Changes between -00 and -02

- Added links to the IOTOPS mailing list and the GitHub repository.
- Made it clearer that the document focuses on comparing the security protocols and not underlying layers.
- Added a short section on underlying layers. Added references to SCHC documents.
- Changed “Conclusion” to “Summary”.
- Corrected Group OSCORE numbers.
- Added new section on EDHOC Over CoAP and OSCORE. Thanks Marco!
- Updated cTLS numbers to align with -08. Use “cTLS-08” in tables to make it clear that numbers are for -08.
  - cTLS is more stable now. Seems like cTLS will not optimize P-256/ECDSA and instead focus on x25519 and EdDSA. The impact of any cTLS changes are now much smaller than before.
- Editorial changes.

---

draft-mattsson-core-security-overhead
draft-mattsson-lwig-security-protocol-comparison
draft-ietf-lwig-security-protocol-comparison
draft-ietf-iotops-security-protocol-comparison
Early IoTDir review by Russ Housley

— Summary: Not Ready

— Major Concerns:

  — Global: The document struggles with terminology. Each of these security protocols have their own terms, which make comparison more difficult. Figure 1 shows the size of some exchanges with three flights, yet OSCORE and Group OSCORE do not really fit this model. This leads me to the conclusion that the document needs to start with a discussion of the comparison methodology.

  — Section 5: Yes, this document is purely informational. Other purely informational RFCs have useful security considerations. I agree that there is little to say here, but the Security Considerations of each security protocol could be referenced.

— Minor Concerns:

  — Section 2: I find the first paragraph hard to put in context. First, a sentence of introduction to this topic would be helpful. Why are these protocols being discussed at all? I ask because the previous section says that "overheads are independent of the underlying transport". Second, this discussion is needed at all, it might help to describe the overhead that is associated with the various underlying protocols, and then say which security protocols are used with the underlying.

  — Section 2.1: I find the section hard to put in context. A sentence of introduction would be helpful. Why is this one case explained in detail and the others not?

  — Section 3: References for the algorithms would be helpful.

— Nits:

  — Section 3.1: It says "key/certificate identifiers included" (two places). I think that "key identifiers" and "certificate identifiers" need a few words of explanation.
Next steps

- Address IoTDir comments from Russ.
- Submit -03.
- All other issues and comments have been addressed.
- More reviews, WGLC?