Bootstrapping TESLA

IETF #61 Washington, D.C., 2004

Steffen Fries
Siemens AG, Corporate Technology, CT IC 3
81730 Munich, Germany
Tel: +49 89 636 53403 E-mail: steffen.fries@siemens.com

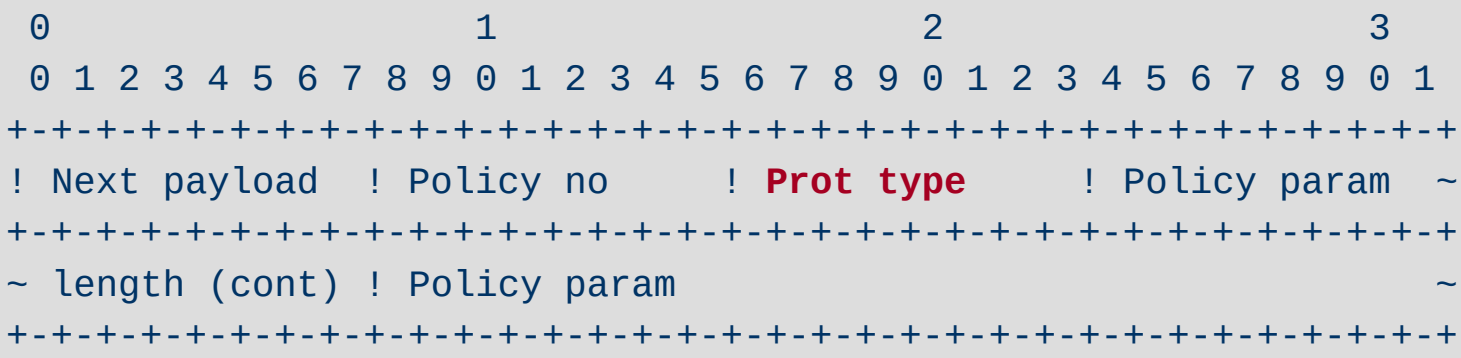
draft-fries-msec-bootstrapping-tesla-00.txt

Overview

- TESLA – Timed Efficient Stream loss-tolerant Authentication
  - scheme for source authentication in multicast communication
  - draft-ietf-msec-tesla-intro-03.txt
- TESLA – SRTP
  - Usage of TSLA within SRTP
  - draft-ietf-msec-srtp-tesla-01.txt
- Key Management for TESLA not addressed so far
  - Draft provides solution based on MIKEY
  - Uses security properties of MIKEY to protect TESLA parameter transport
- Defines new Security Policy Payload within MIKEY
- Uses General Extension Payload for TESLA key transport

Security Policy Payload in MIKEY

- TESLA parameter to be transmitted (11) defined in TESLA – SRTP draft
- Definition of new Security Policy Payload for MIKEY:



- New Protocol Type Definition (defines the supported security protocol):

Prot type	Value	
SRTP	0	→ already defined in RFC3830
TESLA	**1**	

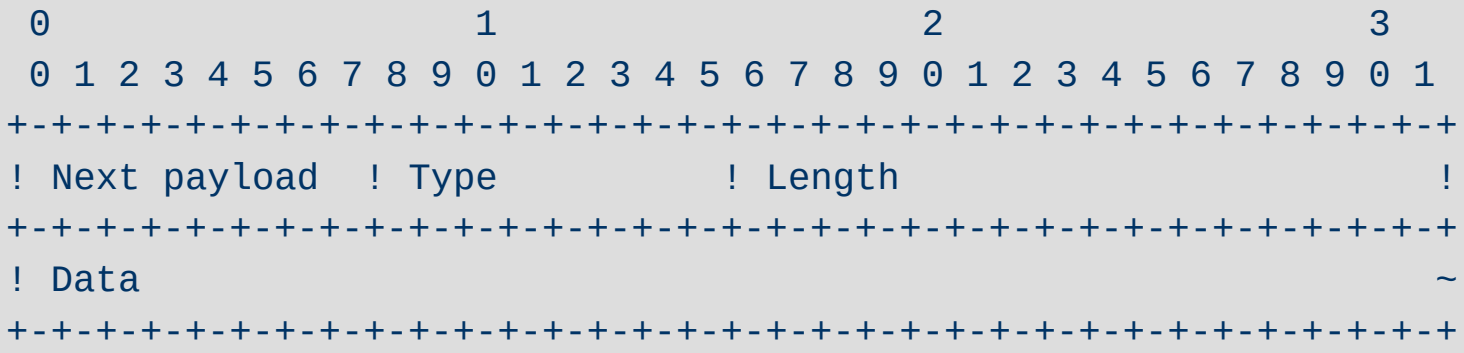
TESLA Policy Parameter Transport in MIKEY

- TESLA policy payload:

```
Type | Meaning
-----------------------------------------------
   1 | PRF identifier for f, realizing F(x)
   2 | Length of PRF f output
   3 | PRF identifier for f', realizing F'(x)
   4 | Length of PRF f' output
   5 | Identifier for the TESLA MAC
   6 | Length of TESLA MAC output
   7 | Start of session
   8 | Interval duration T_int (in msec)
   9 | Key disclosure delay d
  10| Key chain length (number of intervals)
  11| local timestamp media receiver t_r
```

Security Policy Payload in MIKEY

- Disclosed Key Data Transport in General Extension Payload



- New Data Type Definition:

Type	Value	Comments
Vendor ID	0	Vendor specific byte string
SDP IDs	1	List of SDP key mgmt IDs
TESLA I-Key	**2**	**TESLA initial key**

Mailing List Discussion

- Time Synchronization
  - TESLA requires loosely synchronized clocks between sender and receiver
  - Receiver must be able to determine lag between sender's and his clock
  - This may be achieved by using
    - NTP (recommend to be used already in MIKEY)
    - Piggybacking time sync information within MIKEY
      (may depend on the direction of session establishment)

```
MIKEY initiator message: [MIKEY parameter incl. local timestamp (t_r)]

  ------------------>

MIKEY responder message: MIKEY parameter incl. local timestamp (t_s),
  TESLA policy payload, received local time stamp t_r]

  <------------------

Receiver sets D_t = t_s - t_r + S
```

  - Proposal: Use out of band time synchronization using NTP or SNTP

Next Steps

- Discussion about merging this draft with TESLA – SRTP
  - May bind the bootstrapping to SRTP usage
  - On the other hand, SRTP is the only use case for the MIKEY bootstrapping so far
- Adoption as WG item?