AIT's KMS for QKD Networks is available under a commercial software license. This document gives an overview of the offered versions and their corresponding feature set, based on the SW version `v3.0.0`.

1 AURORA KMS Versions

Two versions of the *AURORA KMS* are offered: *AURORA KMS Core* and *AURORA KMS Extended*. The *AURORA KMS Core* comes with all the features required to run in a QKD Network, while *AURORA KMS Extended* additionally provides some extended and partly experimental features. The feature sets are described in the following sections. Items highlighted with a '>' and italicized are exclusive to *AURORA KMS Extended*.

- Application interface:
  - ETSI GS QKD 014 v1.1.1 [1]
  - > *Group key according to ETSI GS QKD 014 v1.1.1 [1]*
  - > *ETSI GS QKD 004 v2.1.1 in http(s) or CoAP [2]*
  - > *CISCO SKIP*
- QKD interface:
  - ETSI GS QKD 014 v1.1.1 [1]
  - > *ETSI GS QKD 004 v2.1.1 push mode in CoAP [2, 3]*
- Key management with:
  - ITS key confirmation
  - Key reserve and dynamic key allocation based on the key pool concept
  - Secure erasure of used or provided keys
  - Key database storage in RAM or disk
  - Static key routing based on preconfigured routes
  - > *Dynamic key routing via an SDN framework*
- End-to-end ITS key establishment with:
  - ITS encryption, authentication and integrity protection
  - TLS overlay protection using preshared certificates, no PKI required.
  - TPM 2.0 support as random source (must be supported by HW platform)
  - http REST management API for basic metric extraction
  - > *PQC hybridization for keys delivered to applications*
  - > *SDN framework and frontend for remote monitoring and configuration*

1.1 The Software Delivery Option

All *AURORA KMS* versions are delivered as docker image. The user is responsible for providing an execution environment with:

- Linux based OS with docker 29 or later.
- In addition to the OS requirements the *AURORA KMS* requires:
  - 512 MB RAM
  - 1 GB disk storage (typical space for databases and logging).
  - Network interface with the ability to send/receive packets.
  - TPM 2.0 module accessible via the standard OS functionality for the *AURORA KMS* process.
- System setup requirements:
  - Each *AURORA KMS* instance must be able to reach other *AURORA KMS* instances in the network.
  - It is recommended that the *AURORA KMS* is deployed in a secure environment.
  - Ports specified in the user manual or configuration must be open.

1.2 The Hardware Delivery Option

All *AURORA KMS* versions can be delivered as a hardware integrated solution, via commercial partners. The system setup requirements are the same as for the software option.

1.3 Tooling

All versions of the *AURORA KMS* come with:

- User manual
- Configuration tool

2 Support

2.1 Support agreement

Refer to the terms and conditions of the support agreement for scope, time frame and other details. If no agreement was made, the *AURORA KMS* is delivered as is.

2.2 Technical version support

Version Upgrades: The customer can upgrade to a newer supported version of the *AURORA KMS* according to the negotiated upgrade plan.

Version Support: AIT can exclude certain SW versions from being supported. This can happen if released software versions have critical issues.

Customer POC: AIT requires a point of contact (POC), which must be updated by the customer if it changes. This is a requirement for the Secure Software Development Lifecycle. The POC is informed electronically about:

- New available *AURORA KMS* versions and their changelog.
- Discontinued *AURORA KMS* versions and a migration plan to a supported version.
- Discovered vulnerabilities in the *AURORA KMS* and a migration plan to a supported, non-vulnerable version.

3 Contact

For more information, visit our website **qkd-kms.ait.ac.at** or write an E-Mail to **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] 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.