

SFRAME + MLS

draft-barnes-sframe-mls-00

Richard Barnes, Raphael Robert

DTLS-SRTP => MLS-SFRAME

SFrame needs keys, algorithms, etc.

MLS provides authenticated key exchange & parameter negotiation

Prior art: DTLS-SRTP uses DTLS to set up SRTP encryption

MLS is a better fit for conferencing scenarios because it does **groups**

The working group will define a **mechanism for doing SFrame encryption using keys from MLS**, including, for example, the derivation of SFrame keys per MLS epoch and per sender.

DRAFT-BARNES-SFRAME-MLS

Draft does two things:

1. Define how you take keys from MLS and use them in SFrame
2. Define how you negotiate SFrame parameters in MLS

KEYS

SFrame needs: KID -> key mapping

... and per-sender keys to avoid nonce reuse

MLS provides a sequence of group keys, one per “epoch”

This draft defines

- How you derive per-sender keys from the group key
- How you create a KID for the key from (epoch, sender_id)

KEYS

Per-sender keys KDF'ed from the group key

```
sframe_epoch_secret = MLS-Exporter("SFrame 10 MLS", "", AEAD.Nk)
```

```
sender_base_key[index] = HKDF-Expand(sframe_epoch_secret,  
                                     encode_big_endian(index, 8), AEAD.Nk)
```

KIDs carry sender index + the bottom E bits of epoch (=> roll-over)

$$\text{KID} = (\text{sender_index} \ll E) + (\text{epoch} \% (1 \ll E))$$

OTHER PARAMETERS

```
uint16 SFrameCipherSuite;
```

```
struct {  
    SFrameCipherSuite cipher_suites<0..255>;  
} SFrameCapabilities;
```

Offer in KeyPackage

```
struct {  
    SFrameCipherSuite cipher_suite;  
    uint8 epoch_bits;  
} SFrameParameters;
```

Params in Welcome

STATUS + TODO

Key management implemented in <https://github.com/cisco/sframe>

Might add some recommendations about MLS groups used for SFrame

E.g., associating a temporary MLS group with a more permanent one

Mostly just needs to stay current with SFrame as it evolves

ADOPT?