draft-ietf-stir-oob-00
(was “fallback”)

STIR Virtual Interim
June 2017
Limits of RFC4474bis

• It’s in-band – end-to-end IP-IP
  – At best, it addresses the SIP-to-SIP use case
  – Not going to help with SIP-to-PSTN, PSTN-to-PSTN
    • Import for transitional adoption, legacy networks, enterprises, etc.
  – We did in-band first because existing deployments need it
    • Like the IPNNI, now the SHAKEN profile

• Even some IP-IP deployments may not pass Identity e2e
  – Difficult to anticipate what will survive administrative boundaries
    • You can understand “boundaries” pretty broadly
  – And some existing deployments might just block Identity
    • As they block all new headers; especially B2BUAs
Basic STIR Out of Band

Call Placement Service

CPS

Store PASSporT

Retrieve PASSporT

PSTN

POTS Call

Smart Phone

Smart Phone

Smart Phones are not just mobile phones, and not just end-user devices
Obvious Questions

• Okay, how does the originating side know where to find a CPS?
  – And how do we make sure the terminating side comes to exactly the
    same conclusion?
    • Need a service discovery mechanism
    • A few initial ideas in the draft now – not the focus today

• How do we make sure the right parties store and retrieve
  PASSporTs from a CPS?
  – Mostly, to manage the risk that someone other than the called party
    will fetch them? Or just record who fetched what?
    • Significant privacy concerns

• These are the things it’s time to work on
Who Gets to Store PASSporTs?

How to authorize a gateway to store it?
Do you need to authorize?

• PASSporTs are signed, so it almost doesn’t matter who stores them
  – Almost – need some kind of DDoS protection from attackers storing millions of bogus PASSporTs

• Relying parties trust a PASSporT based on its signature, not based on the CPS they got it from

• The authority to store might still require a STIR credential
  – Possible to limit storage with some kind of fancy tokens based on having a valid STIR cert (Ekr?)
    • Effectively pre-associate with the CPS before storing

• Ultimately, a GW could be authorized to store as well
  – Would require the GW to have some pre-association with a CPS
The Three Retrieval Semantics

• Draft today: what question does the retrieval side ask of the CPS? Three potential semantics:
  – (a) “Give me PASSporTs for the calling number”
  – (b) “Give me PASSporTs for the called number (me?)”
  – (c) “Give me PASSporTs for with both (a) and (b)”

• Those three options have different security implications
  – For case (b), can require a STIR credential
    • Identified as the best choice
    • Has implications for service discovery
    • (b) however has some complications in call forwarding cases (divert?)
Encrypting PASSporTs

• Encrypting PASSporTs is promising
  – Hides data from a nosy CPS (a likely PERPASS target)
  – Makes retrieval authorization less of a problem
    • Need to decrypt PASSporTs to get any value from retrieval
    • Provided of course CPSs always give back an encrypted blob when a retrieval request is made, even when there are no PASSporTs

• But there are problems
  – Much harder to manage call forwarding cases
    • Divert requires linking PASSporTs in a way that might be hard to retrieve if things are encrypted blobs
  – Encrypt to whom?
    • May be multiple authorities associated with a number (carrier, reseller, enterprise, user)
    • And how to discover their keys?
The Least Worst Way?

• Allow anyone to store encrypted PASSporTs, indexed by the public key used to encrypt
  – PASSporTs are encrypted with a key of the target
    • CPS cooperates with a cert cache, allows retrieving of public keys by target TN
      – Might give you multiple keys for the same TN: carrier, reseller, user, etc.
    – CPS can prevent abuse with some fancy Ekr way of authorizing storage
  • CPS always returns at least one encrypted blob when asked for a PASSporT for a given public key
    – Whether there is a call in progress or not
    – Only the intended recipient will be able to decrypt real PASSporTs and determine that there is a legit call in progress
• Doable?
Remaining Challenges

• Divert
  – Divert is needed, but requires special OOB behavior
    • Diverting entities need to place both the original and the divert PASSporT into the CPS encrypted to the new target

• Service Discovery
  – The more we “federate” the CPS function, the more pressing this becomes
    • How can the caller and callee agree on which CPS serves both?
    • How much pre-association does a caller need to have with a CPS to place a call?
  – If a CPS requires an adjacent credential service, that adds some more complexity to the mix
What about this case?

Maybe a SIP Identity-Encrypted header? RCD might need it anyway
Next Steps

• To Do
  – Need to write up the solution more
  – Need to describe the storage/retrieval protocol
    • Pro tip: it’s HTTP
  – Need to specify an OOB authentication and verification service procedure
    • Varies from RFC4474bis because that text is based on comparison to SIP fields
  – Need more on interaction with divert