Requirements for Private Media in a Switched Conferencing Environment

(draft-jones-avtcore-private-media-reqts-01)

IETF 92 / March 2015

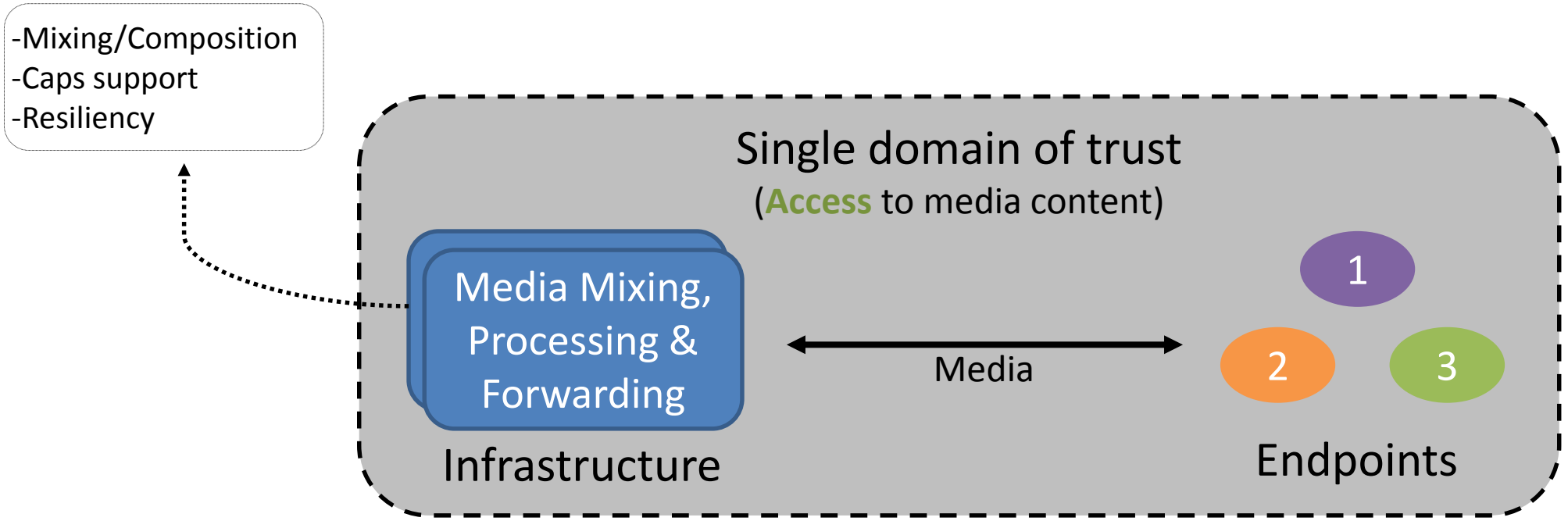
Paul E. Jones
Cisco

John Mattsson
Ericsson

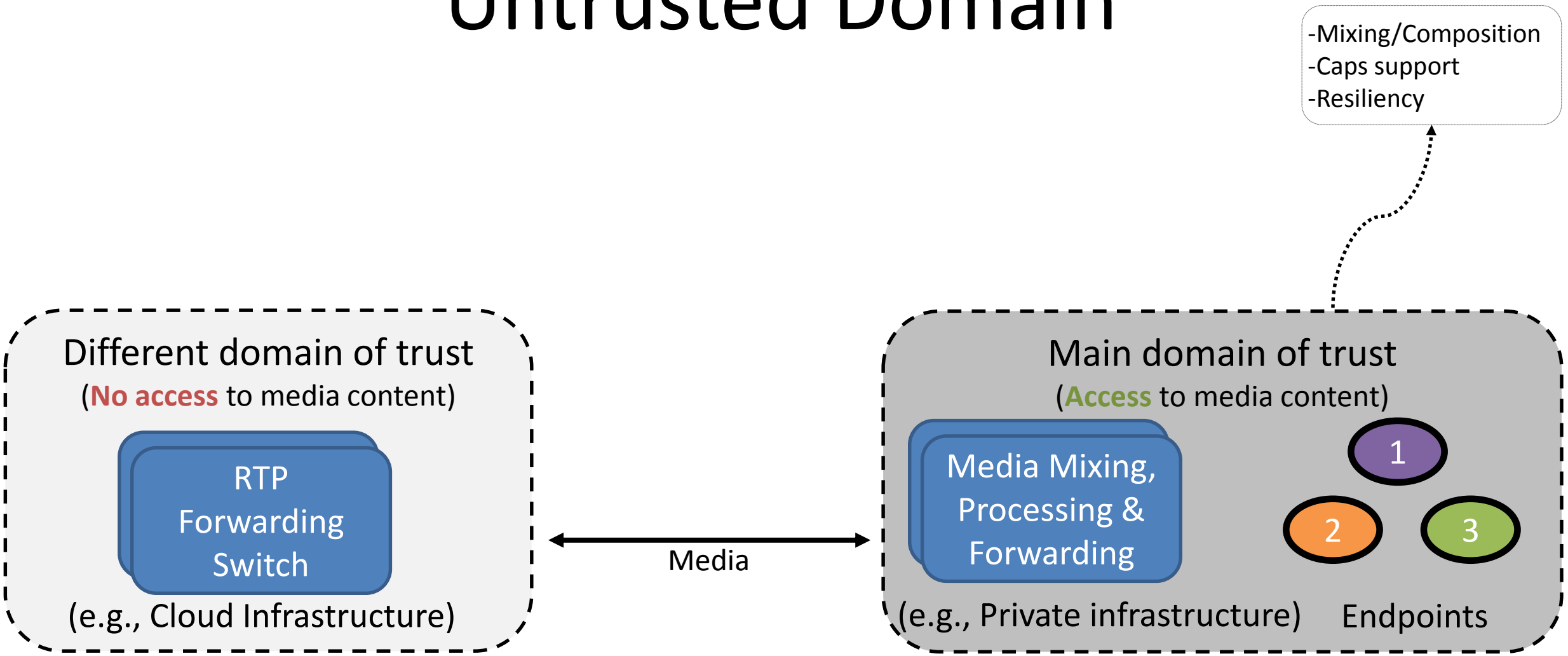
Agenda

- What this work is about
- High-level changes
  - Terminology
  - Trust model
- Discussion/Questions

Traditional Conferencing



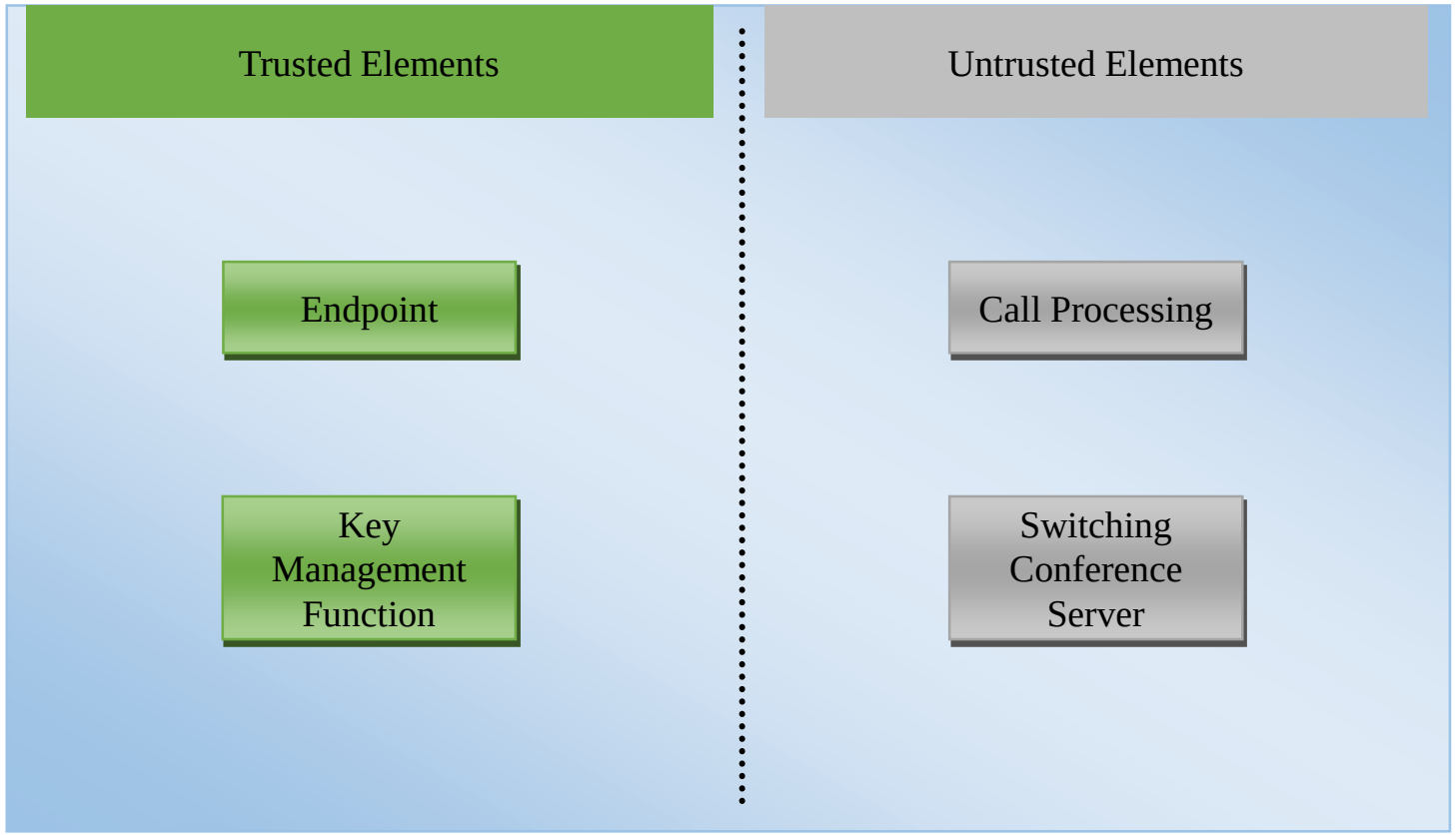
Switched Conferencing in an Untrusted Domain



High-Level Overview of Changes

- Terminology section
  - Added “media content” as a term
- Added a significantly expanded “trust model” section
- Made changes to the language of nearly every requirement
- Added a new requirement related to congestion control

Trust Model



- Elements on the left are trusted
- Elements on the right are not trusted
- It is not the intent to preclude a call processing function or switching conference server from being placed in the trusted domain, but we do not want to assume either is needed

Questions

- PM-06 points out that the SRTP crypto context is dependent on SSRC, ROC, and packet sequence numbers.
  - To be neutral to other potential mechanisms, should we re-word PM-06 as:

    A cryptographic context suitable for enabling end-to-end authenticated encryption MUST be defined. Note that in SRTP, the cryptographic context includes the SSRC, sequence number and rollover counter (ROC).

Questions (continued)

- PM-09 (old PM-08) used to say:
  - It MUST be possible for the switching conference server to determine if a received media packet was transmitted by a valid conference participant.
- Now it reads:
  - It MUST be possible for the switching conference server to determine if a received media packet was transmitted by a conference participant in possession of the end-to-end media encryption keys and hop-by-hop authentication keys.
- That's not quite right, so we propose:
  - It MUST be possible for the switching conference server to determine if a received media packet was transmitted by a conference participant in possession of a valid hop-by-hop key.

Questions (continued)

- Related to PM-10, there is an editor's note about "who should know when a participant joins or leaves a conference".
  - Should this be covered in the requirements or left to a framework or solution document?

Questions (continued)

- In the background text (section 5.2) it is noted that switching conference servers might optionally encrypt RTP header extensions and RTCP.
  - Is there a requirement for end-to-end encryption of either?
    - If so, is there a requirement to perform “selective encryption” where part of the RTP header extension or the RTCP packet is encrypted end-to-end and part is encrypted hop-by-hop?