



SDP Specification Update

Colin Perkins

<http://csparks.org/>

Status

- draft-ietf-mmusic-sdp-new-13 submitted in late May
 - Attempt to clarify when it is appropriate to use "k="
 - Deprecate unregistered "x-" attributes and media formats
 - Descriptive text and IANA Considerations sections were inconsistent previously
 - Clarify that RTP can use non-contiguous ports
 - To match changes in RTP specification since RFC 1889
 - Clarify that "a=charset" is a session level attribute
 - Edit IANA Considerations text for clarity
 - Update references
- A few minor comments on the mailing list
- IESG review found a number of issues
 - Full set sent to the mailing list yesterday
 - Looking for input today...

Issues raised on the mailing list (1)

- Inconsistency between ABNF definition of token-char and the comment following it (Pekka Pessi)
 - Affects "m=", "a=", "k=", "c=" and "b=" lines
- Two options:
 1. Leave ABNF as-is, and change the comment
 2. Update the ABNF for token-char, making the following legal:

0x22 0x2f 0x3d 0x3f 0x5b 0x5d 0x5c
" / = ? [] \

⇒ Opinions from implementers?

Issues raised on the mailing list (2)

- Clarify use of "b=" with layered coding (Belling Thomas)
- For the CT modifier add:

For RTP, if several RTP sessions are part of the conference, the conference total refers to total bandwidth of all RTP sessions.

⇒ Accept?

Issues raised on the mailing list (3)

- Clarify which ports are associated with which "m=" line, with layered coding (Belling Thomas).
- In the definition of "m=" change:

For RTP, the default is that only the even numbered ports are used for data and the corresponding one-higher odd port is used for **the RTCP belonging to this RTP session, and the <number of ports> denotes the number of RTP sessions.**

⇒ Accept

IESG comments (1)

- The "k=" field is under-specified
- Should it be deprecated and/or replaced by the work in sdescriptions or key-mgmt?

⇒ Opinions from implementers?

IESG comments (2)

Specify that, when using "k=":

"ensure that the secure channel is with the party that is authorized to join the session, not an intermediary"

"If a caching server is used, there ought to be a way to keep the server from accessing the key"

⇒ Good points, need to be specified by users of SDP?

IESG comments (3)

Regarding "k=":

"Also, it is generally a good idea to indicate the algorithm that a cryptographic key is intended to support. I suggest that the encryption key type be revised to specify the key as well as the algorithm that the key will be used with."

⇒ Implied by the URI reference or media protocol

"Finally, many security protocols require two keys, one for confidentiality and another for integrity. This specification does not support the transfer of two keys."

⇒ use sdescriptions or key-mgmt if this is important

IESG comments (4)

Two suggested additions to "k=":

"name the key without actually including the key. In PEM (see RFC 1040), the Recipient-ID was used to name key-encryption keys, and a similar scheme could be employed here."

"would be nice to encrypt the session key in a key that is not included in SDP. PEM also includes a mechanism for wrapped symmetric keys."

⇒ Use sdescriptions or key-mgmt if this is important

IESG comments (5)

In security considerations: SHOULD NOT automatically drop you into an interactive session ⇒ MUST NOT

⇒ Accept

IESG comments (6)

Regarding "c=":

Just as a query, has anyone considered using a specific marker of private address realms for SDP? That is, using a network type other than IN to indicate that the domain name or address given are not globally unique/globally reachable?

⇒ Reject; Interesting, but not backwards compatible

IESG comments (7)

"The text on internationalisation says UTF-8 only applies to informational fields. Does this mean it isn't required to perform any normalization whatsoever on the UTF-8? Would it make sense to explicitly state that normalization isn't needed."

⇒ Seek clarification...

IESG comments (8)

For "a=inactive"

It was suggested apps use something like "sdp.inactive" so that the .inactive TLD could reinforce the a=inactive flag. In that instance, would the presence of that TLD be a condition under which the RTCP SHOULD is appropriately not done, and no RTCP sent? If so, is mentioning that case appropriate here?"

⇒ Note that it might be appropriate to set the "c=" line for inactive media to indicate no transport address. Specify in the users of SDP?

IESG comments (9)

- The "u=" and "k=" lines assume that the URI can be de-referenced. This is not always the case; so we may need to explicitly state the assumption
- The URI for "k=" only makes sense for particular types of URI. Might give guidance that this is typically an http or https URI?

⇒ Accept both

The way forward

- Summarise these slides and discussion to the list...
- Incorporate comments into a -14 revision in the next couple of weeks – **please give feedback!**
- Discuss with IESG and resubmit...