Symmetric Key Exchange (SKEX)

A framework for standardizing interfaces, protocols and systems for symmetric key distribution

HotRFC, IETF 119, 18–22 March 2024, Brisbane, AU

Mattia Montagna

Problem statement

- **Asymmetric-key cryptography** is a versatile tool for securing communication but it does have some shortcomings and limitations, including:
  - It is generally **computationally intensive**
  - Its security relies on the difficulty of solving **certain mathematical problems**.
- The arrival of the quantum era is now additionally **jeopardizing the security** of key exchanges based on asymmetric cryptography:
- Several government institutions and users of cryptography have requested newer and **standardized** methods for **symmetric key exchange**.
- System integrators and architects need to be able to abstract the symmetric key distribution so that their systems do not depend on a specific vendor.
- Symmetric Key Distribution mechanisms are not yet standardized.
- Existing interface standards do not address all abstraction levels nor the range of applications.
  For example, ETSI GS QKD 014 is a high-level protocol, unsuited to internal low-level APIs.
  - Security of key management must be considered in a wide range of contexts.

Proposed Solution

- There is need to establish a framework, and potentially also protocols, describing methods used to securely exchange symmetric keys between parties.
- Define system-level APIs to decouple symmetric key providers and consumers, to ensure interoperability.
- Provide for the standardization of specific symmetric key exchange protocols for general use.
- Specify security criteria against which specific solutions are to be graded.
- Standardize specific open protocols that meet the framework criteria.

Next steps

We are asking support:

- Help organize a **BOF at IETF 120 Vancouver**
- Subscribe to **mailing list**
- Join the side-meetings in **P6-7 at 15:00–16:00 on Tuesday and Wednesday**
- Reach out to the proponents with **ideas**

Mailing list: https://www.ietf.org/mailman/listinfo/skex

Names and email addresses:

Mattia Montagna: mattia.montagna@qubridge.io
Melchior Aelmans: maelmans@juniper.net
Daniel Shiu: daniel.shiu@arqit.uk