Key Usage Limits for OSCORE

draft-ietf-core-oscore-key-limits-00

Rikard Höglund, RISE
Marco Tiloca, RISE

IETF 116 meeting – Yokohama – March 28th, 2023

Overview

- **New draft submitted as working group document**
  - Content split out from *Key Update for OSCORE (KUDOS)* (draft-ietf-core-oscore-key-update)
  - Discussed during previous core interim on 2022-09-28 [1]
  - Also discussed and confirmed during IETF 115 [2]

- **Content of the draft: AEAD Key Usage Limits in OSCORE**
  - Excessive use of the same key can enable breaking security properties of the AEAD algorithm*
  - Defining appropriate limits for OSCORE, for a variety of algorithms
  - Defining counters for key usage; message processing details; steps when limits are reached

[1] https://datatracker.ietf.org/meeting/interim-2022-core-13/session/core
[2] https://datatracker.ietf.org/meeting/115/session/core

*See also *draft-irtf-cfrg-aead-limits*

Summary and next steps

- **New document with content split from *Key Update for OSCORE***

- **Next steps**
  - Address open points
  - Follow updates to *draft-irtf-cfrg-aead-limits* and align accordingly

- **Comments and reviews are welcome!**

Thank you!

Comments/questions?