

Notes to the ETSI GS QKD 014 Integration into QuStream Proof of Concept

<https://research.oxfordscientific.com/qustream/etsi/qkdpoc.php>

Introduction

This document provides accompanying notes to the Proof of Concept that was conducted to integrate QuStream with a QKD implementation using the ETSI GS QKD 014 standard.

The PoC allows for a model where master and slave SAE's can be on either different ip addresses, or on the same ip address.

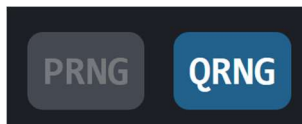
In either case, the provided example **make** commands of **make get_enc_key** and **make get_dec_key** are proxied through PHP scripts, **run_enc_key.php** for the master SAE, and **run_dec_key.php** for the slave SAE, as they would not otherwise be accessible as an external service.

Files for local installation

\PoC Files (any webserver)			
29/08/2025	10:07	1,031	get_qustream_block.php
29/08/2025	10:41	21,731	qkdpoc.php
29/08/2025	10:07	48,000,000	QRNG1.bin
29/08/2025	10:08	25,472	qustreamsquare.png
\PoC Files\Server.103 (ETSI Ref Install)			
31/08/2025	15:13	346	run_dec_key.php.php
31/08/2025	15:13	321	run_enc_key.php.php
\PoC Files\Server.104 (Proxy)			
31/08/2025	15:14	1,237	run_dec_key.php.php

<https://research.oxfordscientific.com/qustream/etsi/QuStream-PoC.zip>

Configuration Options



Select the QuStream block RNG source, either PRNG or QRNG. The QRNG is taken from a QRNG file that is part of the PoC.



VALIDATE – all data is artificially generated to validate that the PoC is installed correctly and functioning without errors in the browser instance.



ETSI TEST – a two-server implementation of QuStream integrated with ETSI QKD, where the ETSI QKD reference implementation is installed on 194.105.10.103, with the master SAE accessed via the 194.105.10.103 webservice, and the slave SAE accessed via the 194.105.10.104 webservice (which is just a proxy to the .103), in order to model separate/remote SAEs.



ETSI LIVE – amend with target ip addresses of a live QKD instance.

Initial State

ETSI GS QKD 014 Integration into QuStream Block PRNG QRNG  QuStream-QKD - Proof of Concept VALIDATE ETSI TEST ETSI LIVE

SAE A (Master) 194.105.10.103 Get Key [SAE_ID='B'] => KME A

(raw server response)

KME A Key ID:
KME A QKD Key:

SAE B (Slave) 194.105.10.104 Get Key [ThisID, KeyID=empty] => KME B

(raw server response)

KME B Key ID:
KME B QKD Key:

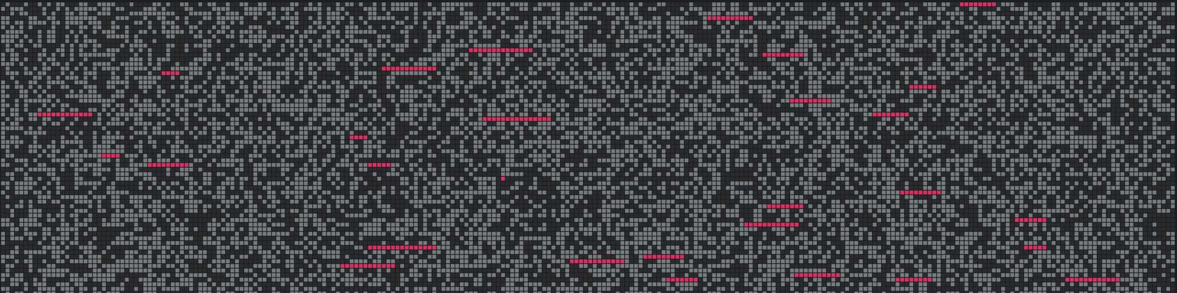
After Get Key requests for both master and slave

ETSI GS QKD 014 Integration into QuStream Block PRNG QRNG  QuStream-QKD - Proof of Concept VALIDATE ETSI TEST ETSI LIVE

SAE A (Master) 194.105.10.103 Get Key [SAE_ID='B'] => KME A

```
https://194.105.10.103/run_enc_key.php
Command: make -C /root/etsi-gs-qkd-014-referenceimplementation get_enc_key make: Entering directory '/root/etsi-gs-qkd-014-referenceimplementation' HTTP/2 200 content-length: 113 content-type: application/json date: Sun, 31 Aug 2025 13:00:52 GMT {"keys":[{"key_ID":"ce809490-5514-4057-93ad-dcaf5ce7ab1e","key":"Mgbzd0LDqXSFmFFcozFh0R+d14ziL3oF56tBeeqSKhI="}]}Strings are equal. make: Leaving directory '/root/etsi-gs-qkd-014-referenceimplementation'
```

KME A Key ID: ce809490-5514-4057-93ad-dcaf5ce7ab1e
KME A QKD Key: Mgbzd0LDqXSFmFFcozFh0R+d14ziL3oF56tBeeqSKhI=



SAE B (Slave) 194.105.10.104 Get Key [ThisID, KeyID='ce809490-5514-4057-93ad-dcaf5ce7ab1e'] => KME B

```
https://194.105.10.104/run_dec_key.php?keyid=ce809490-5514-4057-93ad-dcaf5ce7ab1e
Command: make -C /root/etsi-gs-qkd-014-referenceimplementation get_dec_key KEY='ce809490-5514-4057-93ad-dcaf5ce7ab1e' make: Entering directory '/root/etsi-gs-qkd-014-referenceimplementation' HTTP/2 200 content-length: 113 content-type: application/json date: Sun, 31 Aug 2025 13:00:54 GMT {"keys":[{"key_ID":"ce809490-5514-4057-93ad-dcaf5ce7ab1e","key":"Mgbzd0LDqXSFmFFcozFh0R+d14ziL3oF56tBeeqSKhI="}]}make: Leaving directory '/root/etsi-gs-qkd-014-referenceimplementation'
```

KME B Key ID: ce809490-5514-4057-93ad-dcaf5ce7ab1e
KME B QKD Key: Mgbzd0LDqXSFmFFcozFh0R+d14ziL3oF56tBeeqSKhI=

