draft-peterson-stir-rfc4196-update-02
Connected Identity

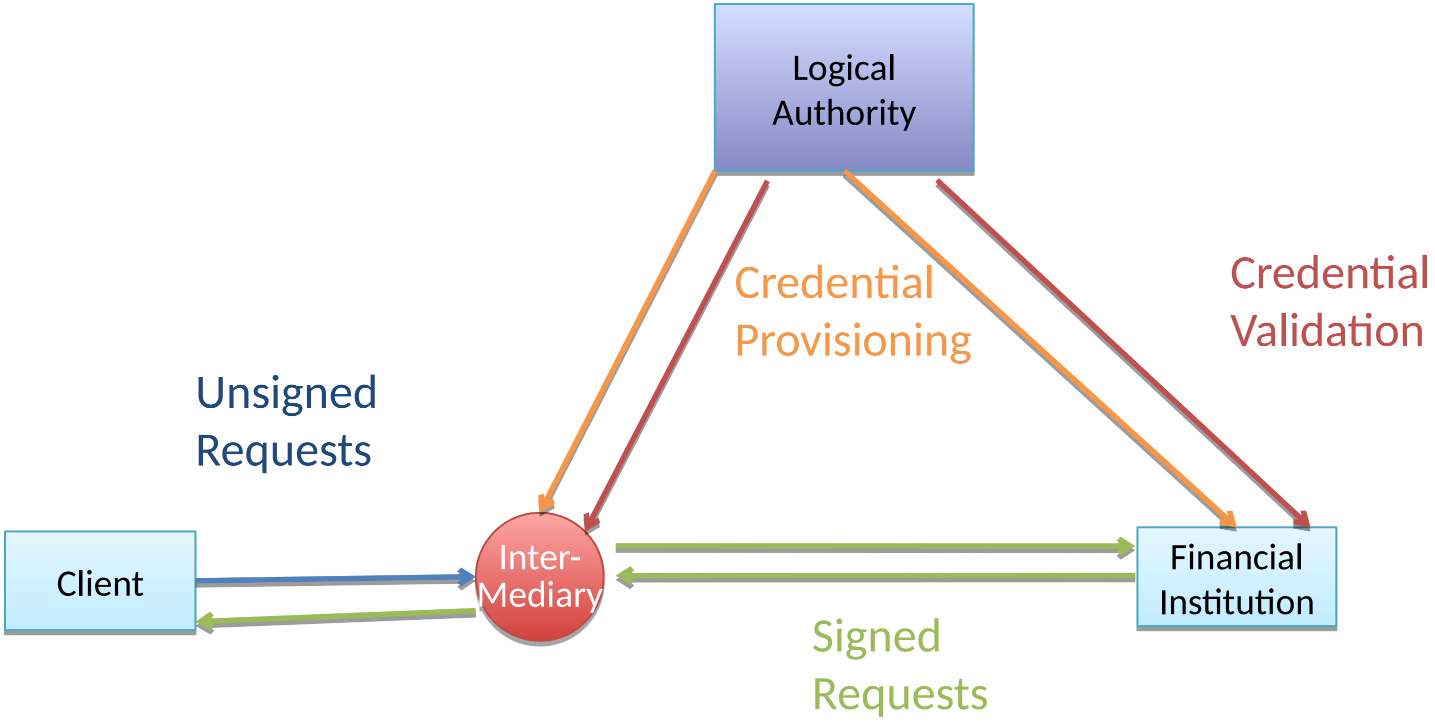
STIR WG IETF **109** Virtual

November 2020

An old draft returns

- The “connected identity” draft, update to RFC4916
  - How to make Identity work in the backwards direction, since it can’t work for responses
  - Covers mid-dialog and dialog-terminating requests
    - Classic use case is UPDATE in the backwards direction before 200 OK: telling you who you actually reached
- Leveraging STIR to close security vulnerabilities
  - Route hijacking
    - I tried to call my bank, by an attacker somehow interposed
  - “Short stopping” and similar attacks
    - Intermediary networks forging BYE in one direction while the call proceeds in another
  - sipbrandy (in C238) needs it (if anyone will use sipbrandy)
- This would take STIR past the threat model of RFC7375

STIR Backwards



Did I actually reach the bank?

How useful is it?

- **What will we use backwards Identity for?**
  - Authorization decisions about sending/receiving media
  - An approach: treat it like negotiating SRTP, in how failure is handled
- **What kind of user experience can we offer?**
  - Right now when you place a call you don’t always look at a display during alerting
    - Unlike the Caller ID case where users look at a display to decide how to answer
  - We won’t dictate a user experience, but we’ll at least provide cues it could follow
- **Can we do this before a call even starts?**
  - Easy to imagine discovering keys, determining what security services are available offline before a call is placed
    - Especially for destinations in an address book
    - Could help to know when you need to fail the call

How much of an update?

- Generally, RFC4916 guidance is still relevant
  - Lots of text about Identity-Info no longer applies
  - Back in 2016, Adam identified one more piece of normative behavior we should fix in 4916
    - Relates to the re-sending mechanism we hacked into RFC8224 for compact form failures
- Big idea is the same
  - e.g., use an UDPATE request in the backwards direction while the dialog is being formed
    - Sign it with RFC8224, let the PASSporT reflect the connected identity in the “orig”

Next Steps

- Been a while… an idea whose time has come?
    - If so, we’ll do some more work

- Adoption?