SDP Attributes for ZRTP

draft-zimmermann-avt-zrtp-02.txt

Phil Zimmermann <prz@mit.edu>
Alan Johnston <alan@sipstation.com>
Jon Callas <jon@pgp.com>

ZRTP Flag Attribute

- a=zrtp
- Used to signal support for ZRTP
  - Discovery
- Can be media level or session level
- SHOULD be included by all ZRTP endpoints in offers and answers

ZRTP SAS and SASvalue Attributes

- a=zrtp-sas and a=zrtp-sasvalue
- Media level attribute
- Used to convey ZRTP Short Authentication String (SAS)
  - a=ztrp-sas conveys it in same format SAS was rendered to user (i.e. base32 or other)
    - Can be used by users to compare with GUI display when no GUI is available.
  - a=zrtp-sasvalue conveys last 32 bits of SAS in hex form, independent of how rendered to user
    - Useful for automated authentication by endpoints or servers.
- Conveyed in offer/answer exchange subsequent to successful ZRTP exchange

Security

- Attributes do not need confidentiality
  - SAS is computed from public values and is not a secret.
- Attributes need integrity protection to be relied upon for authentication
- As such, attributes should be sent even when confidentiality and integrity not available
  - Logging, confirmation, etc.

Example - Initial O/A exchange

```
v=0
o=bob 2890844527 2890844527 IN IP4 client.biloxi.example.com
s=
c=IN IP4 client.biloxi.example.com
a=zrtp
t=0 0
m=audio 3456 RTP/AVP 97 33
a=rtpmap:97 iLBC/8000
a=rtpmap:33 no-op/8000
```

Example - O/A Exchange after ZRTP

```
v=0
o=bob 2890844527 2890844528 IN IP4 client.biloxi.example.com
s=
c=IN IP4 client.biloxi.example.com
a=zrtp
t=0 0
m=audio 3456 RTP/AVP 97 33
a=rtpmap:97 iLBC/8000
a=rtpmap:33 no-op/8000
a=zrtp-sas:opzq
a=ztrp-sasvalue:45e387ff
m=video 51372 RTP/AVP 31 33
a=rtpmap:31 H261/90000
a=rtpmap:33 no-op/8000
a=zrtp-sas:qvjj
a=ztrp-sasvalue:5e017f3a
```

Note: There is an error in SAS examples in draft

Note: Media lines could be promoted to SAVP

Next Steps

- Appendix A eventually split out into separate MMUSIC I-D for IANA registration