

Key Management Extensions for SDP and RTSP

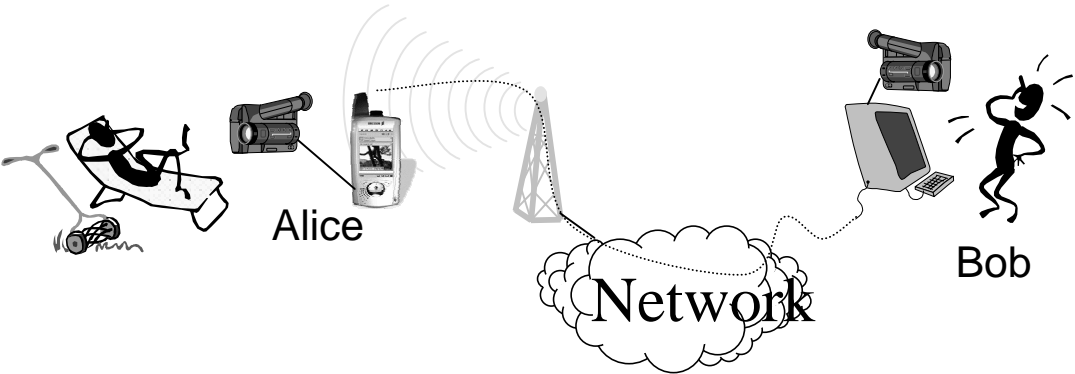
`<draft-ietf-mmusic-kmgmt-ext-00.txt>`

Background

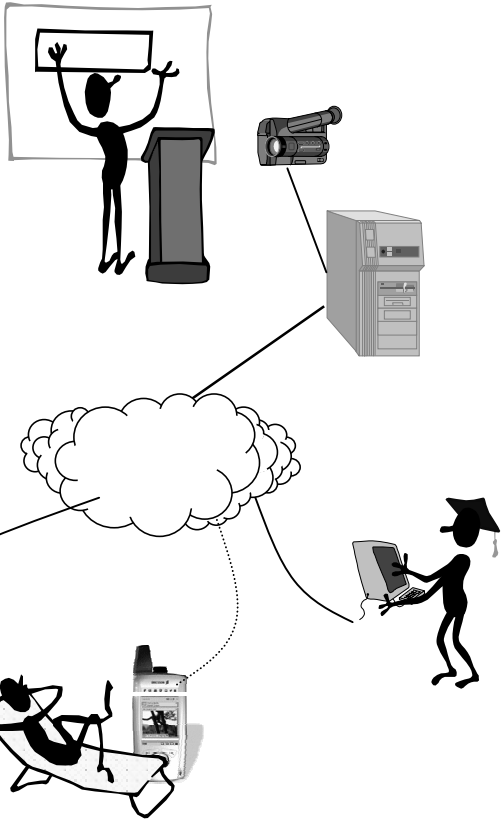
- Draft “Key Management for Multimedia Sessions” at the 51st IETF
- Work split between MSEC WG an MMUSIC WG
 - Extensions to SDP and RTSP in MMUSIC WG
 - Security part in MSEC WG (“MIKEY: Multimedia Internet KEYing”, draft-ietf-msec-mikey-00.txt)

Scenarios

SIP call



RTSP



Extensions

- MUST support a 1-roundtrip protocol
- Created to have a small impact on current SDP, RTSP, and SIP implementations
- Let the key management protocol do the work of parsing etc!

SDP extensions

- Three new attributes

`a=keymgmt-prot:<protocol name>`

e.g. MIKEY

`a=keymgmt-data:<data>`

the actual key management data (base64-encoded recommended)

`a=keymgmt-auth:<auth-data>`

extended authentication data

SDP example

Applies to
all streams

```
a=keymgmt-prot:MIKEY
a=keymgmt-data:uiSDF9sdhs727ghsd/dhsoKkdOokdo7eWsnDSJD...
m=audio 49000 RTP/SAVP 98
a=rtpmap:98 AMR/8000
m=video 2232 RTP/SAVP 31
```

Applies to
one stream

```
m=audio 49000 RTP/AVP 98
a=rtpmap:98 AMR/8000
m=video 2232 RTP/SAVP 31
a=keymgmt-prot:MIKEY
a=keymgmt-data:uiSDF9sdhs727ghsd/dhsoKkdOokdo7eWsnDSJD...
```

RTSP extensions

- One new header
 - use in ANNOUNCE, SETUP, PLAY, RECORD, SET_PARAMETER, GET_PARAMETER, OPTIONS

```
KeyMgmt      = "KeyMgmt" ":" [stream-url] protocol data [auth]
```

```
stream-url   = "url" "=" url ";"
```

```
protocol     = "Prot" "=" prtcl-name
```

```
data        = ";" "Data" "=" string
```

```
auth        = ";" "Auth" "=" string
```

```
string      = 1*(alpha-numeric|SAFE|"=")
```

How to use the attributes

SIP

- SDP in INVITE message + OK message
- Re-keying by sending a re-INVITE

RTSP

- Initial key management message created by server
 - Sent in SDP (e.g. via response to Describe or via HTTP)
- Response, in the new RTSP header (SETUP or PLAY)

The End

- Questions and Comments?

- How to proceed?