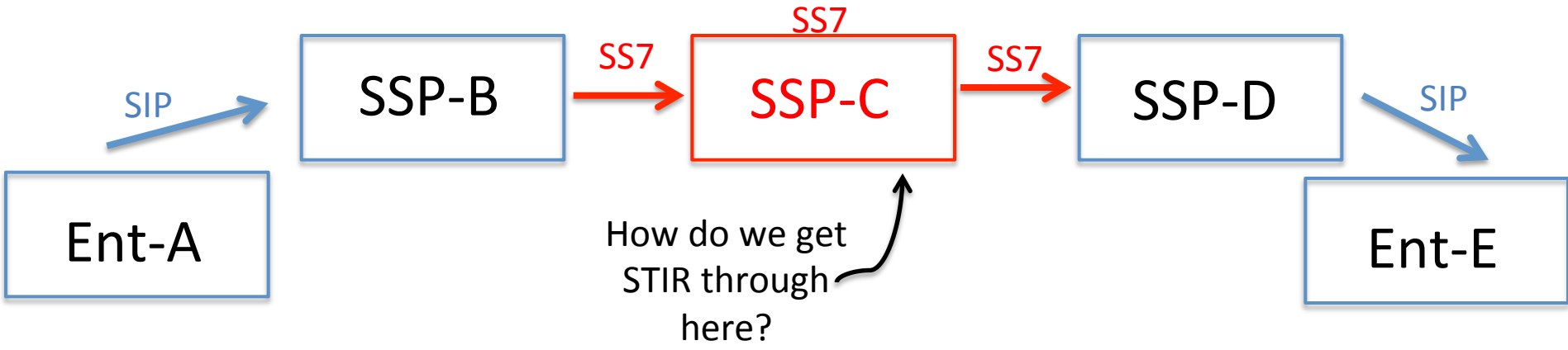
STIR In-Band Signature Transport

draft-kaplan-stir-ikes-out-00

Hadriel Kaplan

The Problem(s)



- SIP isn't the only call control protocol
  - SS7/ISUP, ISDN, H.323, BICC, XMPP, etc.
- The originator and terminator can't enforce everyone uses SIP
- Choices: ignore or accommodate

Proposed Solution: IKES

- Define rules for generating the info which must be signed, in a protocol-agnostic fashion
  - The resulting "info" is not specific to SIP, SS7, etc.
- Sign the information using a private key
- Define protocol-specific encoding rules for carrying the info and signature
  - E.g., a SIP header, or ISUP parameter
- Define rules for verifying the info

Passing STIRaight Through

- For SIP, XMPP: define the header/xml
- For SS7, ISDN, H.323: put it in a UUI
- Interworking can be done by gateways or SBCs
- But... this won't always work:
  - UUI doesn't normally survive across multiple SS7 domains
  - For ISDN, UUI is often used for inter-PBX calls
    - Though we probably don't need to care about that scenario for STIR

How is this different from 4474?

- 4474 is SIP-specific
  - To, From, Date, Contact, Call-ID, etc. are all SIP-specific fields (so is SDP obviously)
- IKES takes a minimalistic approach
  - only sign what is absolutely needed for caller-id
- 4474 tried to prevent MitM as well as replay
  - IKES doesn't: replay is only prevented against different targets

What are the drawbacks?

- Only 128 bytes available in UUI
  - For ISUP we can also use the Call Reference parameter to get another 3 bytes, but not in ISDN
- This impacts signature algorithm and key size
  - With 1024-bit RSA that's the signature size
  - ECC is smaller
- Key index size is also limited
  - Currently up to 8k indices in draft-01
- No signing of SDP/body/random-stuff

What are the benefits?

- It's not a lot of work to define it in a RFC
  - Even if no one implements it for SS7 or ISDN
- Forcing size restrictions keeps the SIP message size lower
- Keeps the information used for signing SIP-agnostic
  - Someday there may be a new protocol (SIPv3?)
  - Proprietary protocols can do it too
    - E.g.: IAX, WebRTC-based, Facetime, TIP, Skype

The Questions

- Do we care about anything other than SIP?
- Do we care about SS7 or ISDN?
- How many indices do we need?
- Can we use ECC instead of RSA?
- What's a better name than "IKES"?