S/MIME for SIP and MSRP messaging

draft-campbell-sip-messaging-smime-00

Ben Campbell
Russ Housley
Motivation

• Organizations increasingly use mobile messaging for user notifications
  – Financial Transaction Notices
  – Password Change Attempt Notices
  – 2FA

• Lots of ways to go bad
  – Phishing attacks
  – Diverted 2FA notices
  – Etc
SIP/SIMPLE still matters (really)

• A number of mobile messaging frameworks use SIP and MSRP
  – VoLTE SMS : SIP MESSAGE
  – OMA CPM : SIP MESSAGE and MSRP
  – GSMA RCS: Builds on CPM

• Signed messages = low hanging fruit
  – … but encryption still matters
Highlights

• Signed Messages
  – MUST support ECDSA + SHA256
  – Prefer application/pkcs7-mime over multipart/signed

• Encrypted Messages
  – MUST support AES-128-CBC
  – MUST support ECDH with SHA256 if you support key agreement

• Certificates
  – Put SIP URIs in Subject Alternative Name
More Highlights

• Some general stuff about expressing UA capabilities

• SIP MESSAGE:
  – Keep messages small
  – Updates to 415 and 493 response requirements

• MSRP
  – Do S/MIME before chunking
  – Don’t use MSRP URIs for cert matching.
  – Clarify 415 response requirements.
Issues and To Dos

• Does anyone care about CPIM?
  – Maybe for SBCs that mess with SIP From and To?
• IMDN interactions
  – IMDN lets application servers modify CPIM messages. (Bad for signatures)
• Need to add examples
• May need more security considerations
What’s Next?

• Is this worth working on?
  – If so, how do we move it forward?
    • WG seems like overkill
    • AD sponsored?
    • Something else?
Thanks!