MIKEY

IESG Evaluation

elisabetta.carrara@ericsson.com

- Some crypto clarifications
  - Require new PRF to be defined by its own RFC
- Secure clock synch protocol
  - not in MIKEY's scope
  - normative language
  - add refs to standards
- More references
- Clarifications (language), expansions
- "Companion RFC" when adding e.g. DH groups
  - Standard-track or Informational?

Transport issues

- Standalone, piggybacked (SDP/RTSP), or both?
- Standalone use is under-specified.
  - The section on reliability is lacking, e.g. congestion avoidance
  - Sugg: assume only reliable transport. In unreliable transport, a reliability mechanism MUST be used [ref]. BUT…
- Replication of material from mmusic-kmgmt-ext
  - Why not totally decoupled?
  - Normative dependency on a work-in-progress draft
  - Sugg: eliminate section
  - Our sugg: reduce to a ref; bidding-down attack description must be here. Drop standalone use (lack of scenario, TBD).