Aliro SECURITY™

# Integrating Entanglement-based Advanced Secure Networks with Classical Networks

Aliro Security

www.alirosecurity.com

# Integrating Entanglement-based Advanced Secure Networks with Classical Networks

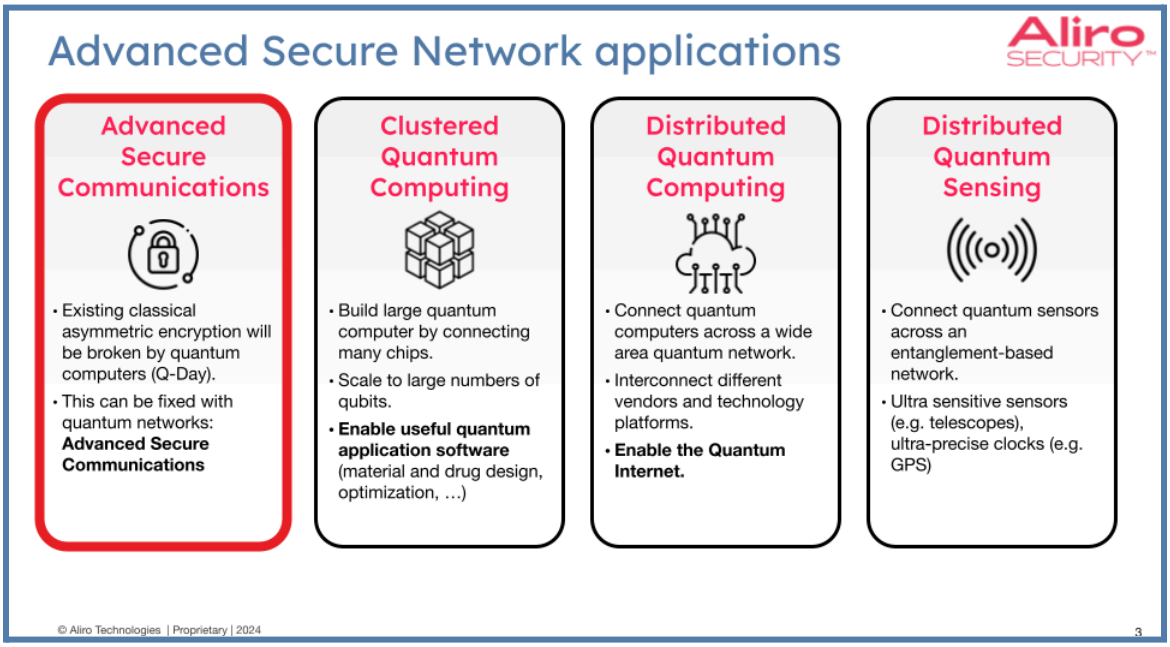
## What is an entanglement-based network?

The term classical network is typically used to refer to types of traditional networks that are not entanglement-based networks. This includes local area networks, WiFi networks, cellular networks, optical fiber networks, satellite networks, the Internet - likely every network you have ever used. Classical networks send classical bits: ones and zeroes. These ones and zeroes are typically encoded as strong optical pulses that are sent through optical fibers, digital signals across copper wires, or strong radio pulses sent through the air.

Entanglement-based networks communicate using qubits. Qubits have special properties described by the laws of physics. There are many properties that are leveraged by entanglement-based technologies - including superposition, entanglement, Heisenberg's uncertainty principle, the no-cloning theorem, and many others. These properties allow entanglement-based networks to do things that are impossible to accomplish with classical networks.

## Entanglement-based network applications

Entanglement-based networks can be used for a variety of applications: clustered quantum computing, distributed quantum computing, distributed quantum sensing, and Advanced Secure Communications.




The most well-known application of entanglement-based Advanced Secure Networks is Advanced Secure Communications, and this use case is the focus throughout this white paper. Advanced Secure Communication addresses the problem posed by Q-Day, in which existing encryption protocols such as RSA and Diffie Hellman will be broken by quantum computers capable of implementing Shor's algorithm. Advanced Secure Communication refers to the entanglement-based successor to Quantum Key Distribution (QKD) that addresses the weaknesses of QKD.

Advanced Secure Communication uses entanglement-based protocols such as E91 and BBM92 that have been studied for many decades, are well understood, and that have security proofs. However, instead of using unsecure trusted relay nodes as QKD does, Advanced Secure Communication uses secure entanglement-based repeaters. Once an entanglement-based network makes use of entanglement-based repeaters, it becomes a general-purpose entanglement-based network, capable of running other applications on the same entanglement-based network, including the other use cases mentioned above.

## Today's entanglement-based Advanced Secure Network requirements

While entanglement-based Advanced Secure Networks enable new applications, they also have particular boundary  requirements today. Most of these requirements are due to the fact that these networks use extremely weak light pulses - typically single photons.

The range of entanglement-based network point-to-point links is limited. The exact limit varies, but 100 kilometers is a typical maximum distance. Beyond 100 kilometers you need trusted relay nodes, entanglement-based repeaters, or satellites to extend the distance between points. This will be addressed as entanglement-based repeaters become commercially available.

The second requirement is that the throughput of an entanglement-based network in qubits per second is low. Once again, the exact limit varies, but one million usable qubits per second is typical for short links. As the distance approaches the maximum of 100 kilometers, the throughput decreases down to a few thousand qubits per second. This will be addressed as hardware devices become capable of producing higher qubit throughput.

The third requirement is that the links in an entanglement-based network must be either optical fiber connections or point-to-point free-space laser connections. Those free-space connections can be terrestrial, or they can be a satellite. As newer hardware technologies evolve this requirement may be mitigated.

In some ways, entanglement-based networking is a technology that is quite mature. It is actually more mature than quantum computing. Several companies have been offering commercial QKD products for over 10 years now, and these products have been deployed in operational networks. The components required for the next generation of general-purpose entanglement-based Advanced Secure Networks are just now being commercialized. This includes hardware like quantum memories, transducers, and entanglement-based repeaters. The range, speed, and cost of entanglement-based networks will improve over time as a result of further innovations into multi-mode memories, error correction, integrated photonics, and other technologies.

## Entanglement-based networks augment classical networks

One of the questions Aliro is frequently asked is, "Will entanglement-based networks replace classical networks?”

The answer is no. We may never watch Netflix or do a Zoom call over an entanglement-based network. Instead, entanglement-based networks will be used in conjunction with classical networks. We can understand this better by looking at what happened with the development of classical computers. Classical computers have been using co-processors to perform specialized tasks for a long time already.

- Graphical processing units, or GPUs, are used to offload graphics rendering.
- Tensor processing units, or TPUs, are used to offload machine learning.
- Data processing units, or DPUs, are used to offload networking tasks.

These GPUs, TPUs, and DPUs do not replace the general-purpose CPUs; instead, they augment CPUs by off-loading very specific, specialized tasks.

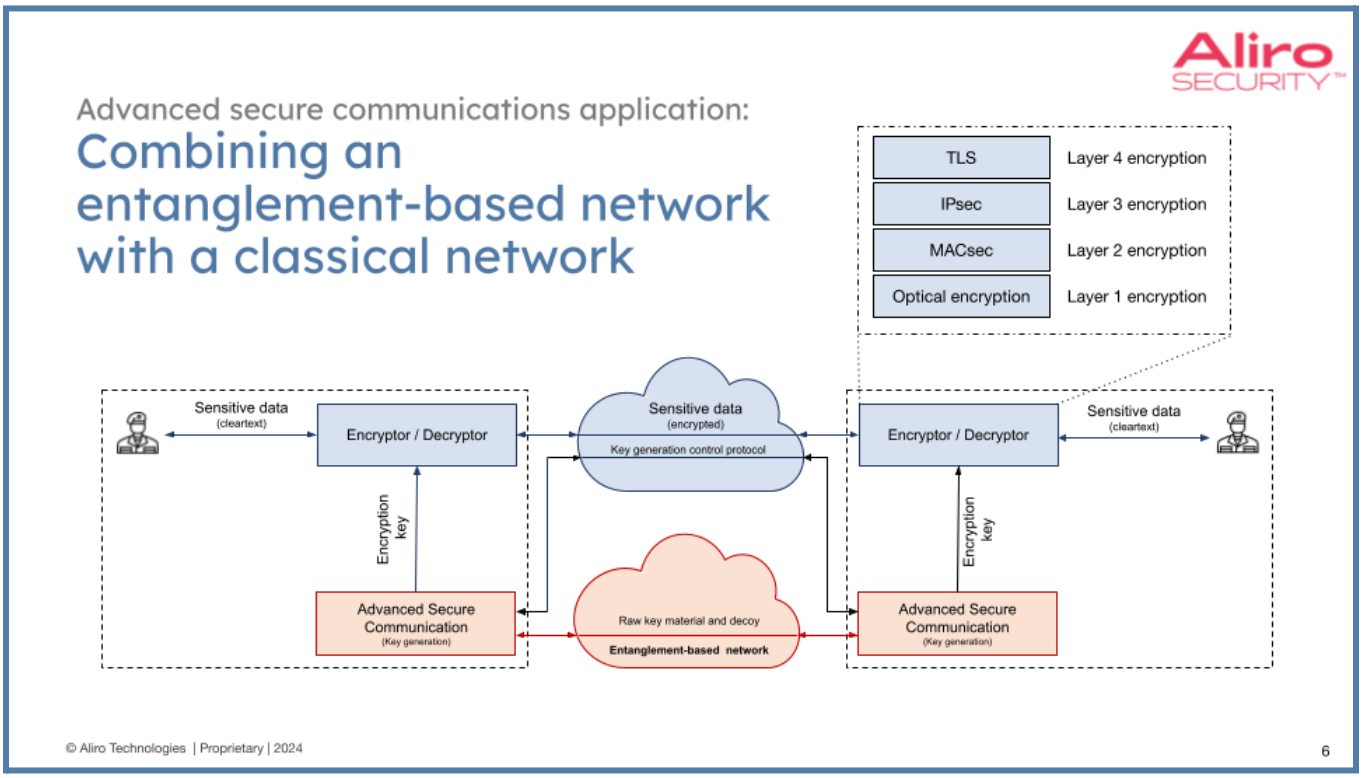
Similarly, quantum processing units, or QPUs, will not replace classical computers. Just like GPUs, TPUs, and DPUs, quantum processing units will be used to offload very specific tasks that quantum computers are good at. This includes things like drug design, material design, optimization, simulation, and cryptanalysis.

Although quantum computers are much better at certain tasks than classical computers, there are plenty of tasks that quantum computers are just not suitable for. No one would dream of using a quantum computer to edit an Excel spreadsheet or play a video game. Hence, quantum computers will never fully replace classical computers.

The same is true for entanglement-based networks. Entanglement-based networks are not intended to replace classical networks. Instead, entanglement-based networks will augment classical networks. There are some specific applications that entanglement-based networks are exceptional at, including secure communications and connecting entanglement computers or entanglement sensors to each other. Entanglement-based networks are not just better at these applications; some of these applications are simply not possible on classical networks. For example, a clustered quantum computer data center cannot be created using a classical network. It is only possible with an entanglement-based network because it must transfer qubits, which is not possible on a classical network.

## Combining an entanglement-based network with a classical network

Here is a concrete example of how a classical network and an entanglement-based network work together.




We'll focus on the Advanced Secure Communications use case throughout this white paper, as it is the application that is the furthest developed. Similar diagrams could be drawn for clustered and distributed quantum computing and sensing.

At the top, in blue, is the classical network. There are two parties that want to exchange encrypted data over this classical network. Many companies including Cisco, Juniper, Fortinet, and many others offer the hardware encryption devices that do encryption at various layers in the networking stack. The bulk encryption of the data can take place at multiple gigabits or even terabits per second and uses symmetrical encryption protocols such as the advanced encryption standard: AES.

The symmetrical encryption protocols need both parties to agree on a session encryption key. In today's networks, this is typically implemented using asymmetrical encryption protocols such as RSA, Diffie Helman, or Elliptic Curve Diffie Helman. These existing session key establishment protocols are expected to be broken by quantum computers through the implementation of Shor's algorithm and need to be replaced by a new key establishment protocol which will be safe against attack by quantum computers. This is what we mean when we use the terms Advanced Secure Communications and post-entanglement security. For an in-depth look at the threats and impacts of

Q-Day (the day a quantum computer is capable of running Shor's algorithm) see the on-demand webinar **What is Q-Day**.

One possible way to implement advanced secure key establishment is to use an entanglement-based network. In this diagram, the entanglement-based network is shown in red at the bottom. The entanglement-based network uses the special properties of physics to establish an encryption key between the two parties in a secure manner. The basic principle behind this security is that the laws of physics guarantee that it is impossible to steal the key without being detected. Thus, the term physics-based security is sometimes used for this approach.

There are two important things to notice in this diagram. The first observation is that the entanglement-based network is not responsible for high-speed bulk data encryption at multiple gigabits per second. The high-speed bulk encryption still happens on the classical side of the network. The entanglement-based network is only responsible for producing the encryption key. Even if you roll over the encryption key very frequently, the entanglement-based network is typically more than fast enough to produce the necessary session encryption keys. The entanglement-based network hands over the encryption keys to the classical encryptors using a well-defined interface.

The second observation is that the entanglement-based network does not replace the classical network. We do not need a forklift upgrade of the classical equipment. The entanglement-based network only augments the classical network to offload a specific function, namely encryption key establishment in this case.

## Layers of network integration between entanglement-based Advanced Secure Networks and classical networks

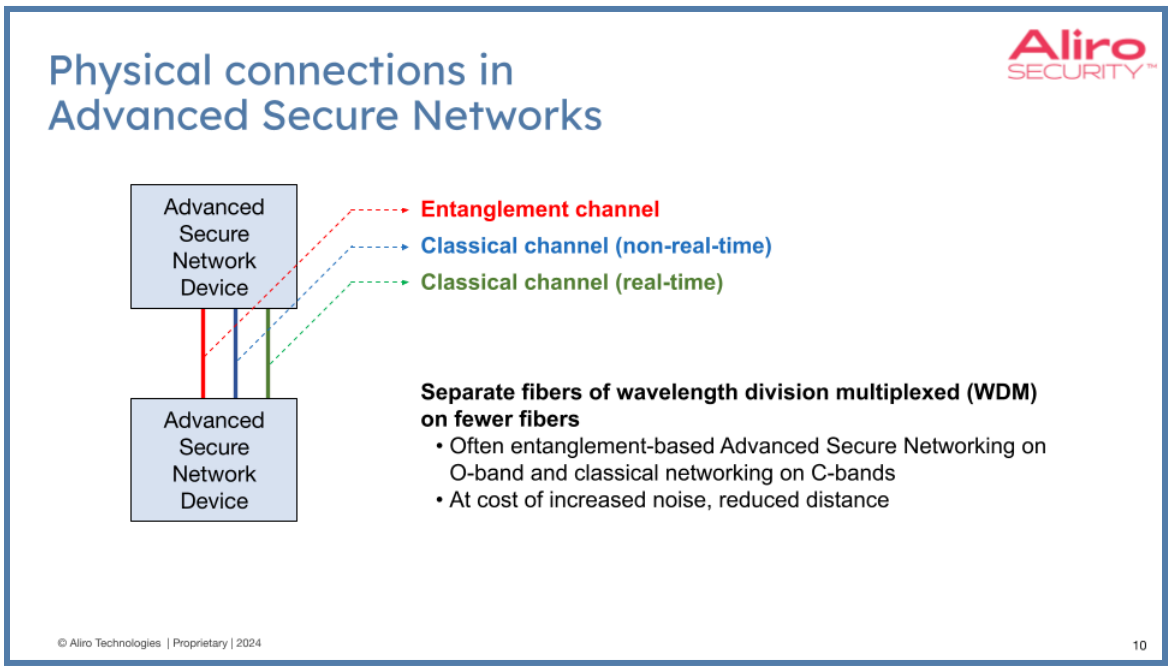
There are three layers of integration between classical networks and Advanced Secure Networks: the physical layer, the control layer, and the orchestration and management layer.

### Physical layer integration

Devices in an entanglement-based network are connected to each other using multiple channels. Here the term entanglement-based network device is used in a very general way, which could refer to advanced secure communication devices, quantum computers, entanglement-based repeaters, entanglement-based routers, quantum sensors, or any other type of device that might be found in an entanglement-based network.

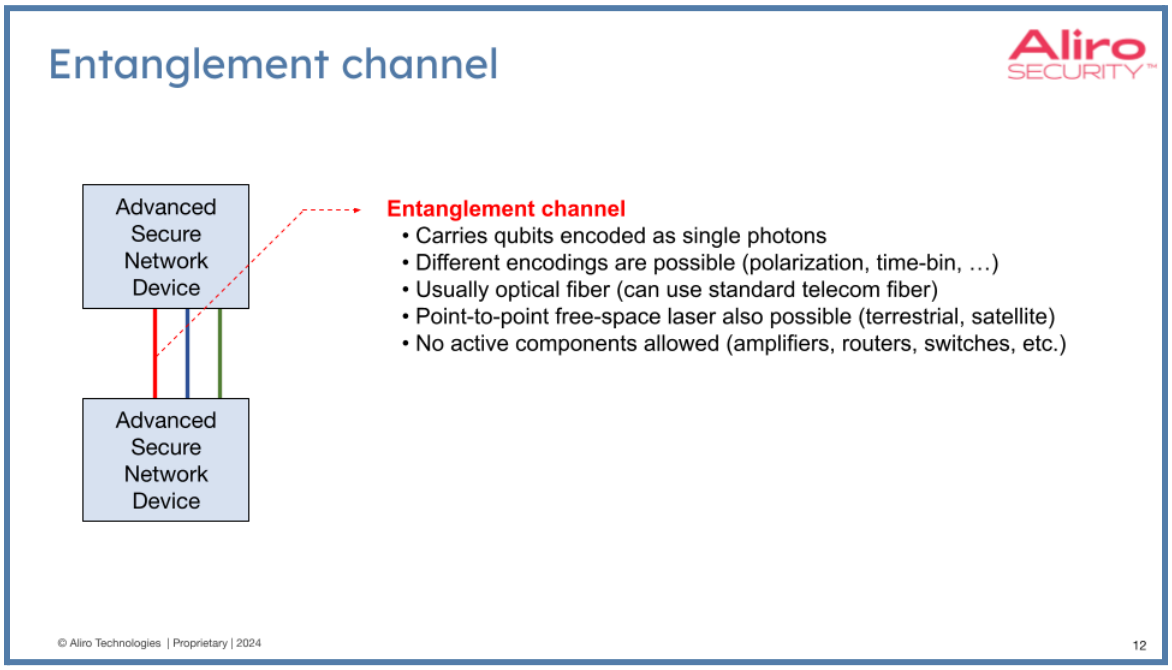
There are three channels: the entanglement channel, the real-time classical channel, and the non-real-time classical channel. Each of these channels can be implemented using optical fiber connections or using free-space connections subject to certain restrictions. When optical fibers are used, each channel can be assigned to a separate optical fiber strand, or multiple channels can be

multiplexed onto a single fiber using dense wavelength division multiplexing, or DWDM, once again subject to certain restrictions.




### Entanglement channel

The first channel is the entanglement channel. This is the channel that carries the qubits, which encode the qubit state information typically in the form of individual photons. There are multiple different encoding schemes, including polarization encoding and time-bin encoding, each with their own advantages and disadvantages. An in depth analysis of these encoding schemes is discussed in the on-demand webinar **Qubits: Understanding Quantum Information**.

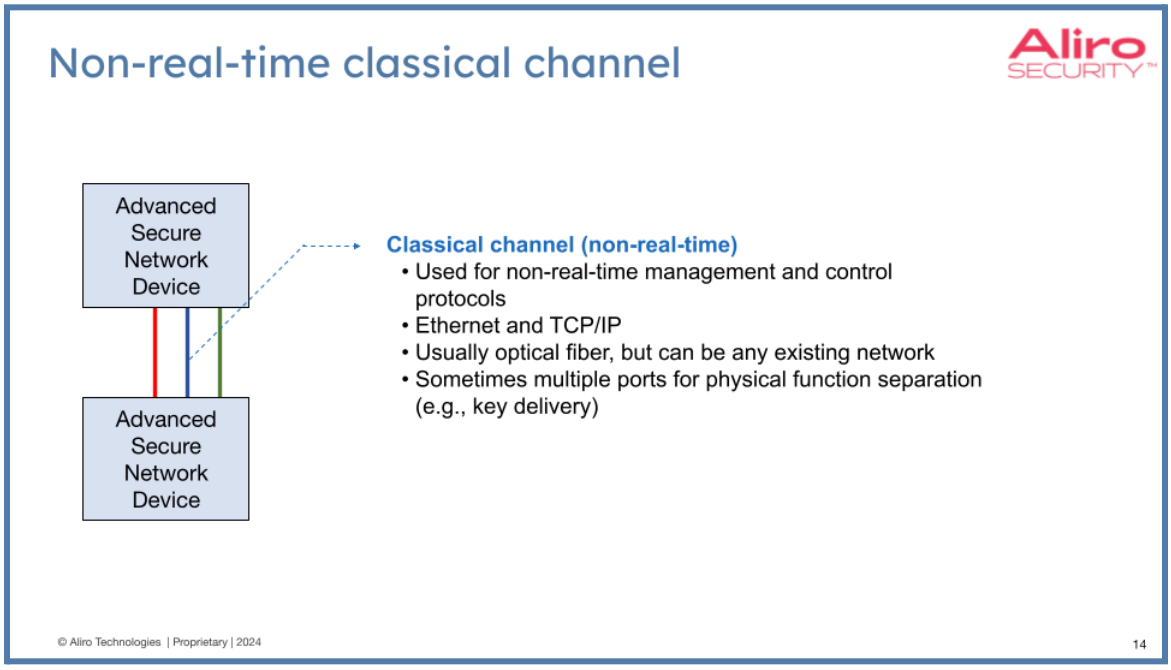


The entanglement channel is typically carried over optical fibers. It is possible to use typical telco fiber that is already deployed for the entanglement channel. It is not necessary to deploy a new kind of special fiber for the entanglement channel. However, the optical path used for the entanglement channel must not contain any active components. Passive components such as patch panels and optical cross-connects are compatible, but active components such as classical routers or classical switches or even simple classical amplifiers are not compatible with the entanglement channel.

It is also possible to carry the entanglement channel over a free-space connection. This may be a terrestrial point-to-point free-space connection, or it may be a ground-station to satellite free-space connection. Either way, the free-space connection must be implemented using a point-to-point laser. Radio networks, such as WiFi networks or cellular networks, are currently not suitable for the entanglement channel, and neither are copper links, such as DSL links.

### Non-real-time classical channel

The second channel is the non-real-time classical channel. This channel is used to carry orchestration, management, and non-real-time control protocols. The orchestration protocols are used to orchestrate the end-to-end service delivery to the end-user. The management protocols are used to configure and monitor the network devices. Orchestration and management protocols typically use YANG and NETCONF, which are protocols that are also widely used in classical networks.




The control protocols are used to control various aspects of the entanglement-based network. A small subset of these control protocols are extremely hard real-time, in the sense that they must be synchronized down to the nanosecond level. However, most of the control protocols are not hard

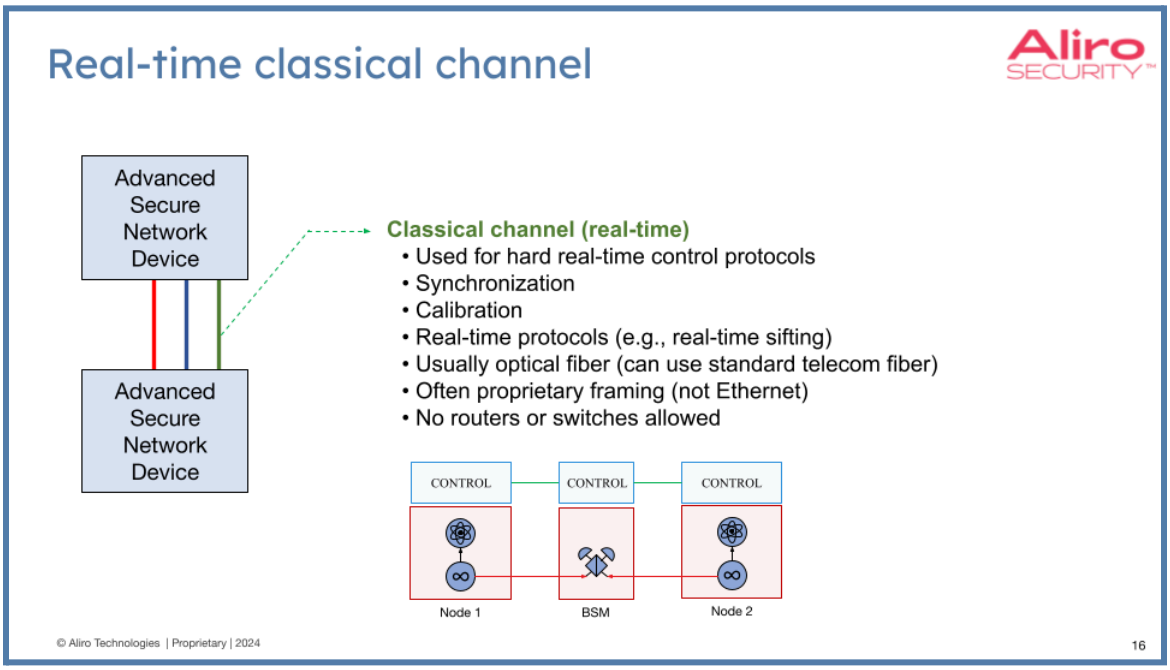
real-time. Examples of non-hard real-time control protocols include key post-processing (such as information reconciliation and privacy amplification), key delivery, topology discovery, resource discovery, session establishment signaling, and many more.

These non-real-time control protocols can be carried over the non-real-time classical channel along with the orchestration and management protocols. The non-real-time classical channel uses completely normal TCP/IP and Ethernet networks, and thus it is possible to use an existing classical network with existing classical routers and switches.

In practice, there are often multiple non-real-time classical channels using separate ports on the device for security reasons. For example, there might be separate physical ports for key delivery and network management.

### Real-time classical channel

The third channel is the real-time classical channel. This channel is known by many different names including the service channel or the synchronization channel. Examples of hard-real-time control protocols include synchronization, calibration, key sifting, elementary entanglement generation, entanglement swapping, entanglement distribution, and teleportation. These hard-real-time control protocols are carried over a dedicated channel.




Above is one possible mechanism for implementing elementary entanglement generation. In this example, the source on the left (Node 1) and the source on the right (Node 2) generate photons that need to arrive at the bell state analyzer in the middle (BSM) at exactly the same time, down to the nanosecond level. This requires extremely precise clock synchronization protocols. The entanglement generation protocol is non-deterministic in the sense that multiple attempts are needed to get a

successful entanglement. For this, a real-time control protocol is needed to track the attempts and retry until success is achieved.

Because of the sheer volume of control messages and because of the very precise timing requirements, these real-time control protocols typically don't use TCP/IP or even Ethernet. Instead, these protocols often use proprietary framing and are typically implemented in FPGAs. Due to this proprietary framing, the optical path for the real-time classical channel must not contain any IP routers or Ethernet switches. However, DWDM and amplifiers are still compatible with this channel.

## Maximum link distance

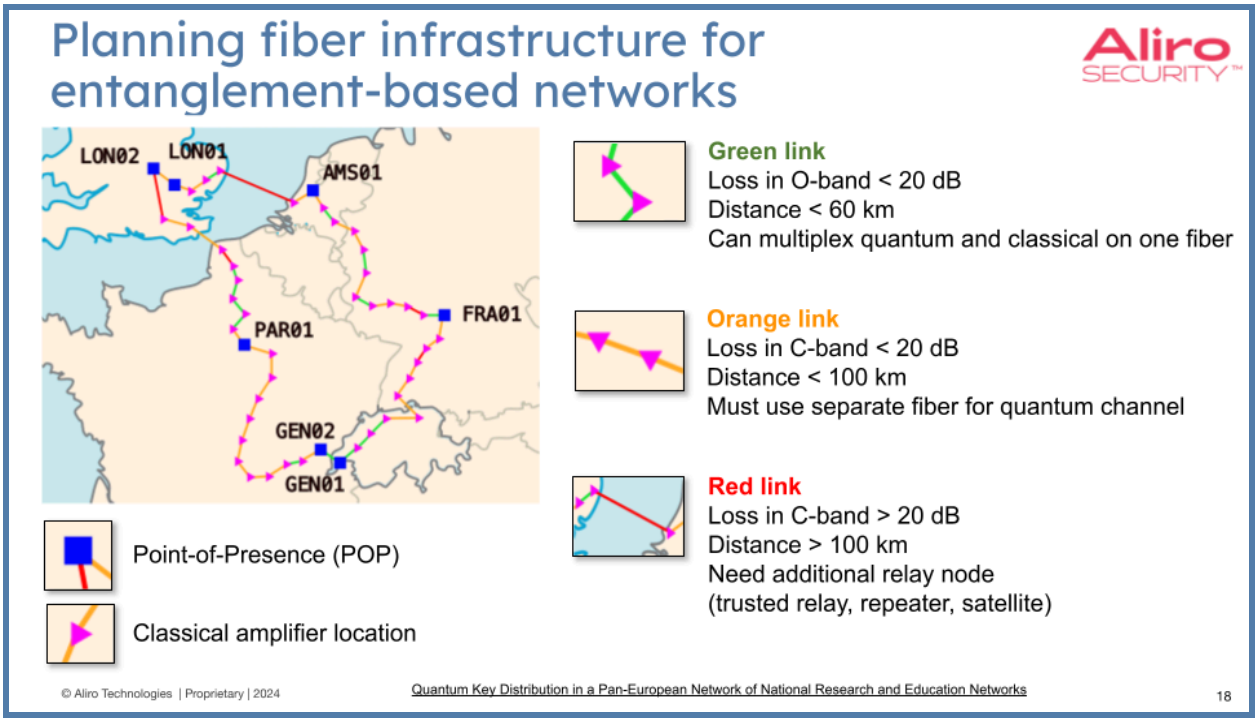
One of the challenges in implementing entanglement-based networks at the physical layer is the limited maximum distance for point-to-point links on the entanglement channel. As a general rule of thumb, we can say that the maximum loss on a point-to-point entanglement link is around 20 decibels which translates into a maximum distance of roughly 100 kilometers. The exact limit depends on various technical details, for example, what type of sources and what type of detectors you use. The actual distance limit may be higher or lower; but 100 kilometers is typical, and this is the number used in the examples throughout this white paper. Beyond 100 kilometers, a kind of relay mechanism is necessary. This might be a trusted relay node, an entanglement-based repeater, an entanglement-based router, or a satellite.

In many real-world deployments, it is very desirable to use dense wavelength division multiplexing, or DWDM, to multiplex classical and entanglement channels onto the same fiber. This greatly reduces the cost of the network because you have to deploy fewer fibers.

It is customary to put the entanglement channels in the O-band and the classical channels in the C-band to minimize interference between the entanglement and the classical channel. When you put the entanglement channel in the O-band, the maximum distance is reduced by about 40% because the optical fiber has more loss in the O-band than in the C-band.

## Planning fiber infrastructure for entanglement-based networks

GEANT, which is a pan-European research network, published a very interesting paper studying how much it would cost to upgrade their existing classical network to a quantum network. In this GEANT study, they were evaluating a QKD network, so they only considered QKD trusted relay nodes.[GEANT] However, a similar methodology can also be used for general-purpose entanglement-based Advanced Secure Networks, such as those used for Advanced Secure Communication.




The map shows one ring in the existing classical pan-European GEANT network.

- The blue squares represent points-of-presence or POPs.
- There are two POPs in London, one in Amsterdam, one in Frankfurt, two in Geneva, and one in Paris.
- The pink triangles represent classical amplifier locations.
- The lines represent optical fiber spans between these POPs and amplifier stations.

First of all, the study assumes that the trusted relay nodes are deployed at every existing POP and amplifier location. That makes sense because that's where the existing buildings with power and access to the management network are. Then, the study looked at each of these fiber spans and color coded them green, orange or red.

The green links have less than 20 dB loss in the O-band, roughly less than 60 kilometers. This is the ideal and cheapest scenario. In this case the distance is short enough to be able to do a wave division multiplex of the quantum channel onto the same existing fiber for the classical channels. New DWDM devices may need to be deployed if they are not already there, but we don't need to deploy any new fiber which is typically much more expensive.

The orange links have less than 20 dB loss in the C-band, roughly less than 100 kilometers. Here we have to use a separate fiber for the quantum channel, which is more expensive.

The red links have more than 20 dB loss in the C-band, roughly more than 100 kilometers. Here the distance is too long for a quantum channel, even if we use a separate fiber. The only option is to introduce an additional relay node, which is the most expensive.

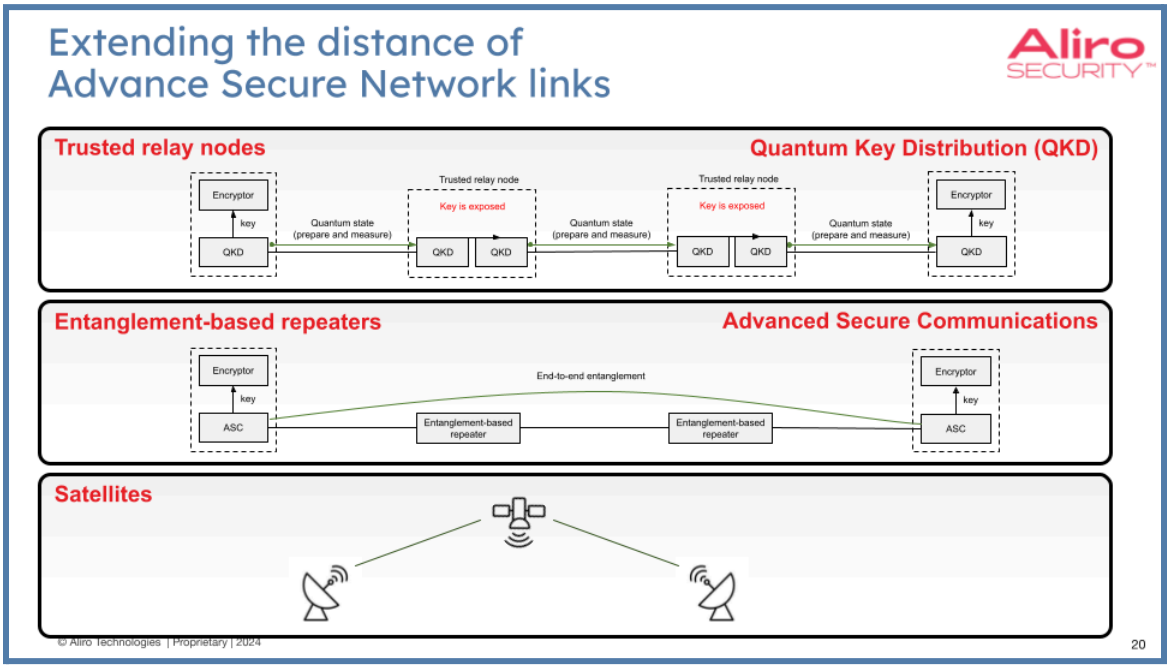
This particular study is unusual, in the sense that it studied a large pan-European network. Currently most entanglement-based Advanced Secure Communication networks are deployed in metro region networks.

## Extending the distance of entanglement links

There are several options for relay nodes to extend the distance of a point-to-point entanglement link exceeding 100 kilometers.

In current Quantum Key Distribution networks so-called "trusted relay nodes" are used. The way they work is that they first establish a point-to-point encryption key on each link, then the end-to-end encryption key is forwarded hop-by-hop through this series of encrypted point-to-point links. This method has a critical disadvantage: the end-to-end key is exposed in the clear inside each of the trusted relay nodes. The name trusted relay node is somewhat misleading. It is not that the node is trustworthy. It is that trust is forced: the node must be trusted to not leak the exposed key. This need for trusted relay nodes is one of the most important criticisms of current first generation Quantum Key Distribution networks. Another important drawback is that QKD networks are single-purpose: they can only ever be utilized for key distribution alone.

A better method to extend the distance of entanglement links is to use entanglement-based repeaters in place of trusted relay nodes. Entanglement-based repeaters offer two important benefits. The first benefit is that the keys are not exposed at the repeaters. The second benefit is that an entanglement-based network built out of entanglement-based repeaters is a general-purpose Advanced Secure Network.



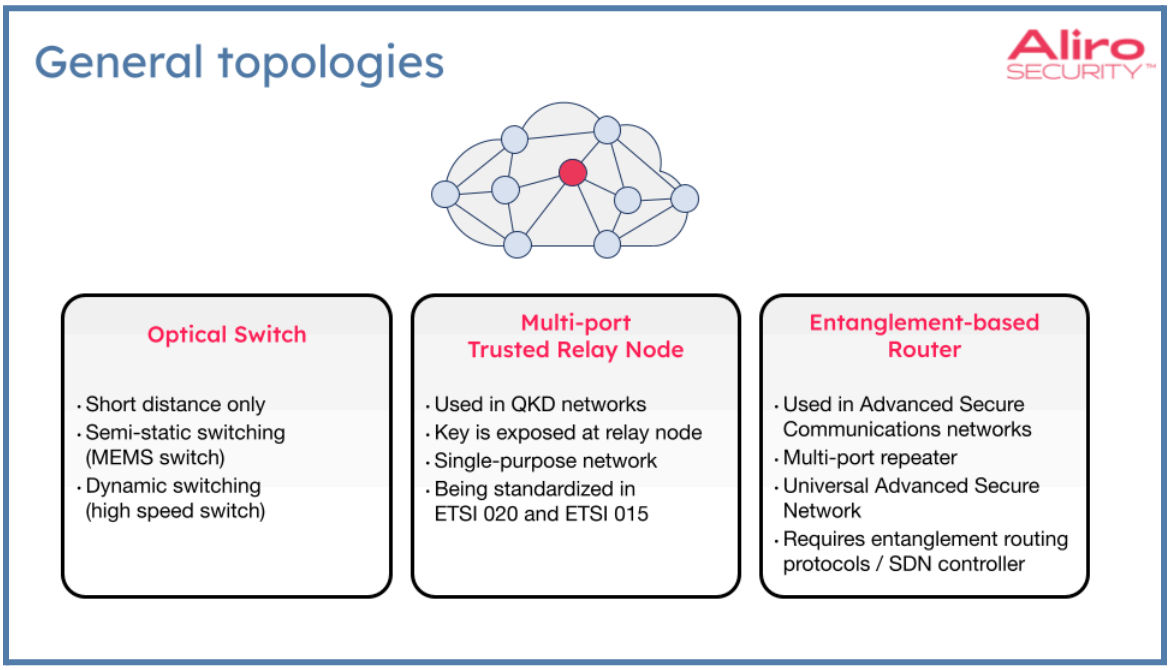

It can be used not only for Advanced Secure Communications but also for other applications such as clustered and distributed quantum computing and sensing.

The current first generation of QKD networks are similar to the telephone networks of the 1980s: they can only run one single application. Entanglement-based Advanced Secure Networks are like the Internet of today in the sense that they can run any application.

The challenge with repeaters, however, is that they are an emerging technology. The components that are needed to build entanglement-based repeaters (notably quantum memories) are only just now becoming commercially available. Aliro expects entanglement-based repeaters to become a viable option to replace trusted relay nodes over the next few years.

Finally, for intercontinental distances, there is the option to use satellites and ground stations connected by free-space lasers. Because the loss in the vacuum of space is much lower than in fiber, they can cover large distances of up to several thousands of kilometers. The downside to using this method is that satellites and ground stations are expensive to deploy.

## General topologies




If you have a more general graph topology, then it's necessary to implement relay nodes that have more than two interfaces and some sort of routing functionality. This can be achieved in several ways.

If the distances are short enough, for example in metro area networks (MANs), then you can use layer one optical switches. Those optical switches can be relatively slow, such as a MEMS switch. The optical switches could also be very fast, such as with Mach-Zehnder Interferometry switches, to do very dynamic switching.

For longer distances, in the current first generation of Quantum Key Distribution networks, it is customary to use multi-port trusted relay nodes. The software has routing functionality to determine the path for the end-to-end key generation session through which the encryption key needs to be relayed. This approach has the same problem that we mentioned before: the relay nodes must be trusted because the key is exposed at each hop. The need to trust multiple devices which are potentially owned and operated by another organization (e.g., a service provider), to keep your information secure makes for a fragile solution.

A better approach is to use multi-port entanglement repeaters which we refer to as entanglement-based routers. Once we have entanglement-based routers, we have a general-purpose general-topology entanglement generating network.

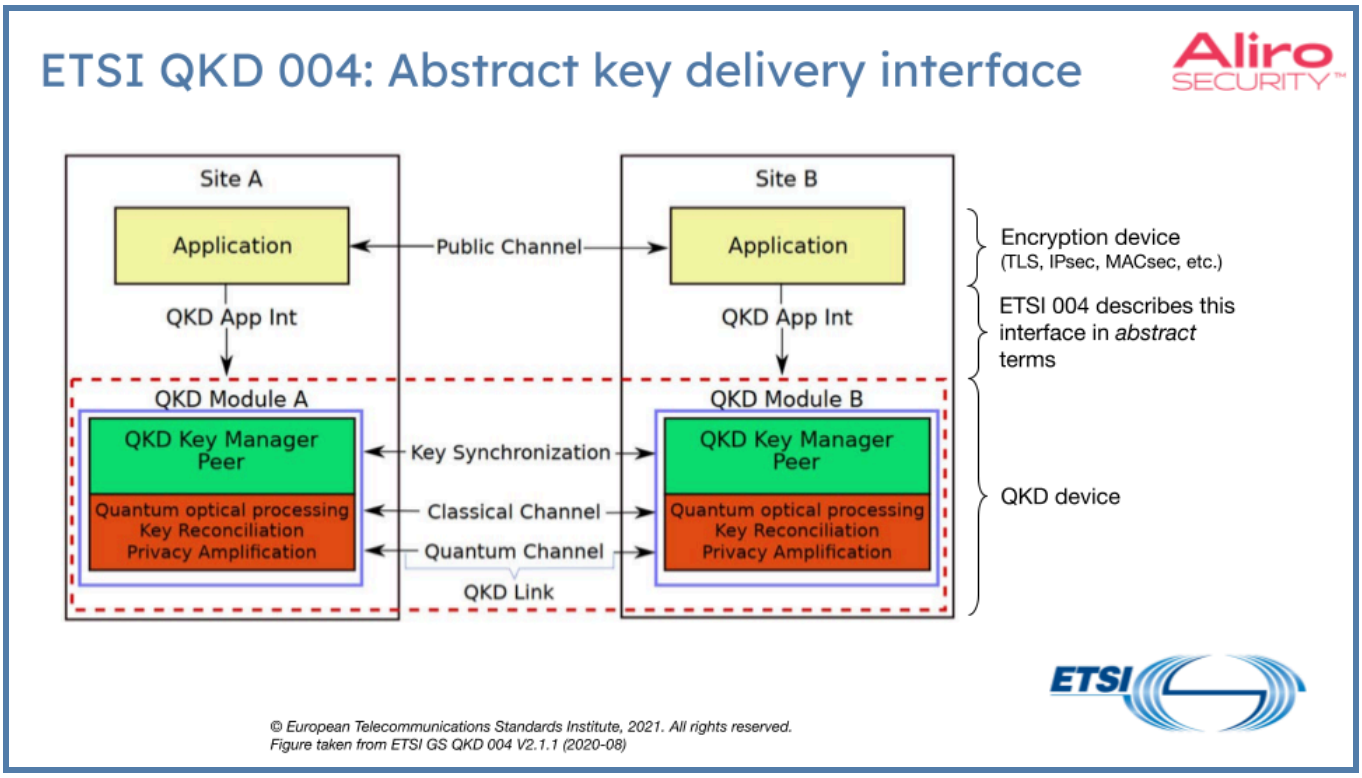
## Application layer integration

For the purposes of this white paper, when discussing application layer integration the focus will be on the Advanced Secure Communications application. In this case, the primary purpose of the entanglement-based network is to generate encryption keys and the primary purpose of the classical network is to do the bulk encryption using those keys. An interface between the entanglement-based network and the classical encryptors to hand off these keys will be necessary.

### ETSI 004 abstract key delivery interface

Contrary to what you might expect, this key delivery interface is already very well defined and standardized by ETSI, the European Telecommunications Standardization Institute. ETSI has defined a series of so-called group specifications that include a definition of this interface. All of these ETSI specifications are publicly available at no cost. They are short and very readable, and we highly recommend downloading and reading them. While ETSI specifications refer frequently to QKD and Quantum Key Distribution, with a few exceptions all of these ETSI specifications can also be applied to entanglement-based networks (which use entanglement-based repeaters and entanglement-based routers instead of trusted relay nodes) with little or no changes.

The first of these group specifications is called ETSI QKD 004 which is summarized below.[ESTI004]




In the diagram above, the yellow boxes are the classical encryptors.

The red and green boxes are the quantum network devices.

We can see the quantum channel, the non-real-time classical channel, and the real-time classical channel (here referred to as the synchronization channel) that was discussed previously in this paper. The key delivery interface that ETSI 004 describes are the vertical arrows labeled QKD Application Interface between the yellow and green boxes.

ETSI 004 is a rather abstract document. It talks about the types of primitives that are needed on the key delivery interface in very general terms. ETSI 004 is not concrete enough to enable interoperable implementations.

## ETSI QKD 014

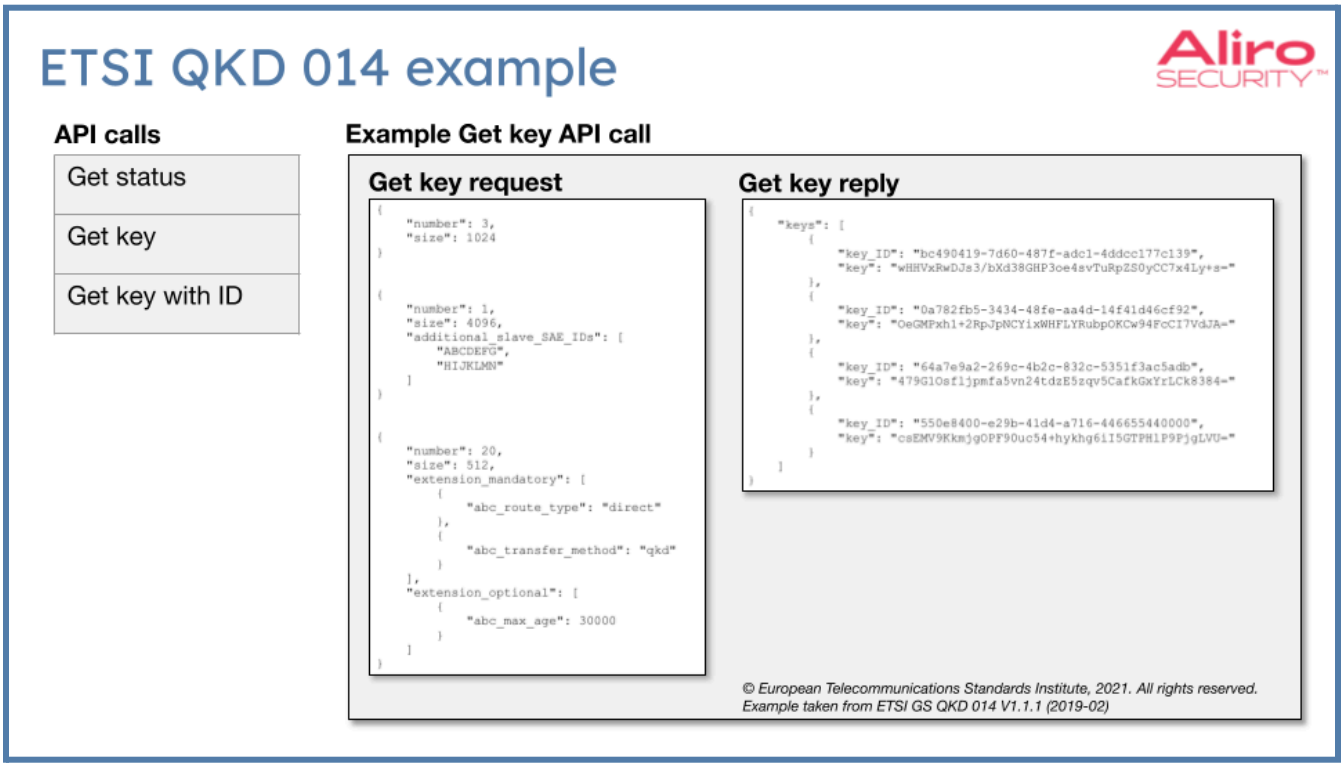
Specification ETSI 014 takes the general principles described in ETSI 004 and makes them much more concrete and specific. ETSI 014 defines a REST interface, which is a very common type of HTTP-based interface that is very frequently used to integrate different systems with each other.

Unlike ETSI 004 which is rather abstract, ETSI 014 is very concrete. If a classical encryptor from one vendor and a quantum network device from another vendor both support ETSI 014, then they will interoperate. In fact, most existing QKD vendors already support ETSI 014, and many classical encryptor vendors are in the process of adding ETSI 014 support.[ETSI014] Many have already done public proofs of concept.

The ETSI 014 protocol is extremely simple. There are only three messages. The Get Status message is used to check whether a quantum device has keys available, as well as other operational status parameters. The encryptor uses the Get Key message to get the encryption key. The decryptor uses the Get Key with Key IDs message to get the decryption key. The encryptor must use some out-of-band mechanism to transfer the key IDs to the decryptor. The Internet Engineering Task Force (IETF) is already working on enhancements to IPsec and other protocols to facilitate this key ID transfer from the encryptor to the decryptor.

## ETSI QKD 014 Example

Below is an example of what the ETSI 014 protocol looks like in real life.




On the left are several examples of the Get Key message, which is the message that the classical encryptor uses to request an encryption key from the quantum network. In its simplest form, the encryptor specifies the number of keys needed and the size in bits of each key. On the right, is an example of the Get Key reply message. This is the message that the quantum network sends back to the encryptor to actually provide the requested session encryption keys. Each provided key has a key ID and the actual key value itself. The REST communication session between classical encryptor and the quantum network is itself encrypted and mutually authenticated.

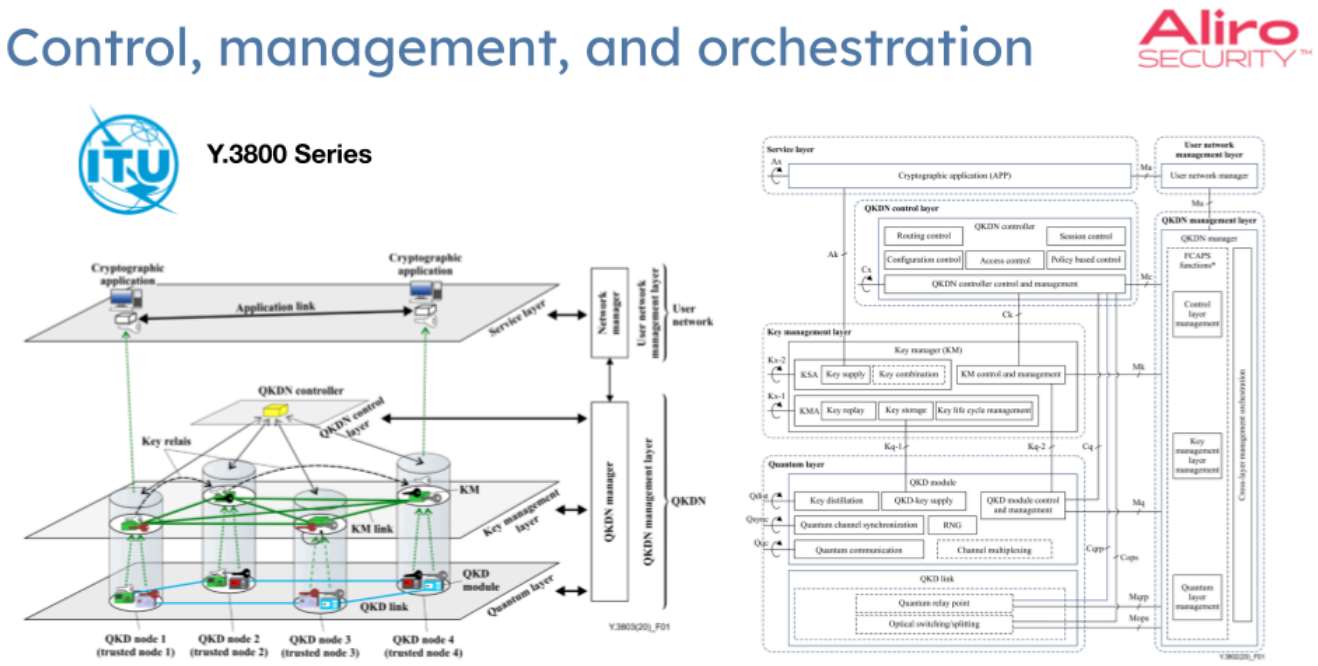
## Management and orchestration layer integration

Just like any other network, entanglement-based Advanced Secure Networks need to be controlled, managed, and orchestrated. This is another area where entanglement-based networks and classical networks are deeply intertwined with each other.

### Control, Management, and Orchestration

There has been a surprising amount of standardization in the area of controlling, managing, and orchestrating quantum networks. The International Telecommunication Union International Telecommunications Standardization Sector (ITU-T) has published a series of standards called the Y-3800 series describing quantum networks.[Y3800] The ITU-T standards are publicly available at no cost.

Just like the ETSI specifications that discussed previously, the ITU-T standards are currently framed in terms of QKD networks, but many of these standards can also be generalized for entanglement-based Advanced Secure Networks that use entanglement-based repeaters, and to facilitate other applications such as distributed quantum computing.




The figure on the left in the graphic above is taken from ITU-T Y.3803. It shows the layers of a secure communications network.

At the bottom is the quantum layer with the quantum network devices.

Above the quantum layer is the key management layer.

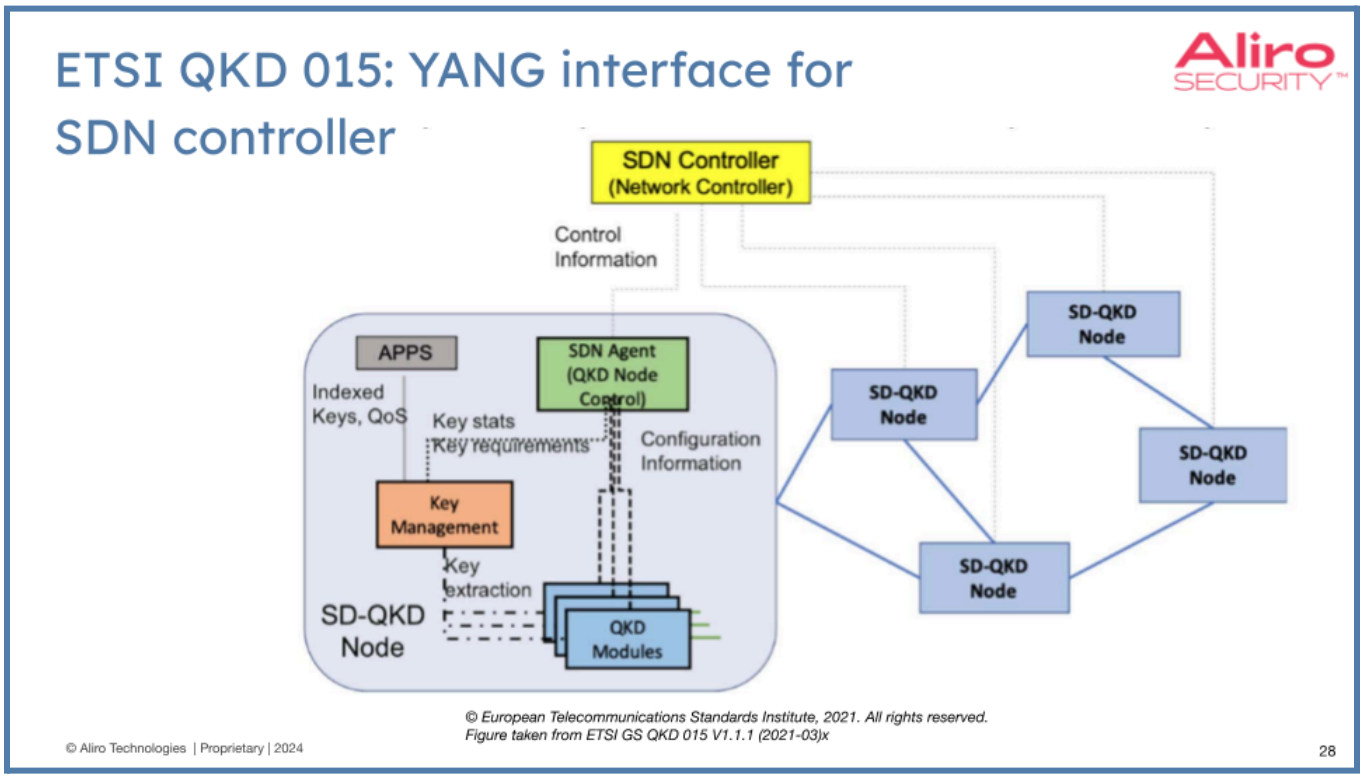
Above the key management layer is a quantum network controller, represented here by a yellow box. This controller is similar to a software defined networking (SDN) controller in existing classical networks.

The job of the controller is to control the network nodes to create an end-to-end quantum session for the delivery of encryption keys to the application nodes. In today's QKD networks, these quantum relay nodes are assumed to be trusted relay nodes, but the same approach also works when creating end-to-end entanglement generation sessions in an entanglement-based repeater network, such as an Advanced Secure Network.

The application nodes are shown in the service layer at the top. The two white boxes next to the layers represent the management functions. There is a network management function responsible for managing the devices in the network, and there is an orchestration function responsible for managing the end-user service.

## ETSI 015 : YANG Interface for SDN Controller

As of now, the ITU-T has not yet standardized any concrete protocols; they have only defined abstract reference models. Once again, ETSI has gone further: they have defined concrete protocols for controlling, managing, and orchestrating QKD networks. In particular, ETSI group specification 015 defines the protocol between the quantum network controller and the quantum nodes.[ETSI015]

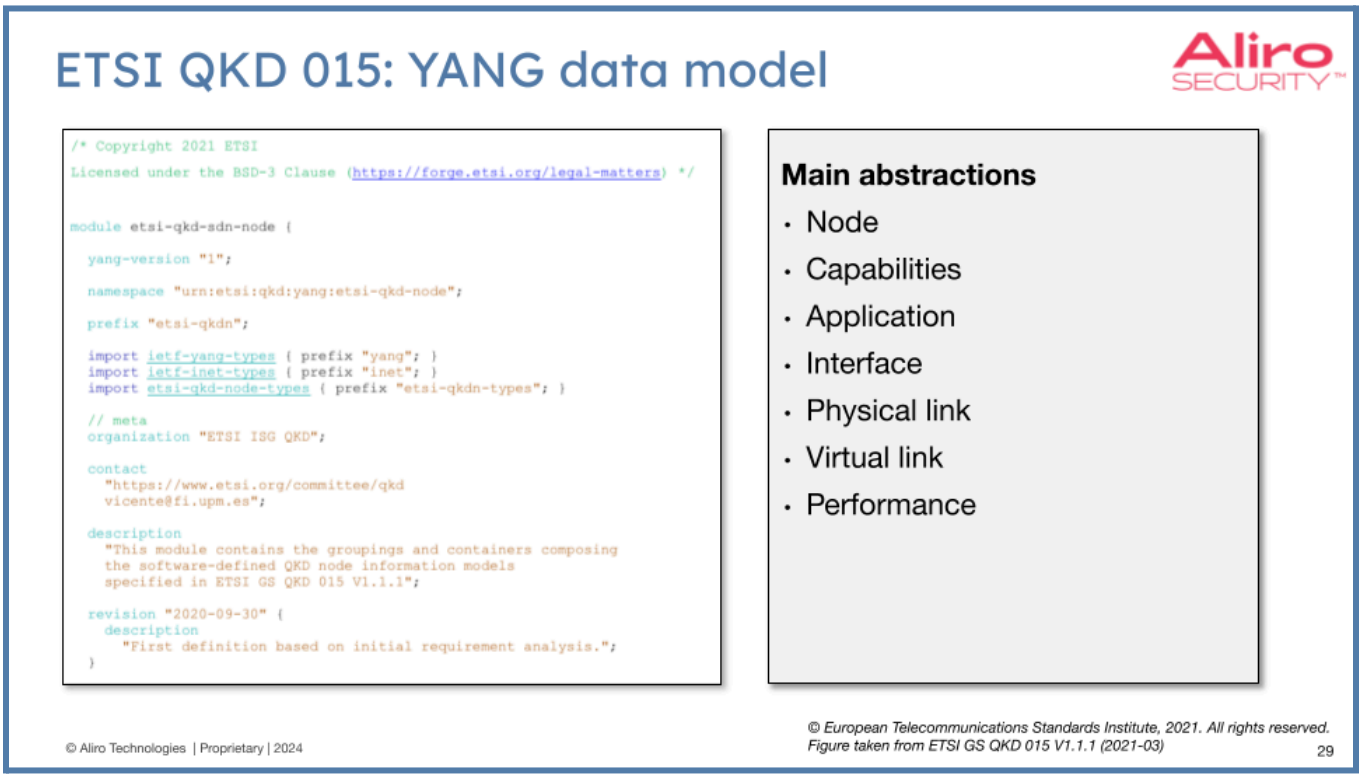



In the diagram above, the yellow box represents the quantum network controller, and the blue boxes below represent the quantum network nodes. One of the blue boxes on the left has been magnified to show its internal structure.

ETSI  015 defines the quantum network control protocol using YANG data models and the NETCONF and RESTCONF protocols. If these acronyms don’t mean much to you, the important thing is that YANG and NETCONF or RESTCONF are the exact same protocols that are already widely used in classical networks today.

## ETSI QKD 015 YANG Data Model

The ETSI 015 group specification includes a YANG data model which describes the configuration and operational objects for quantum nodes. The YANG data model is remarkably easy to read, even if you have never seen a YANG data model before.



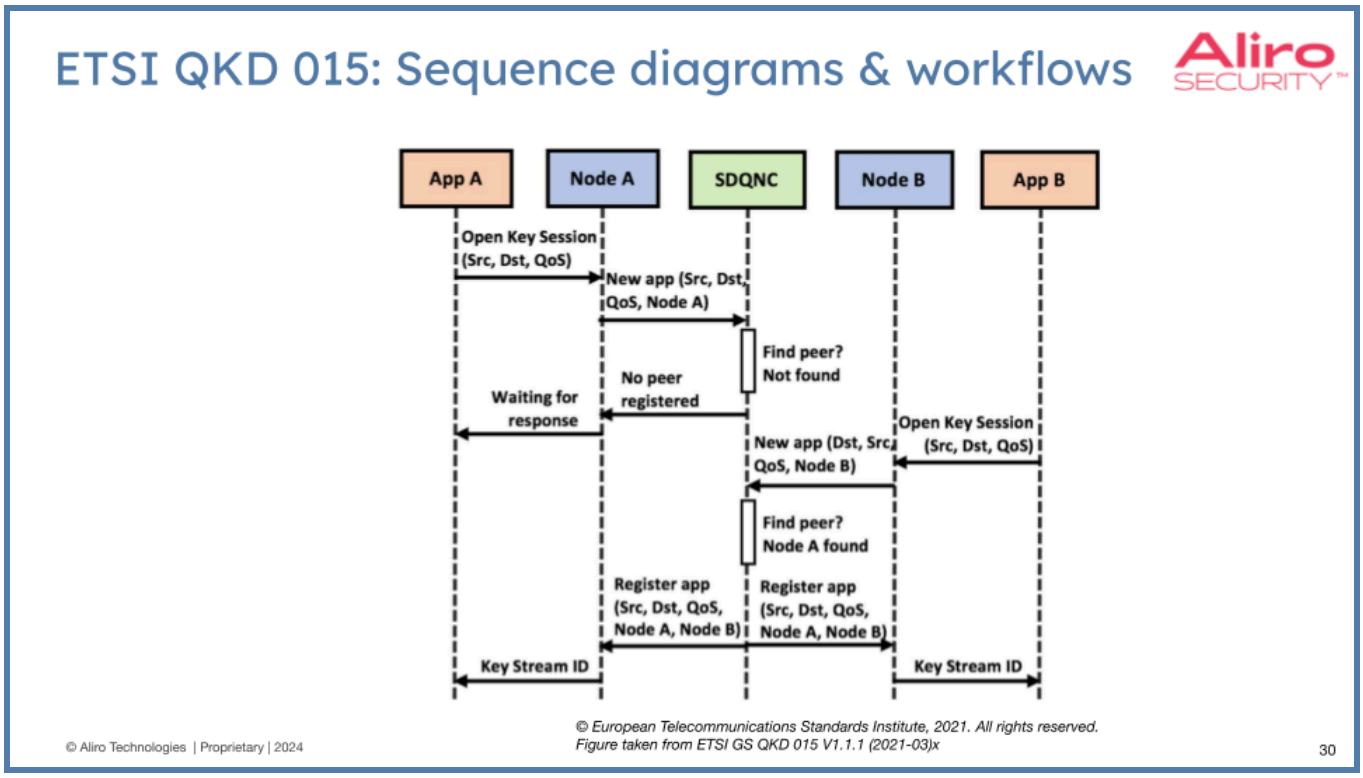

Node attributes can be configured and monitored. For example, the hardware and software versions of the node can be retrieved. The capabilities of nodes can be discovered. For example, it's possible to discover whether or not the node can act as a trusted relay node. Application endpoints can be configured and monitored. For example, it's possible to configure which encryptors are allowed to get keys from that particular node.

Quantum key generation sessions a node participates in can be configured and monitored. These key generation sessions are confusingly referred to as "links" in the specification. A quantum key generation session can include trusted relay nodes, using a concept referred to as virtual links in the specification. It is even possible to configure quality of service parameters for the key generation sessions such as rate and jitter.

## ETSI QKD 015 Sequence diagrams and workflows

That same specification ETSI 015 also contains multiple sequence diagrams describing various workflows.

One example is shown below.

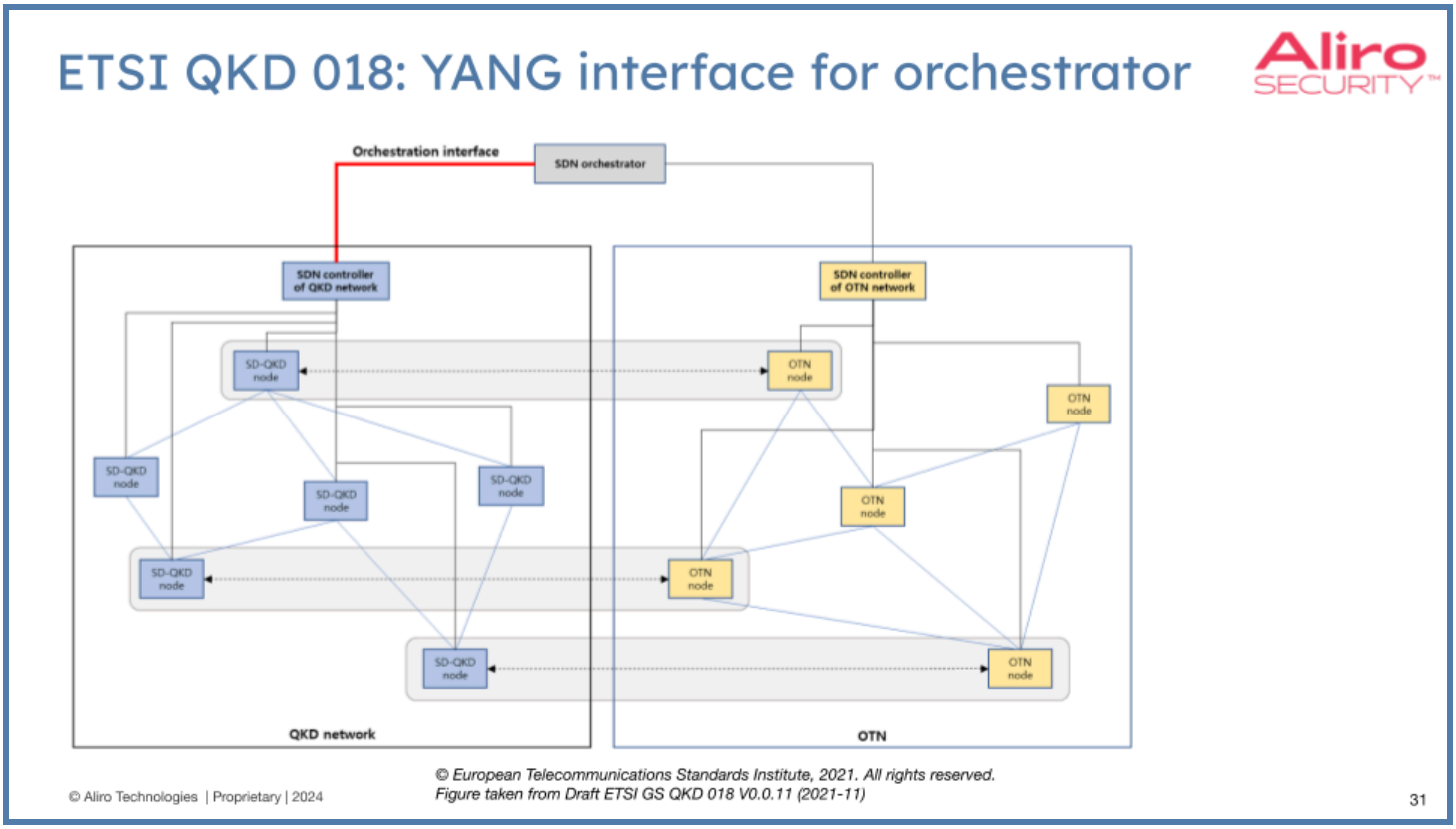



This is the workflow for two application nodes, in this case two classical encryptors, to register themselves with the quantum network and to establish a key exchange session amongst themselves.

## ETSI QKD 018: YANG interface for orchestrator

The final ETSI group specification this white paper will cover is ETSI 018, which defines the interface between the orchestrator and the controller. The gray box at the top is the orchestrator which is responsible for orchestrating end-to-end services to end-users. In this application, the end-user service is delivering encryption keys.[ETSI018]

For example, the end-user could ask for a key delivery session between Amsterdam and Brussels, with a key rate of five kilobits of key material per second. It is the role of the orchestrator to facilitate this across multiple management domains. The orchestrator has to configure the quantum nodes to produce and relay the quantum keys. To do this, the orchestrator talks to the quantum network controller (as discussed above) - this is the top blue box in the diagram below. The orchestrator is also responsible for configuring the optical transport nodes or OTNs to create the necessary optical paths in the network. To do this, the orchestrator talks to the OTN controller which is the top yellow box in diagram below. ETSI 018 defines the interface between the orchestrator and the quantum network controller, which is the red line in the diagram below.

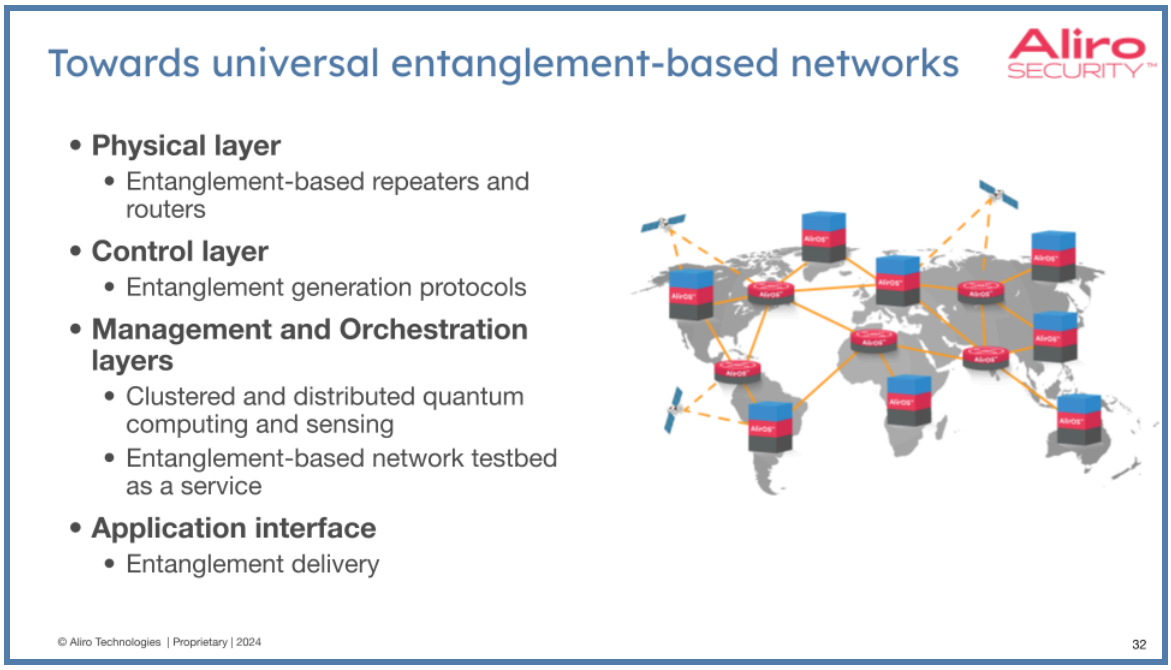



Once again, the ETSI specification is not an abstract reference model. It is a well-defined protocol specified using a YANG data model and can be implemented by vendors for interoperability between components.

## Towards universal entanglement-based Advanced Secure Networks

This white paper has discussed several interfaces, protocols, and standards in the context of secure communications. The next step is to generalize all of these interfaces, protocols, and standards to general-purpose entanglement-based Advanced Secure Networks.

At the physical layer, entanglement-base repeaters and entanglement-based routers will need to be introduced to the network. At the control layer, entanglement generation protocols - including elementary entanglement generation, swapping, purification, and teleportation - need to be implemented. At the management and orchestration layer, the network needs to continue to enable new end-user services such as clustered and distributed quantum computing and sensing and network testbed as a service. Finally, at the application interface, it is necessary to support general-purpose entanglement delivery.




Quite a lot can be implemented through software. An entanglement-based network software stack for building general-purpose entanglement-generating Advanced Secure Networks should have these primary components:

- An orchestrator to implement the orchestration and management layer. This provides an interface to the operator to manage the entanglement-based Advanced Secure Network and provides an interface to end-users to orchestrate the services provided by the quantum network
- An SDN controller for the entanglement-based Advanced Secure Network
- An on-device distributed control plane for the entanglement-based Advanced Secure Network

A simulator for modeling Advanced Secure Networks at different levels of abstraction for testing potential hardware and topologies is also recommended, as it can be integral to the design phase of entanglement-based Advanced Secure Network implementation.

## A full-stack solution for entanglement-based Advanced Secure Networking

Entanglement-based secure networks are being built today by a variety of organizations for a variety of use cases – benefiting organizations internally, as well as providing great value to an organization's customers. Telecommunications companies, national research labs, intelligence organizations, and systems integrators are just a few examples of the organizations Aliro is helping to leverage the capabilities of entanglement-based Advanced Secure Networking.

Building entanglement-based secure networks is no easy task. It requires:

- Emerging hardware components necessary to build the Advanced Secure Network.
- The software necessary to design, simulate, run, and manage the Advanced Secure Network.

- A team with expertise in the science of entanglement-based networking as well as classical networking.
- Years of hard work and development.

This may seem overwhelming, but Aliro is uniquely positioned to help you build your entanglement-based Advanced Secure Network. The steps you can take to ensure your organization is meeting the challenges and leveraging the benefits of the quantum revolution are part of a clear, unified solution already at work in entanglement-based networks like the EPB Quantum Network℠ powered by Qubitekk in Chattanooga, Tennessee.

AliroNet™, the world's first full-stack entanglement-based network solution, consists of the software and services necessary to ensure customers will fully meet their entanglement-based networking goals. Each component within AliroNet™ is built from the ground up to be compatible and optimal with entanglement-based networks of any scale and architecture. AliroNet™ is used to simulate, design, run, and manage entanglement-based Advanced Secure Networks as well as test, verify, and optimize hardware for network performance. AliroNet™ leverages the expertise of Aliro personnel in order to ensure that customers get the most value out of the software and their investment.

Depending on where customers are in their Advanced Secure Networking journeys, AliroNet™ is available in three modes that create a clear path toward building full-scale entanglement-based secure networks: (1) Emulation Mode, for emulating, designing, and validating quantum networks, (2) Pilot Mode for implementing a small-scale quantum network testbed, and (3) Deployment Mode for scaling entanglement-based Advanced Secure Networks and integrating end-to-end applications. AliroNet™ has been developed by a team of world-class experts in quantum physics and classical networking.

To get started (or continue on your advanced secure networking journey), reach out to the Aliro team for additional information on how AliroNet™ can enable your Advanced Secure Network.

info@alirosecurity.com www.alirosecurity.com

## References

**[GEANT]** Karel Van Klink. “Quantum Key Distribution in a Pan-European Network of National Research and Education Networks”. Thesis presentation, University of Twente, The Netherlands and GÉANT Vereniging, The Netherlands
http://essay.utwente.nl/93637/1/van%20Klink_MA_EEMCS.pdf

**[ESTI004]** ETSI. “Quantum Key Distribution (QKD); Application Interface. ETSI GS QKD 004 v2.1.1”. European Telecommunications Standards Institute. 2020.
https://www.etsi.org/deliver/etsi_gs/QKD/001_099/004/02.01.01_60/gs_qkd004v020101p.pdf

**[ETSI014]** ETSI. “Quantum Key Distribution (QKD);Protocol and data format of REST-based key delivery API. ETSI GS QKD 014 V1.1.1 (2019-02).” European Telecommunications Standards Institute. 2019.
https://www.etsi.org/deliver/etsi_gs/QKD/001_099/014/01.01.01_60/gs_qkd014v010101p.pdf

**[Y3800]** ITU-T. “Y series: Global information infrastructure, Internet protocol aspects, next-generation networks, Internet of Things and smart cities. Y.3800-Y.3999: Quantum key distribution networks”. International Telecommunication Union International Telecommunications Standardization Sector. 2019. https://handle.itu.int/11.1002/1000/13990

**[ETSI015]** ETSI. “Quantum Key Distribution (QKD); Control Interface for Software Defined Networks. ETSI GS QKD 015 V1.1.1 (2021-03)”. European Telecommunications Standards Institute. 2021.
https://www.etsi.org/deliver/etsi_gs/QKD/001_099/015/01.01.01_60/gs_qkd015v010101p.pdf

**[ETSI018]** ETSI. “Quantum Key Distribution (QKD); Orchestration Interface for Software Defined Networks. ETSI GS QKD 018 V1.1.1 (2022-04)”. European Telecommunications Standards Institute. 2022. https://www.etsi.org/deliver/etsi_gs/QKD/001_099/018/01.01.01_60/gs_qkd018v010101p.pdf