over the internet;
- Use Case B builds up in the first use case, extending it to a scenario where users must connect to a central enterprise location. The enterprise location can have a finite number of connections in a star topology;
- Use Case C addresses a secure connection between two sites with Enterprise infrastructure. The central improvement mentioned by this use case is the availability of "automatic" key management between the sites, to provide crypto-agility for secure communications.

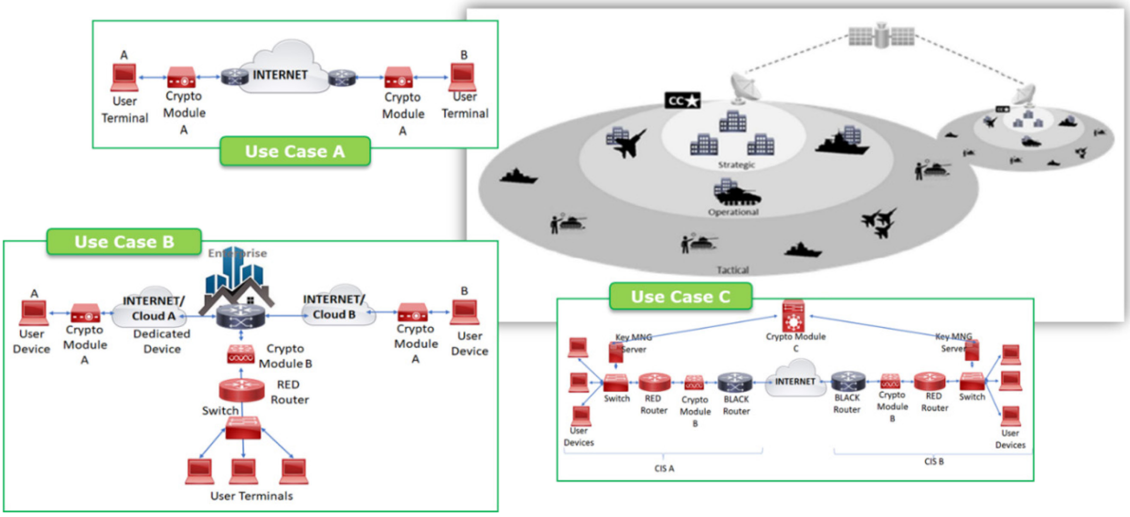

Figure 2: DISCRETION scenarios and use cases.

This year, having the requirements and the different use cases defined, the design of the system could then be defined (see Figure 1).

4.0 CONCLUSIONS

DISCRETION provides **technological, strategic and operational advantages** over the existing technologies. In last few years, European Defence, identified an increasing risk of communication networks disruption through cyber-attacks. In this sense, DISCRETION's expected outcome is a centralized, robust and resilient SDN that is enabled by a QKD physical plane to make it even more robust against cyber-attacks. Although there are already point-to-point QKD technologies in the market, solutions for integrating and controlling QKD links/networks into existing optical communications networks are currently key challenges in this field of optical research. At the same time, the implementation phase of an European quantum communication infrastructure started, EuroQCI [11], and all the member states are building their own networks using most them these technologies developed in DISCRETION. Implementing an SDN enabled by QKD into a military network is then the challenge to cope here, with the security requirements and separation of networks (red-black architecture). DISCRETION addresses several ground-breaking and novel approaches envisioning the integration of QKD in the proposed optical SDN solution for communications in European Defence. The project has a duration of 42 months and should be finished in June 2025.

Finally, it should be noted that DISCRETION paves the way to address more complex challenges in the future, such as scenarios where mobility or big distances are unavoidable (such as scenarios of international crisis situations). This will include integration with **space-based communications** (in a follow up of the project) which is also a Capability Develop Plan (CDP) priority. It should be remarked that in the EuroQCI, a space component is being developed under ESA. It is expected to have QKD-capable satellites for long-distance communications in the not-so-distant future, supporting the idea of a follow up of DISCRETION using this type of communication, for the Defence purposes.

5.0 REFERENCES

[1] P. Shor, "Algorithms for Quantum Computation: Discrete Logarithms and Factoring", 1994.

[2] M. Mosca, and M. Piani, "2021 Quantum Threat Timeline Report", 2021.

[3] D. J. Bernstein, J. Buchmann, E. Dahmen, Eds., "Post-Quantum Cryptography", 1st Edition, 2009.

[4] N. Gisin et al, "Quantum Cryptography", 2002;

[5] S. Pirandola, "Advances in Quantum Cryptography", 2020;

[6] F. Grasselli, "Quantum Cryptography: From Key Distribution to Conference Key Agreement", 1st Edition, 2021.

[7] A. Aguado, V. Lopez, D. Lopez, M. Peev, A. Poppe, A. Pastor, J. Folgueira, V. Martin "The Engineering of a SDN Quantum Key Distribution Network" IEEE Comms. Mag. July 2019, Special number "The Future of Internet" doi: 10.1109/MCOM.2019.1800763;

[8] CIVIQ: https://civiquantum.eu/about-civiq/

[9] NIST, "Computer Security Resource Center - Glossary," 2015. [Online]. Available: https://csrc.nist.gov/glossary/term/RED_BLACK_concept.

[10] L. Contreras, "Considering ALTO as IETF Network Exposure Function - draft-contreras-alto-ietf-nef-01", 2023.

[11] euroQCI: https://digital-strategy.ec.europa.eu/en/policies/european-quantum-communication-infrastructure-euroqci