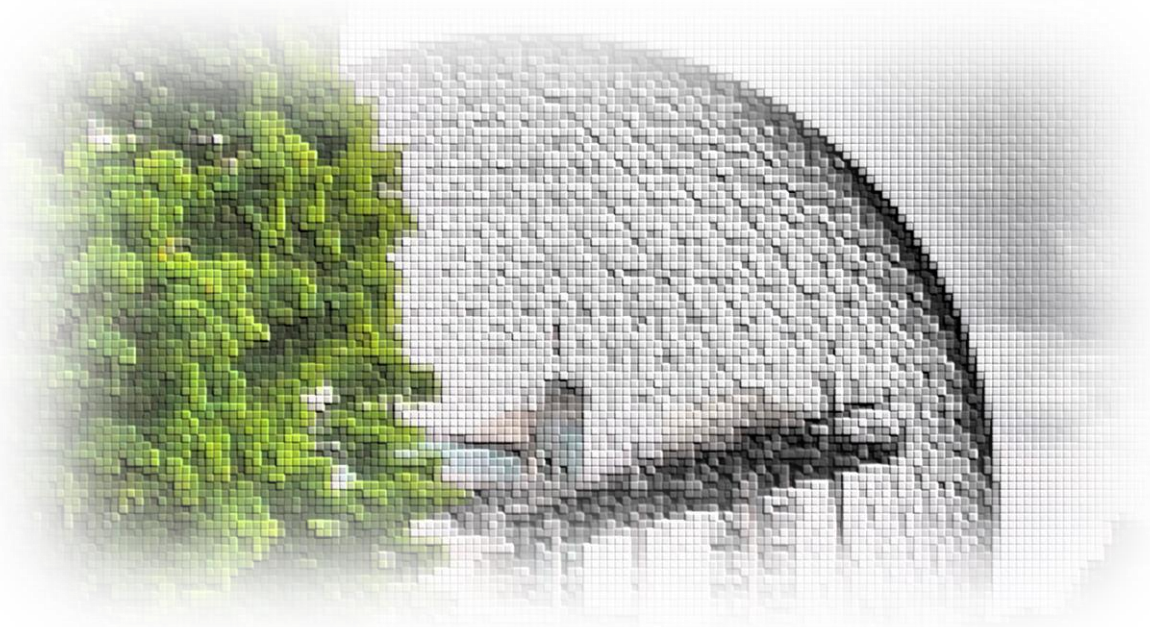
SDP Identity Attribute

IETF#102
Montreal, Canada
draft-ietf-rtcweb-security-arch

christer.Holmberg@ericsson.com



BACKGROUND & ASSUMPTION

BACKGROUND:

- Some issues and questions related to the SDP Identity attribute were raised in the SDP directorate review of the attribute
  - https://www.ietf.org/mail-archive/web/rtcweb/current/msg17124.html

ASSUMPTION:

- The SDP Identity attribute is a generic attribute, that can be used to carry identity assertions in different environments
  - Not WebRTC specific

ISSUE: Non-fingerprint based identity assertion?

QUESTION:

— Is it allowed to use some other information than fingerprint to create the identity assertion?

ANSWER:

— From a protocol perspective, it is allowed to use other information

— Outside the scope of the rtcweb draft

WAY FORWARD:

— Indicate that it is allowed to user other information than fingerprint to create identity assertions

— Indicate that the associated procedures, JSON structure for the Identity attribute value etc must be defined

ISSUE: Updated identity

QUESTION:

- Is it allowed to update the identity in a subsequent offer/answer?
  - Could happen e.g., in a call transfer scenario where an endpoint receives a subsequent offer with SDP information associated with a new peer

ANSWER:

- From a protocol perspective, it is allowed to update the identity
- May not be supported by the receiver
  - WebRTC does not allow updating the identity of the peer

WAY FORWARD:

- Indicate that it is allowed to update the identity in a subsequent offer or answer
- Indicate that, if the receiver does not support the update, it must not accept the offer or answer

THE WAY FORWARD

- Create Pull Request(s)
  - Fix/clarify the technical issues
  - Adopt “template” for SDP attributes
    - Sending initial offer, Sending answer, etc.

- Existing Pull Request for related issues
  - https://github.com/rtcweb-wg/security-arch

THE END