IPsecME WG

IETF 98, Chicago

ipsec@ietf.org

Tero Kivinen

David Waltermire

Note Well

Any submission to the IETF intended by the Contributor for publication as all or part of an IETF Internet-Draft or RFC and any statement made within the context of an IETF activity is considered an "IETF Contribution". Such statements include oral statements in IETF sessions, as well as written and electronic communications made at any time or place, which are addressed to:

- The IETF plenary session
- The IESG, or any member thereof on behalf of the IESG
- Any IETF mailing list, including the IETF list itself, any working group or design team list, or any other list functioning under IETF auspices
- Any IETF working group or portion thereof
- Any Birds of a Feather (BOF) session
- The IAB or any member thereof on behalf of the IAB
- The RFC Editor or the Internet-Drafts function

All IETF Contributions are subject to the rules of RFC 5378 and RFC 3979 (updated by RFC 4879).

Statements made outside of an IETF session, mailing list or other function, that are clearly not intended to be input to an IETF activity, group or function, are not IETF Contributions in the context of this notice. Please consult RFC 5 378 and RFC 3979 for details.

A participant in any IETF activity is deemed to accept all IETF rules of process, as documented in Best Current Practices RFCs and IESG Statements.

A participant in any IETF activity acknowledges that written, audio and video records of meetings may be made and may be available to the public.

Logistics

- Blue Sheets
- Two note takers
- One jabber scribe

Agenda

- Agenda bashing, Logistics – Chairs (5min)
- Draft status
  - Finished & Almost finished WG drafts – Chairs (5min)
  - 4307bis & 7321bis issues (10 min)
  - EdDSA – Chairs (10 min)
- Work Items
  - Split DNS (10 min)
  - Postquantum preshared keys (20min)
  - Implicit IV (20min)
- Other items
  - Minimal ESP (10 min)

Finished & Almost finished WG drafts

- Published:
  - DDoS Protection published as RFC8019
  - Curve25519 & Curve448 published as RFC8031
- Approved by IESG, but ...:
  - RFC4307bis (draft-ietf-ipsecme-rfc4307bis-17)
  - RFC7321bis (draft-ietf-ipsecme-rfc7231bis-05)
- Submitted to IESG for publication
  - TCP encaps (draft-ietf-ipsecme-tcp-encaps)

4307bis issues

- GENART, OPSDIR: Ready
- SECDIR: Has nits (typo resolved in -17)
- IESG:
  - ENCR_3DES: inconsistent SHOULD NOT or MAY
    - Table is correct: it should be MAY. Text has been wrong since -04.
    - Note that ENCR_3DES is SHOULD NOT for 7321, but MAY for 4307.
  - Some nits: fixed in unpublished -18

4307bis new issues

- New inconsistencies:
  - EcDSA based Authenticated Methods “expected downgrade” but is SHOULD and not SHOULD-
  - Digital Signatures “expects promotion” but is SHOULD and not SHOULD+
  - ecdsa-with-sha256: is SHOULD, should this be SHOULD+

7321bis reviews

- GENART: Ready with nits
- SECDIR: Has nits
- OPSDIR: in review (overdue)

7321bis IESG issues

- IESG:
  - This document obsoletes RFC7321 on the “cryptographic recommendations only.”
    - Remove “cryptographic” qualifier?
  - If manual keying is used anyway, ENCR_AES_CBC MUST be used.
    - This needs to be fixed.
  - AUTH_NONE clarification “MUST / MUST NOT” and AUTH_NONE intermixed with NULL
  - Add note on renaming some algorithms from 7321 to their IANA names in introduction
  - NITS: “Interoperability with IoT” is unclear
  - Request to clarify not listed entries MAY be used?

EdDSA

- Working group last call done
  - Issues raised:
    - Whether to use 0 or next available number for “Identity” hash algorithm.
      - Mailing list seemed to favor next available number over 0
  - Quick poll here
    - In favor of using 0 vs in favor of using next available number?
- Next steps
  - Will confirm poll on the mailing list, revise document, submit to IESG for publication

Work items: Split DNS

- Adoptation call done, should be ready
- Needs more reviews.

Split DNS

- Updates in last version
  - Requesting limited domains removed
  - INTERNAL_DNS_DOMAIN on sender is 0 size
  - Local policy clarificatins
  - Remove requirement for Child SA for DNS server IPs

Split DNS open issues

- Sync CFG_REQUEST/CFG_REPLY requirements to comply to RFC-7296
- Sync ATTRIBUTE sending to comply to RFC-7296
- No consensus on language on reconfiguring DNS on connect/disconnect

Work items: Postquantum preshared keys

- Adoptation as WG document done

Work items: Implicit IV

- Needs more reviews