# Identity in SIP (and in-band)

STIR BoF

Berlin, DE

7/30/2013

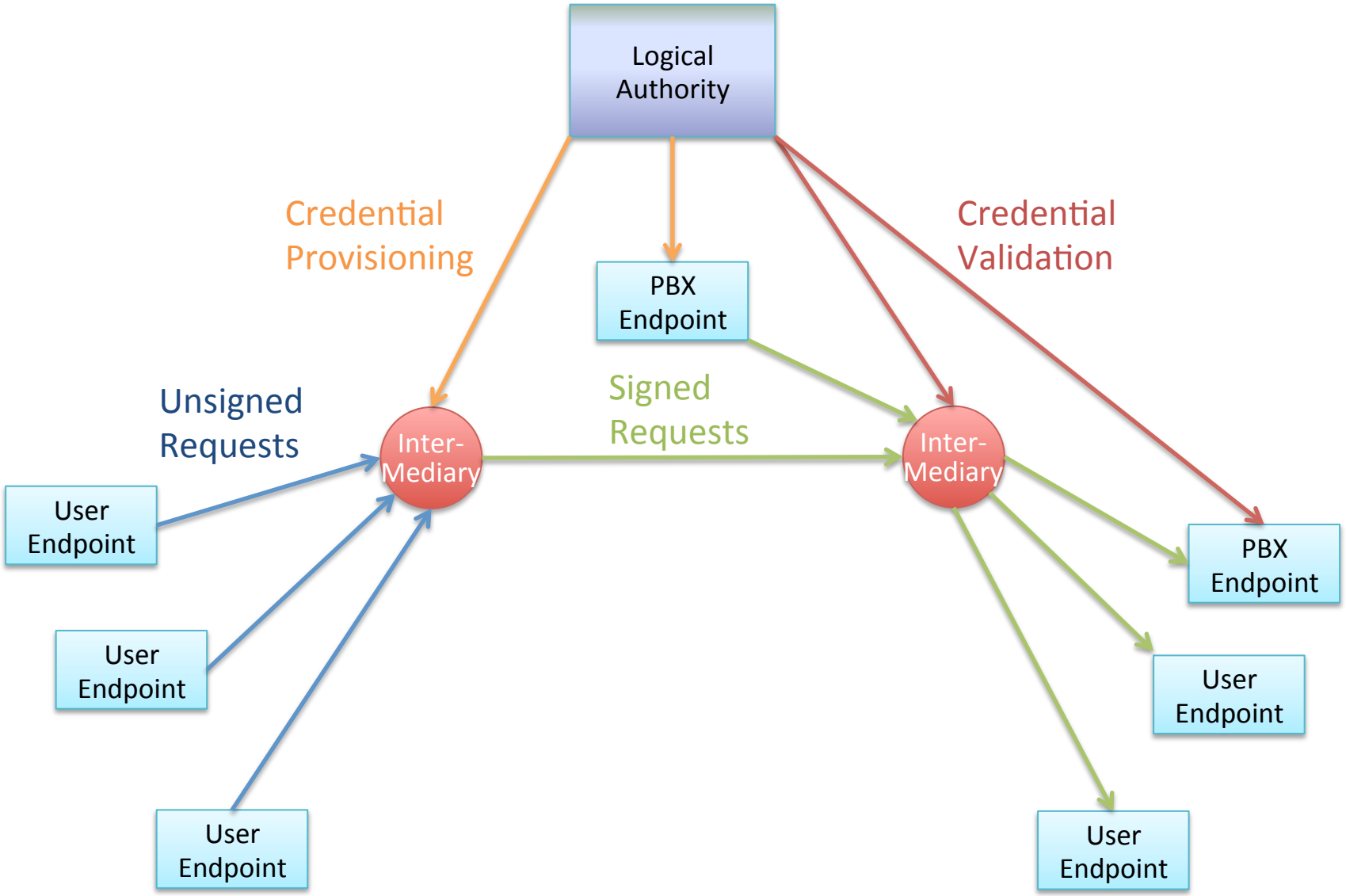
# In-band precedents

- **RFC3325** (short-term identity)
  - Advantages: deployable, deployed!
  - Disadvantages: requires trusted network, and…
    - Impersonation thrives in existing trusted networks
- **RFC4474** (long-term identity)
  - Advantages: Great for SIP URIs and RFC3261 compliance
  - Disadvantages: doesn't play well with telephone numbers, much of the world isn't RFC3261-compliant
- Many subsequent attempts to do better
  - Alternative signature scopes, tokens, etc.
  - VIPR notably tried to solve identity and a host of related problems

# Components of an in-band solution

- A field to carry a signature over various headers in a SIP request
  - e.g., RFC4474 Identity header
  - Intended to provide a cryptographic assertion of authority over the From header field and other components of the message:
    - Prevent replay by cut-and-paste attacker
  - **Problem**: many elements are changed by SIP intermediaries, which to choose?
- A way to acquire and validate the public key of the signer over those headers
  - e.g., the RFC4474 Identity-Info header
    - Includes carrying the key in band
  - **Problem**: Many viable approaches, which to allow/disallow?
    - RF4474 vaguely assumed public ENUM would have certs for numbers in the DNS

# In-band STIR Logical Architecture



# Revisiting what?

Which RFC4474 assumptions **failed**?

- SIP deployments remained focused on **PSTN interworking**
  - IP-PSTN, PSTN-IP, IP-PSTN-IP, PSTN-IP-PSTN
  - **Telephone numbers** are therefore the primary identifier of SIP
  - No story for certs in e164.arpa ever took hold
- Lack of unmediated **end-to-end** SIP signaling
  - Deployments are highly mediated, intermediary agency is not bounded
  - Mediated for various reasons, from NAT to interop to security
    - Policy enforcement of many kinds
  - Many calls still drop to the PSTN due to lack of IP routes
- RFC4474 solved for SIP requests in general
  - Assumed a world with MESSAGEs and NOTIFYs, not just INVITEs

# Rescoping to the Problem

- For threats like robocalling and voicemail hacking, man-in-the-middle attacks are not a real concern
- How best to separate the **replay-protection** goal from the **man-in-the-middle prevention** goal?
  - Not an entirely clean split
  - Scope the **To**/**From** protection to just the telephone number, when a telephone number is present
    - Domain or other parameters not helpful
    - Canonicalization required, a non-trivial problem
  - Necessarily include some kind of timestamp (**Date**)
  - Handle body protection separately, when you need it
    - Ultimately, possible to create some kind of linked two-layer signature

# Limits of in-band

- It's in-band
  - At best, this addresses the SIP-to-SIP use case
    - Maybe, e.g. IKES, with something else in the middle
  - Not going to help with SIP-to-PSTN, PSTN-to-PSTN
  - But we believe IP-to-IP is the future, right?
    - So we still need in-band
- Will SIP networks allow it?
  - Difficult to anticipate what will survive deployments
    - No guarantees are possible
  - Needs to change existing service behavior
    - Intermediaries need to do new things