A Path Forward on Identity

• Agreement on a problem space
  – We all agree that E.164 numbers don’t work well with RFC4474
  – Less agreement about the requirements for intermediary traversal
    • Skepticism about some use cases

• Solutions that overcome the deficiencies of existing approaches
  – Where existing solutions include both 4474 and 3325
  – Does a solution do a better job with E.164 numbers, for example, than 4474 or 3325?
Desirable Properties

• Generality
  – One mechanism with universal applicability
    • Different mechanisms with different strengths open the door to bid-downs
    • “Configurable” DKIM-style assertions worrisome…

• Authentication, i.e. binding the session with domain-based assertion of identity

• Enables media security
  – At least provides a signature over key/desc

• Unconnected Applicability
  – Useful to decide whether or not to accept a request
Intermediary Authority over Signaling

• Intermediaries do not restrict themselves to the RFC3261 “amdr” rules of proxies (used by RFC4474)
  – However, scope of intermediary agency must have practical limits
  – Otherwise, there is no way to differentiate legitimate actions from attacks and no scope for protecting SIP signaling

• UAs implicitly authorize some intermediary alterations and not others
  – We all seem to agree that UAs do not, for example, authorize intermediary changes to the key fingerprints in SDP

• Today, this is poorly understood
  – We need the real “amdr” before we get into solutioneering
  – That requires, essentially, some formalization of SBCs
Promising Directions

• Intermediaries Instruct UAs
  – ICE, pieces of GRUU, original problem space of session-policy, etc.
  – Original chartered direction on this problem
    • Best architectural approach IMHO

• Verification Assertions
  – Intermediary verifies Identity and resigns as itself
    • May make arbitrary changes before it does so
  – Why is this better? It’s clear who is responsible