This paper gives a high-level technical description of the *AURORA KMS*. As outlined in the product data sheet, AIT's KMS for QKD Networks is available in two versions: *AURORA KMS Core* and *AURORA KMS Extended*. This document provides additional technical information on the feature descriptions, with the extra features available in the *AURORA KMS Extended* highlighted in a colored box. The feature descriptions are based on version `v3.0.0`.

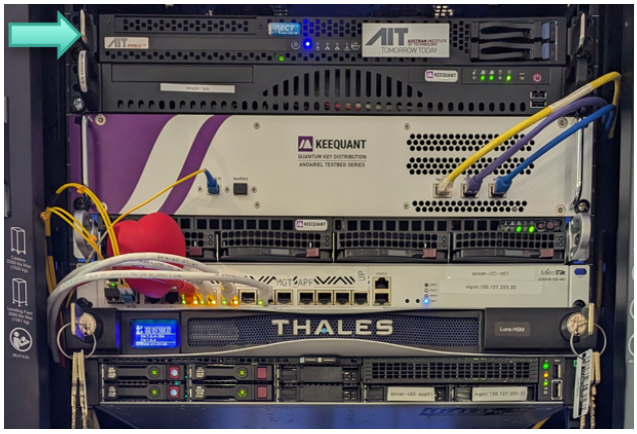


Figure 1: *AURORA KMS* on Hardware (top, highlighted with arrow), integrated with KEEQuant QKD device (below) and Wireguard VPN application (bottom)

1 Application interface

The *AURORA KMS* supports the **ETSI GS QKD 014** [1] v1.1.1 API, the de-facto standard in the QKD ecosystem, therefore compatible with all applications supporting it. The compatibility was verified in deployments with the following applications:

- ADVA encryptors
- Thales Mistral encryptors
- Wireguard VPN with Arnika extension
- Research Systems

The *AURORA KMS Extended* additionally supports **ETSI GS QKD 004 v2.1.1** [2] using http, https or CoAP. It also supports **CISCO SKIP** [3].

2 QKD Device Interface

The *AURORA KMS* connects to QKD devices via the **ETSI GS QKD 014 v1.1.1** [1] API. It is therefore compatible with all devices supporting it. The compatibility was verified in deployments with the following devices:

- LuxQuanta
- ThinkQuantum
- QTI
- KEEQuant
- Quantum Optics Jena
- Q*Bird
- ID Quantique
- zerothird
- heqa

In addition, the *AURORA KMS Extended* comes with an **ETSI GS QKD 004 v2.1.1** [2] push mode interface using CoAP. This interface has been validated in research projects with non-commercial QKD devices and also integrates with AIT's Postprocessing software.

3 Management Interface

The *AURORA KMS* comes with an http REST API, described with OpenAPI, that allows the extraction of the following KPIs:

- **Key Availability (KAV):** indicates the number of keys available for use by applications or internally.
- **Internal Key Rate (IKR):** indicates the key rate for internal usage to generate ITS MACs and for ITS encryption.
- **External key Rate (EXKR):** indicates the key rate for external usage by applications on the node.
- **Secret Key Rate (SKR):** indicates the key rate of the QKD layer as received by the KMS.

The management interface allows:

- Connect and disconnect QKD devices.
- Query the KMS status and version.
- Retrieve Logging information.

4 Inter-KMS API

The inter-KMS API is used for key relay and synchronization. Key relay complies with the hop-by-hop relay technique outlined in "case 2" of ITU-T Y3803 [4] as shown in fig. 2. All messages on this interface are ITS authenticated and integrity protected with an ITS MAC. Additionally, relayed key material is encrypted with ITS encryption. Furthermore, this communication is protected via TLS 1.3.

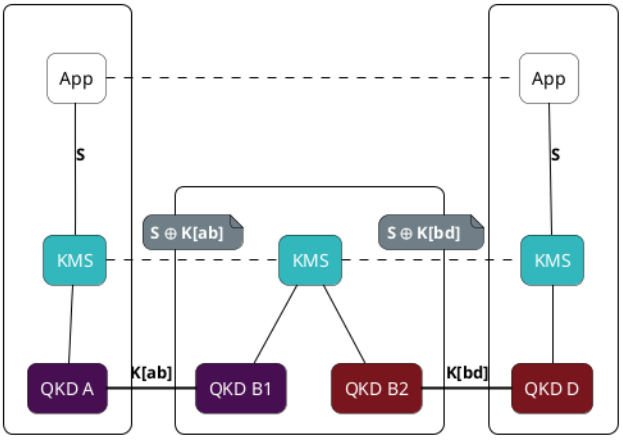


Figure 2: Outline of the *AURORA KMS* key relay mechanism feature.

5 Key management

In this section an overview of the key management features are presented.

5.1 Key Lifecycle and Reserve

The key lifecycle implementation complies with NIST SP 800-57 [5]. Keys retrieved from the QKD layer are synchronized with the peer, ensuring ITS integrity and authenticity. This key confirmation mechanism is best practice in key exchange protocols and also compliant with recommendations for key management [5].

After the keys have been confirmed on both sides, they are added to the key pool, ready for use. Then, depending on needs, a batch of this pool is dynamically allocated for internal or external use.

Key material is zeroized after it has been used or provided to the user. Metadata and the key history is maintained, for a configurable duration for audit purposes, but no key material can be derived from it.

5.2 End-to-End Key Establishment

When an application requests keys via the key provisioning interface, the KMS reserves a key batch for that pair of applications. If required, it resizes the keys to the requested size and ITS forwards them hop-by-hop, as shown in fig. 2. The forwarding mechanism is ITS encrypted, ITS authenticated and ITS integrity protected, a unique capability of this approach. The final key is obtained by a Random Number Generator. If available, a TPM 2.0 Hardware RNG is used to source the keys.

5.3 Key Reformatting

The *AURORA KMS* can reformat the received QKD keys to the Application's demands.

5.4 Group Key

The *AURORA KMS Extended* supports group keys as described in ETSI GS QKD 014 v1.1.1 [1]. The group keys are provided to multiple applications in the network and zeroized as soon as all participants have received the key.

5.5 PQC Hybridization

The *AURORA KMS Extended* can hybridize the key delivered to applications using PQC and classical algorithms as shown in fig. 3. When an application requests a key, ITS QKD key forwarding is performed as usual. An independent second channel is then established using PQC and classical cryptography. The QKD key and the secret established via the second channel are then hybridized according to NIST SP 800-56C [6].

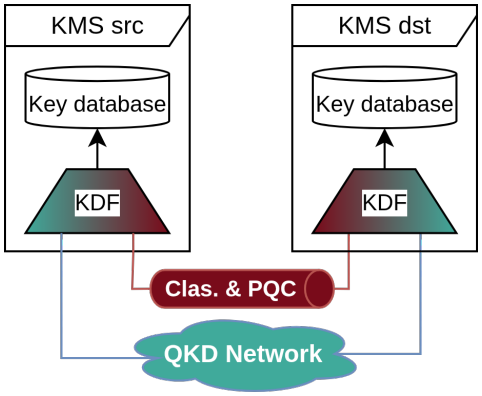


Figure 3: Outline of the PQC hybridization feature of the *AURORA KMS Extended*.

The *AURORA KMS Extended* comes with an SDN framework. This is a completely independent software stack composed of an SDN Agent and SDN Controller, following the architecture outlined in ETSI GS QKD 015 [7]. It is used to determine the key forwarding path and monitor the KPIs of the KMS layer.
It also comes with a network management WebUI, as depicted in fig. 4, allowing for remote KPI monitoring and configuration.

6 Networking

The key relay path can be statically configured. In addition, SDN aided routing is supported by the *AURORA KMS Extended*.

6.1 Static Configuration

Both versions of the *AURORA KMS* can be statically configured, which has the advantage that no additional component is required. The disadvantage though is that it cannot adapt dynamically, however, for medium networks with medium demands a static configuration is usually sufficient. A network planning tool for static configuration is provided that generates all configuration files and required certificates.

6.2 SDN Framework

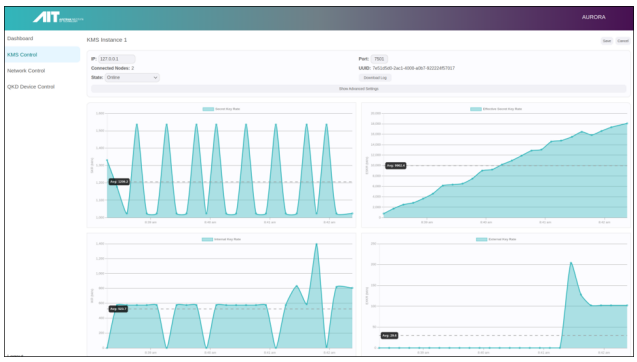


Figure 4: Screenshot of the WebUI visualizing the KPIs of one KMS, a feature of the *AURORA KMS Extended*.

6.3 Development

The *AURORA KMS* is developed following industry grade test driven development methods. The unit-test line coverage achieves 90%. Static and dynamic code analysis is performed automatically during development to detect vulnerabilities. The *AURORA KMS* is tested in simulation and integration tests. It was deployed as part of the Austrian QCI in QCI-CAT and additionally, it was deployed in Telefónica's Madrid QKD testbed and in various other exhibitions and demonstrations.

7 Details and Contact

You can find more details and news on the product page **qkd-kms.ait.ac.at**, where you can find references to publications [8, 9, 10, 11] which provide further details. You can also contact the team directly via **aurora-qci-info@ait.ac.at**.

References

[1] "Quantum key distribution (qkd); protocol and data format of rest-based key delivery api," European Telecommunications Standards Institute (ETSI), Industry Specification Groups(ISG), Group Specification ETSI GS QKD 014 v1.1.1, 02 2019.

[2] "Quantum key distribution (qkd); application interface," European Telecommunications Standards Institute (ETSI), Industry Specification Groups(ISG), Group Specification ETSI GS QKD 004 v2.1.1, 08 2020.

[3] R. Singh, C. Hill, S. Kawaguchi, and J. Lupo, "Secure Key Integration Protocol (SKIP)," Internet Engineering Task Force, Internet-Draft draft-cisco-skip-02, Sep. 2025, work in Progress. [Online]. Available: https://datatracker.ietf.org/doc/draft-cisco-skip/02/

[4] "Quantum key distribution networks – key management," International Telecommunication Union (ITU) Telecommunication Standardization Sector (ITU-T), Recommendation ITU-T Y.3803 v1.0, 12 2020.

[5] "Recommendation for key management," National Institute of Standards and Technology (NIST), Special Publication NIST SP 800-57 Part 1, Revision 5, 05 2020.

[6] "Recommendation for key-derivation methods in key-establishment schemes," National Institute of Standards and Technology (NIST), Special Publication NIST SP 800-56C Revision 2, 08 2020.

[7] "Control interface for software defined networks," European Telecommunications Standards Institute (ETSI), Industry Specification Groups (ISG), Group Specification ETSI GS QKD 015 v2.1.1, 04 2022.

[8] P. James, S. Laschet, S. Ramacher, and L. Torresetti, "Key management systems for large-scale quantum key distribution networks," in *Proceedings of the 18th International Conference on Availability, Reliability and Security*, ser. ARES '23. New York, NY, USA: Association for Computing Machinery, 2023.

[9] C. Bastos, F. Pinto, R. Bacar, G. Anjos, M. Almeida, A. Pinto, R. Chaves, T. Dias, J. Afonso, R. Calé, M. Freitas, L. Maia, L. Magalhães, A. Muñiz, R. Cantó, J. Brito, J. Ballesta, R. Méndez, S. Laschet, S. Ramacher, P. James, L. Torresetti, P. Piscione, A. Abdulwahed, P. Giardina, V. Martin, L. Ortiz, A. Pastor, N. Muga, N. Silva, D. López, M. Vieira, C. Escribano, and L. Mengal, "Discretion: First field demonstration of a quantum enabled sdn in the context of a military exercise," in *2025 International Conference on Military Communication and Information Systems (ICMCIS)*, May 2025.

[10] F. Valbusa, T. Lorünser, G. Spini, and S. Laschet, "Relaxing the single point of failure in quantum key distribution networks: An overview of multi-path approaches," in *Availability, Reliability and Security*, ser. Lecture Notes in Computer Science, vol. 15998. Springer, 2025, p. 183–200.

[11] J. Brito, J. Ballesta, R. Brito-Mendez, L. Mengual, L. Ortíz, V. Martin, R. Cantó, A. Muñiz, A. Pastor, D. Lopez, S. Laschet, S. Ramacher, P. Piscione, A. Abdulwahed, P. Giardina, M. Freitas, R. Calé, L. Maia, L. Magalhães, G. Anjos, R. Chaves, J. Afonso, P. Martins, T. Dias, F. Pinto, M. Vieira, R. Bacar, and C. Bastos, "Secure network innovation in defense: Sdn and quantum cryptography with discretion," in *2025 International Conference on Quantum Communications, Networking, and Computing (QCNC)*, 2025, pp. 261 – 268.