QKD Interoperability Aspects

Project update

Ane Sanz, EHU Elisabeth Andriantsarazo, CESNET Piotr Rydlichowski, PSNC

WP6 T1 Activity

Network Technologies Workshop, online

19th March 2025

Agenda

- QKD Interoperability
- KMS project concept
- Status

QKD Interoperability

- NRENs are directly and indirectly involved in EuroQCI initiative and projects
- Both EuroQCI segments are considered – Terrestrial QCI (optical fiber based QKD transmission) and Space QCI (free space QKD transmission)
- Space QCI along with the interface to Terrestrial QCI is planned to be part of the EU-QCI infrastructure with EU-Secret classification
- National QCIs can establish independent connectivity between its NatQCI networks and as complement to EU-QCI and EuroQCI concepts
- NRENs are interested in open source KMS solutions
- From NREN point of view it would be beneficial to have independent KMS links between its QKD infrastructures for GEANT activities and technology development.

QKD Interoperability

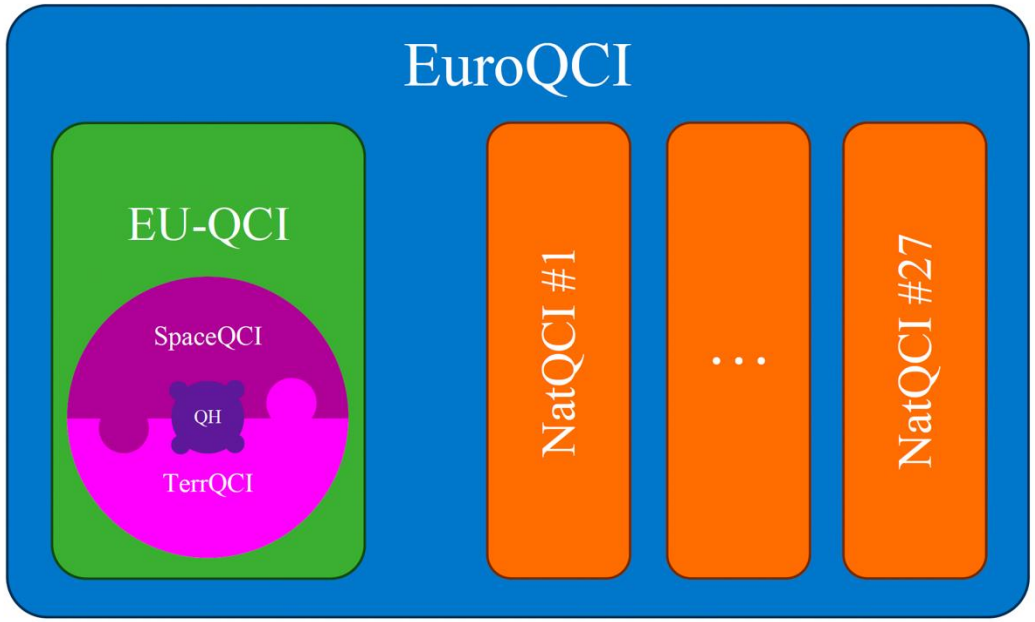


Figure 1: EuroQCI ecosystem

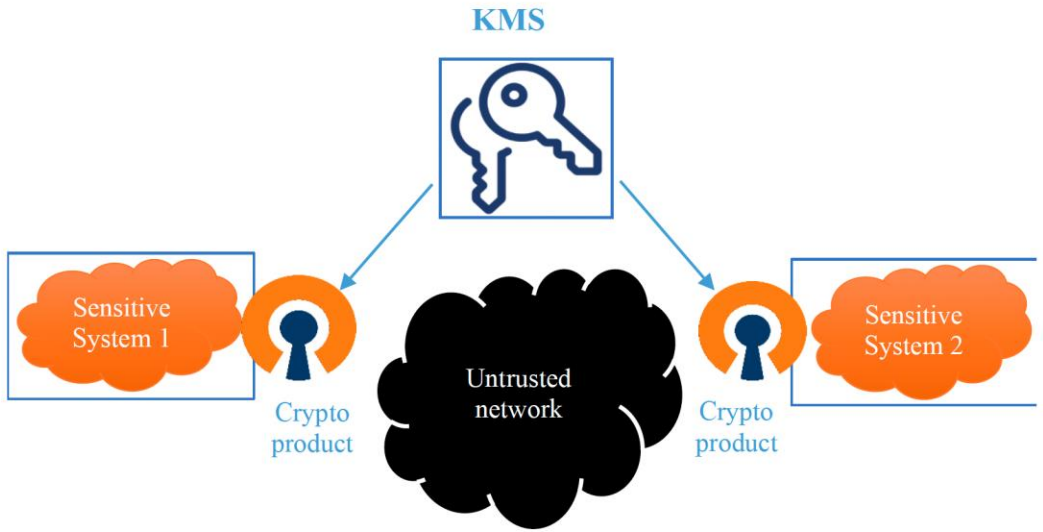


Figure 2: Cryptosystem

QKD Interoperability

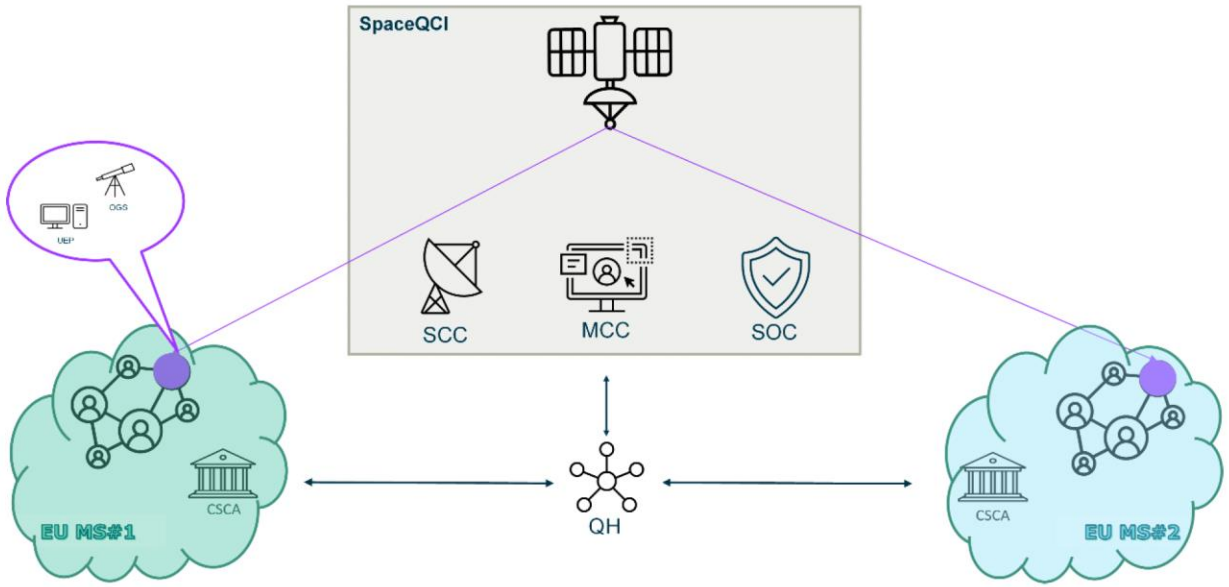


Figure 4: Overview of EU-QCI and its main elements

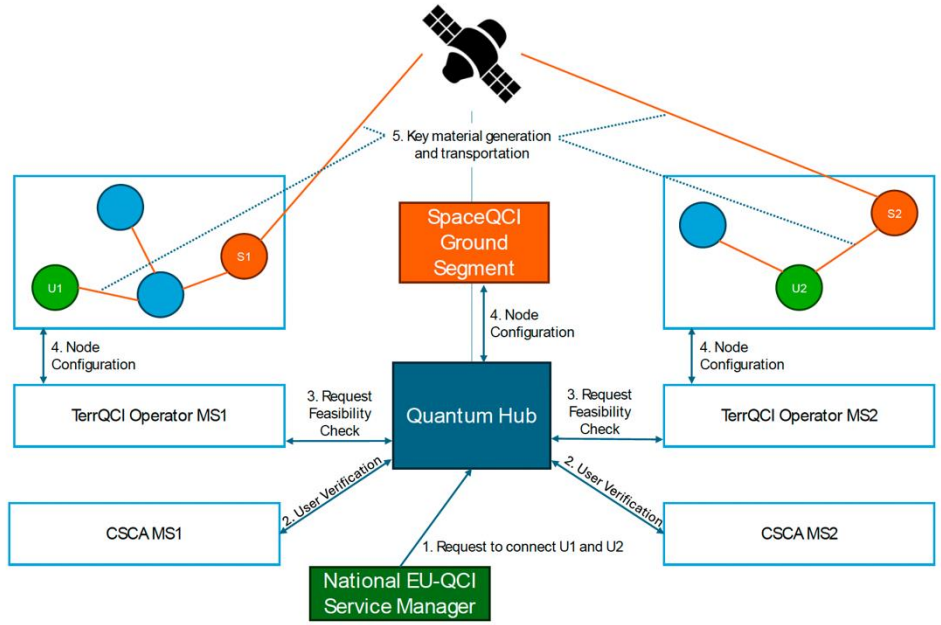


Figure 5: Delivery of Key Material to EU-QCI users via SpaceQCI and TerrQCI

QKD Interoperability

- As proof-of-concept it was agreed to establish test infrastructure between NRENs that will allow connect interoperable QKD and KMS infrastructures
- GEANT will provide Layer 3 links and services between NREN required to establish KMS connectivity. These services can also be secured by QKD services
- NRENs will use its existing QKD and KMS infrastructure to implement ETSI QKD 020 links

QKD Interoperability

portal.etsi.org/webapp/WorkProgram/Report_WorkItem.asp?WKI_ID=63115

2025-03-19 **Work Programme** Version 2.3.3

Simple Search | Advanced Search | Pre-Defined Reports | Help

Details of 'DGS/QKD-020_InteropKMS' Work Item

Work Item Reference	ETSI Doc. Number	STF	Technical Body in Charge	Standard Not Ready For Download
DGS/QKD-020_InteropKMS	GS QKD 020		QKD	
Current Status (Click to View Full Schedule)	**Latest Version**	**Cover Date**	**Standstill**	**Creation Date**
Early draft (2024-08-06)	0.4.1 Draft		View Standstill Information	2021-06-14
Rapporteur	**Technical Officer**		**Harmonised Standard**	
Martin Ward	Carmine Rizzo		No	

Title	Quantum Key Distribution (QKD); Protocol and data format of REST-based Interoperable Key Management System API Interoperable KMS API
Scope and Field of Application	This work item will specify a REST API that allows key management systems to interoperate to pass keys horizontally between two systems located in a common trusted node. The API will enable QKD networks to serve applications that request shared secret keys from key management systems that are not linked by a contiguous chain of systems from the same vendor. It is beyond the scope of the document to describe how the underlying QKD network agrees key material between nodes. URI formats, communication protocols (HTTPS), and the JSON data format encoding of posted parameters and responses (including key material) will be described. An OpenAPI description of the API will be included.
Supporting Organizations	Facultad de Informatica, University of Waterloo, ID Quantique, HUAWEI TECH. GmbH, Toshiba, BT plc, evolutionQ

Keywords	Projects	Clusters	Frequencies	Mandates	Directives
API PROTOCOL quantum cryptography Quantum Key Distribution		Security			

Official Journal

Remarks

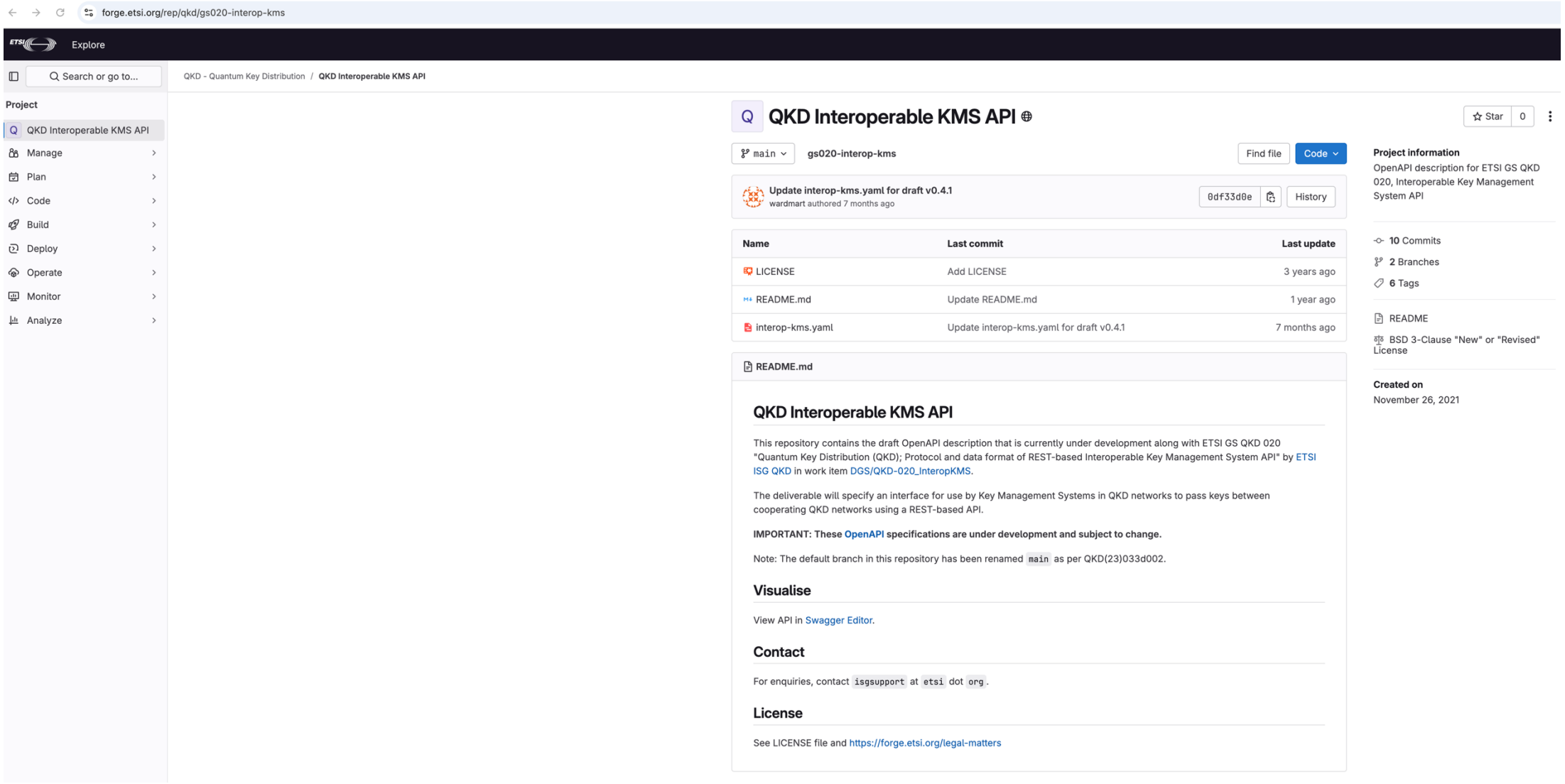
2024-08-06 wardmarti Draft contributed - V 0.4.1 contributed for Discussion in QKD(24)036c007 as Early draft
2024-08-06 WARDMARTI A new draft is uploaded - V 0.4.1 with status: Early draft
2023-11-07 wardmarti Draft contributed - V 0.3.1 contributed for Discussion in QKD(23)034f005 as Early draft
2023-11-07 WARDMARTI A new draft is uploaded - V 0.3.1 with status: Early draft
2023-05-30 wardmarti Draft contributed - V 0.2.1 contributed for Discussion in QKD(23)034012 as Early draft
2023-05-29 WARDMARTI A new draft is uploaded - V 0.2.1 with status: Early draft
2022-11-28 wardmarti Draft contributed - V 0.1.1 contributed for Discussion in QKD(22)033007 as Early draft
2022-11-28 WARDMARTI A new draft is uploaded - V 0.1.1 with status: Early draft
2021-12-15 wardmarti Early draft proposal in contribution QKD(21)031015 was Noted by QKD
2021-12-06 wardmarti Draft contributed - V 0.0.1 contributed for Discussion in QKD(21)031015 as Early draft
2021-12-06 WARDMARTI A new draft is uploaded - V 0.0.1 with status: Early draft
2021-07-14 WARDMART TB adoption of WI QKD, see contribution QKD(21)000005 in RC QKD(21)DEC013
2021-06-14 WARDMART WI proposed to TB QKD, see contribution QKD(21)000005

Specific aspects

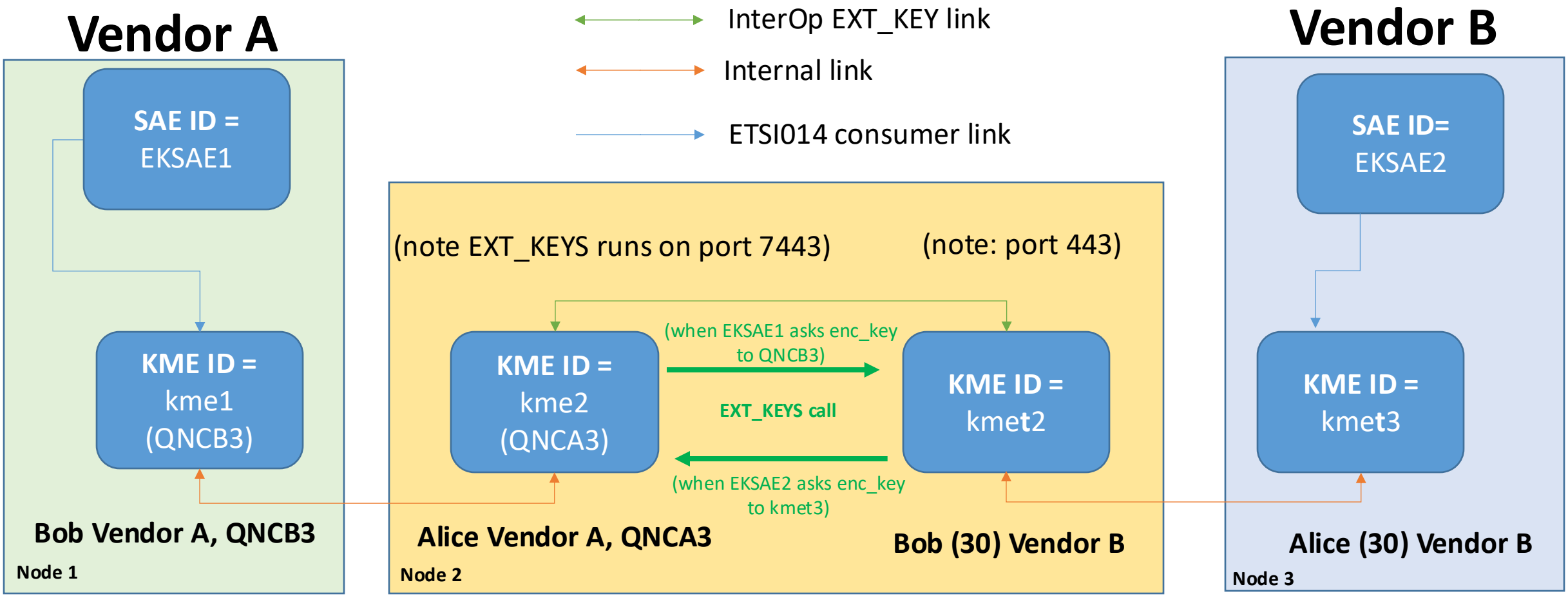
Security/Privacy aspects

Any comments or problems with this application? Please let us know...

QKD Interoperability



QKD Interoperability



QKD Interoperability

Certificates for ETSI QKD 020 tests

- *For ease, single set of certs made for **all** API calls.* This includes all IPs / host names above as SAN fields. CA is created (ca-cert.pem / ca-key.pem) and a signed cert (cert.pem/key.pem).
- All servers present cert.pem (SAN fields added for all server IPs / hostnames). Clients authenticate server by trusting ca-cert.pem since that CA issued cert.pem)
- All clients use cert.pem too. Servers authenticate clients by trusting ca-cert.pem which is what issued cert.pem. that clients use.
- (cert.pem was made with KeyUsage = clientAuth and serverAuth fields)

QKD Interoperability

Certificates for ETSI QKD 020 tests

When Alice Vendor A KME (kme2) issues EXT_KEYS to Bob Vendor B KME (kmet2):

- Vendor A is the client and needs to offer a cert to Vendor B for client auth. The cert must be signed by a CA that Vendor B trusts. For example, Vendor A could use cert.pem as the client cert to be offered and Vendor B has already set kmet2 to trust the CA that signed it (ca-cert.pem)
- Vendor B is the server and needs to offer a cert to Vendor A for server auth. The cert must be signed by a CA that Vendor A trusts. At present, Vendor B kmet2 offers cert.pem, which is signed by the CA (ca-cert.pem). Thus, Vendor A could add ca-cert.pem as a trusted CA, and then kme2 will accept kmet2 as authentic.

QKD Interoperability

Certificates for ETSI QKD 020 tests

Main Test: Use CURL to issue GET_KEY to VENDOR B's kmet3 with remote SAE ID = EKSAE1
(pass header "X-FORWARDED-FOR = EKSAE2" to spoof the curl command as if coming from EKSAE2 encryptor)

PASS if: Vendor B kmet3 returns a key/key_ID. Calling GET_KEY_WITH_KEY_ID on Vendor A kme1 return the same key for this key ID. (this indicates key has been passed correctly using EXT_KEYS at the gateway node kme2/kmet2), repeat the above for GET_KEY to Vendor A KME1 with remote SAE ID = EKSAE2)

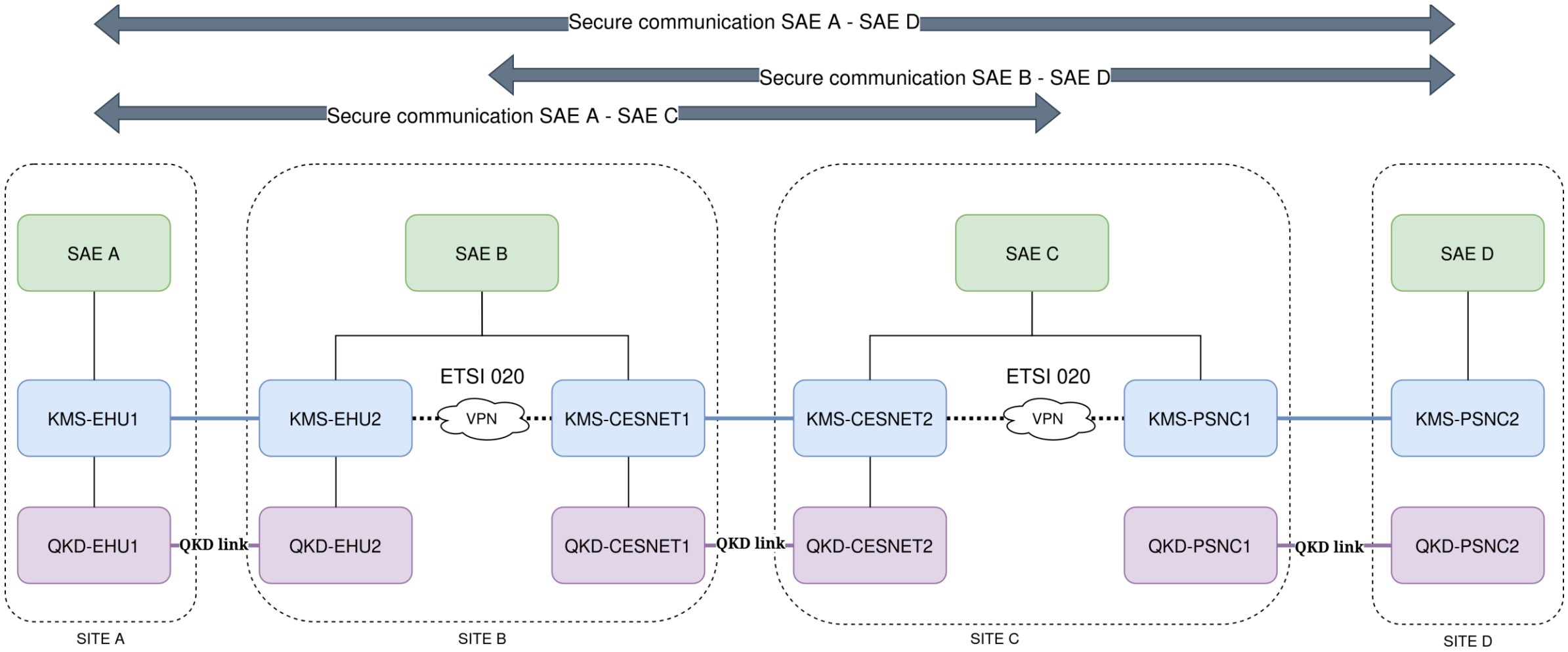
- e.g. Request from EKSAE2 SAE to get ENC key from Vendor B KME, that should pass key across the gateway using EXT KEYS

curl --cert ./cert.pem --key key.pem --cacert ca_cert.pem -H "X-Forwarded-For:EKSAE2" https://192.168.109.41/api/v1/keys/EKSAE1/enc_keys

- this results in middle Vendor B node issuing the following to middle Vendor A node (equivalent curl command below):

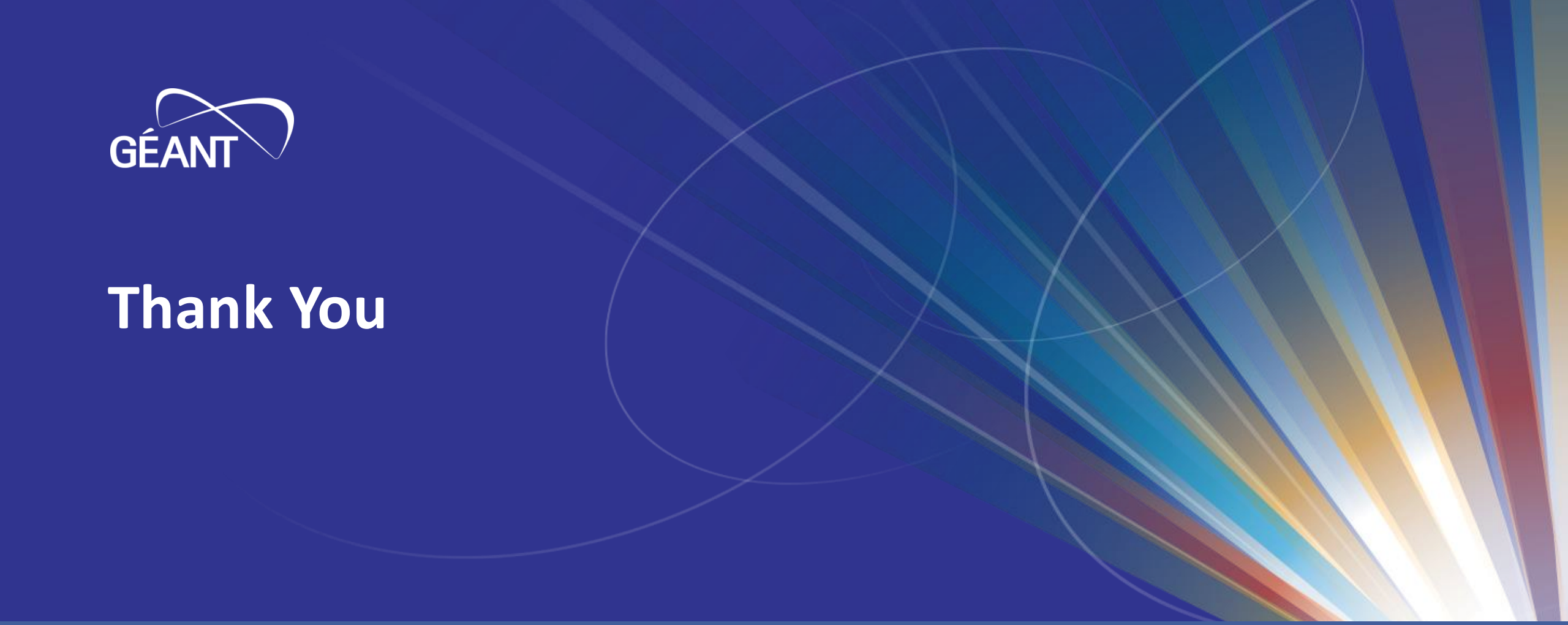
- curl -X POST --cert ./cert.pem --key key.pem --cacert ca_cert.pem -H 'Content-Type: application/json' -d '{"Keys": [{"key": "CEICeq8fqVt/hliVeN9D5BMWeujZ3Os3digzgRpxpyM=", "key_ID": "a4e56ec6-5f30-11ec-a445-6805ca95673c"}],"master_SAE_ID": "EKSAE2","slave_SAE_ID": "EKSAE1"}' https://192.168.102.32:7443/api/v1/keys/ext_keys

KMS Project Concept



Status

- KMS and QKD infrastructure is ready to be interconnected between involved NRENs
- VPN and Layer 3 links over GEANT infrastructure under preparation
- ETSI 020 test prepared and ready to be implemented
- KMS links under preparation



Thank You

www.geant.org

Co-funded by
the European Union