RFC 4895bis: SCTP Authentication

draft-ietf-tsvwg-rfc4895-bis-04

Michael Tüxen (tuexen@fh-muenster.de)
Randall Stewart (randall@lakerest.net)
Peter Lei (peterlei@netflix.com)
Hannes Tschofenig (hannes.tschofenig@gmx.net)

Status (I)

- draft-tuexen-tsvwg-rfc4895-bis-00
  Submit RFC 4895 as an ID.
- draft-tuexen-tsvwg-rfc4895-bis-01
  Update to xmlv3.
- draft-tuexen-tsvwg-rfc4895-bis-02
  Wordsmithing and updating references.
- draft-tuexen-tsvwg-rfc4895-bis-03
  Minor editorial change.
- draft-tuexen-tsvwg-rfc4895-bis-04
  Add socket API related updates required for DTLS/SCTP.
- draft-tuexen-tsvwg-rfc4895-bis-05
  Remove ekr from list of authors, improve socket API.
- draft-tuexen-tsvwg-rfc4895-bis-06
  Update Acknowledgements.

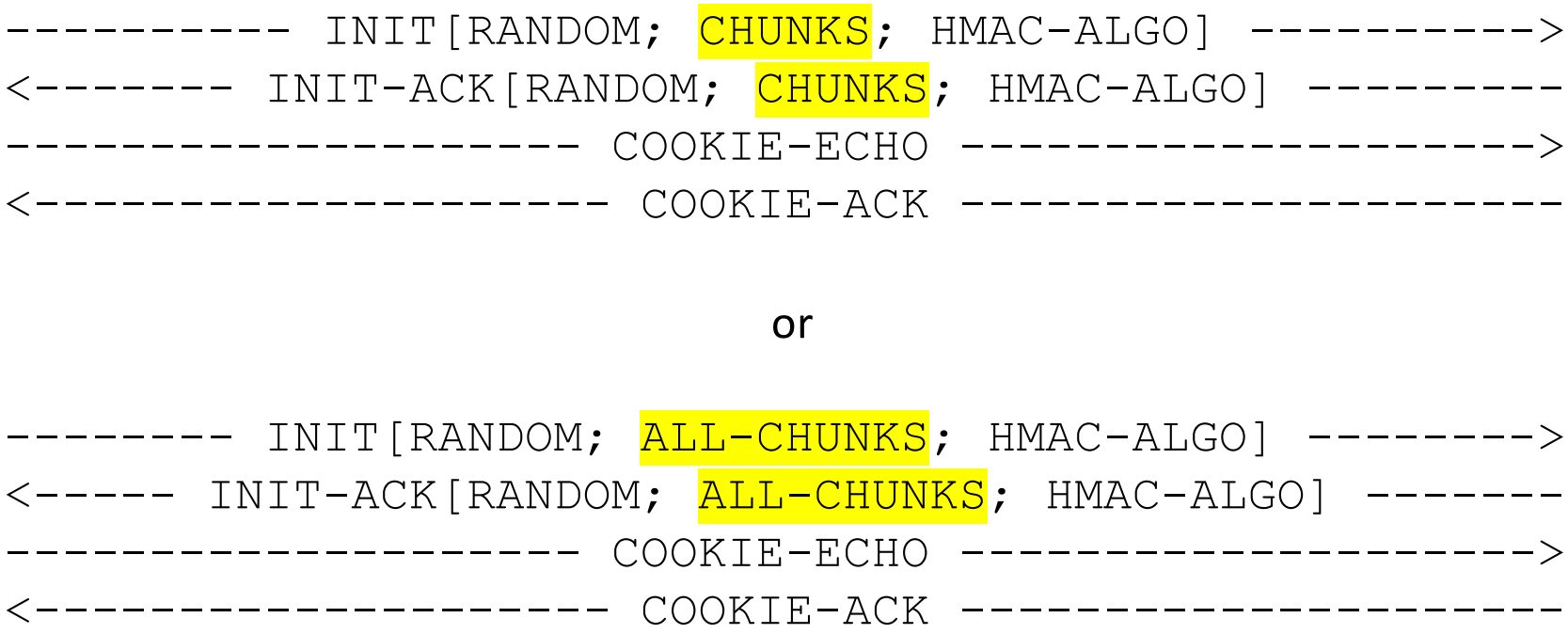
Status (II)

- draft-tuexen-tsvwg-rfc4895-bis-00
  Same as draft-tuexen-tsvwg-rfc4895-bis-06.
- draft-tuexen-tsvwg-rfc4895-bis-01
  Incorporate draft-nagesh-sctp-auth-4895bis-00, editorial changes, update IANA section.
- draft-tuexen-tsvwg-rfc4895-bis-02
  Introduce directional keys.
- draft-tuexen-tsvwg-rfc4895-bis-03
  Deprecate Unsupported HMAC Identifier Error Cause, various editorial improvements (thanks to Timo Völker!)
- draft-tuexen-tsvwg-rfc4895-bis-04
  Add support for the ALL CHUNKS parameter, editorial improvements.

Legacy Mode

- Allows to communicate with RFC 4895 implementations.
- Must be enabled by the upper layer, disabled by default.
- If enabled, the HMAC ALGO parameter sent contains the connectionless SHA-1 algorithm and possibly the connectionless SHA-256 algorithm.
- Will be used only if the peer only supports directionless SHA-1 or directionless SHA-256.

Typical SCTP AUTH Handshake



or

ALL CHUNKS parameter

- Equivalent to a CHUNKS parameter listing all 256 chunk types except INIT, INIT ACK, SHUTDOWN COMPLETE and AUTH, which length is 256 – 4 + 4 = 256 bytes.
- Length is only 4 bytes.
- Must only be used if the peer is not in legacy mode.

Improved Replay Protection

- Use an extended AUTH chunk also containing a 64-bit sequence number.
- Use would be mandatory if not in legacy mode.
- Does the size of the replay window needs to be specified? This is not done by DTLS and IPSec.

Next Steps

- Potentially integrate improved replay protection.
- Use a formula-based description instead of a text based one.
- Generalize in the text HMAC to MAC.
- Add more algorithms. Which ones?
- Address all upcoming comments.