Connected Identity

STIR WG IETF 118
Jul 2023 (Praha)
Revisiting RFC4916

• Otherwise known as the “connected identity” draft
  – How to make Identity work in the backwards direction
  – RFC4916 covered mid-dialog and dialog-terminating requests in light of RFC4474 (predecessor to RFC8224)
    • Classic use case is UPDATE in the backwards direction before 200 OK: telling you who you actually reached
  – We opted for a greatly simpler approach

• Now defines a new “rsp” PASSporT type
  – Can only be sent in responses
    • Not necessarily limited to SIP, but, covered here with SIP as the focus
  – “rsp” is signed like “div” – the signing PASSporT has authority for the “dest” field rather than the “orig”
There’s a new -04 version

• Had some further comments post WGLC (thanks Jonathan)
  – Added the TFA use case explicitly to the motivation
  – Fixed a few places where normative statements could be read too broadly
  – Weakened the MUST to a SHOULD for sending Identity in further mid-dialog messages after receiving a STIR-signed response
    • We don’t want to go down the Required/Supported path for capability negotiation
    • Mid-dialog STIR does mitigate some fraud use cases, and is overall a pretty good idea though, so SHOULD seems right
  – Clarified that this isn’t supposed to work for CANCEL
    • That said, does not explicit forbid sending Identity in CANCEL
Next Steps

• Advance to IESG if everyone is cool with the fixes in my last revision