**ATIS IP-NNI**

**July 12, 2021**

**Contribution**

**Title: Retargeting without “div”**

**Source**\***: Charter Communications**

**Issue Number:**

\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_

Abstract

Propose specifying a service provide when retargeting a call with a “shaken” PASSporT could as a local option

* Discard the received “shaken” PASSporT and generate a new “shaken” PASSporT
* Have a policy for determining what the Attestation level to use – e.g. could always just use the Attestation level from the received “shaken” PASSporT (if passed validation)
* Change the TN in the To header to align with the TN in the r-uri
  + With an option that would allow the To header to remain unchanged

# Replacing “shaken” PASSporT versus adding “div”

An advantage of using “div” PASSporT is that the PASSporT from the OSP can be preserved as the call retargets, which could facilitate traceback.

Disadvantages of using “div” is that support of “div” is not ubiquitous - so even if the forwarding SP adds a “div” PASSporT the TSP may not support “div” and if the TN in To header and r-uri are different the STI-VS would be bypassed – so the Attestation level in the “shaken” PASSporT would not be used.

Advantage of discarding old “shaken” PASSporT and generating a new “shaken” are

Reduce message size

Only requires TSP to support “shaken” PASSporTs (as long as align TN in To header with r-uri)

Note: using the Attestation from the received “shaken” PASSporT to use in a new PASSporT signed by the retargeting SP is analogous to using an enterprise Delegate Certificate.

A disadvantage of changing the To header is that it may impact forwarding loop detection and some applications may want to see the original called number.

# Option for To header & r-uri to have different TNs

Could also allow the To header to maintain its original value, If the current rule in ATIS-1000074 on what to do when the To & r-uri have different TNs was modified from the existing text:

“If the canonicalized value of the Request-URI TN does not match the canonicalized value of the TN in the To header field, then the verifier shall skip verification, and treat this event as if no Identity header was received.”

To something like:

“If the canonicalized value of the Request-URI TN does not match the canonicalized value of the TN in the To header field, then the verifier shall

1. Perform verification using the TN in the Request-URI
2. If this verification fails and the only error is the “dest” claim then this should be treated as if no Identity header was received.

Step 2 is needed to maintain backwards compatibility with current ATIS specifications.

This could be useful for calls to Toll Free numbers that get translated to a routing number – only needs one PASSporT versus 2.

# If support for this where to specify it

3 possibilities of where to specify this are

1. In an update to ATIS-1000074
2. In an update to ATIS-1000085
3. In a new specification

Prefer including this in an update to ATIS-1000085 and to make the document cover retargeting in general rather than be specific to “div” PASSporT.