**ATIS IP-NNI**

**March 3, 2021**

**Contribution**

**Title: Input for the response to the Liaison from the PTSC Non-IP Call Authentication Task Force**

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

**Issue Number:**

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

# FCC Requirement on Identity header

Below is text from <https://docs.fcc.gov/public/attachments/DOC-366783A1.pdf>

“Additionally, we further adopt our proposal to require intermediate providers to pass the Identity header unaltered.  We find that this requirement is necessary to prevent a downstream provider from tampering with the Identity header and thus undermining the end-to-end chain of trust between the originating and terminating voice service providers.”

Based on this intermediate providers would not be allowed to perform any format validation on the content of the Identity header.

Barring unique SHAKEN OOB issue the STI-CPS should provide unaltered transport.

# STI-CPS PASSporT Validation Issues

If PASSporT validation is defined need to clearly specify what is allowed to be verified.

Below are some of the things that PASSporT validation could include and some issues with each

1. Could just verify PASSporT complies with the format rules of RFC 8825
   * One issue with this is that today PASSporTs that do not comply with RFC 8825 are being accepted by STI-VS – e.g. PASSporT with ppt=shaken versus ppt=”shaken”.
   * Would a PASSporT based on distributed ledger technology be accepted? Uses jku parameter and no x5u parameter.
2. Freshness check
   * Because of div check cannot be on a per PASSporT basis but on the freshest PASSporT
3. Certificate Validation
   * There may be scenarios where one of the PASSporTs the Certificate cannot be verified
     + At previous IPNNI meeting the possibility that in some scenarios only some carriers would be able to verify the signature of an rph PASSporT
     + A call between 2 countries that transit via a 3rd country. The 2 countries involved in the call may have agreed on accepting each other Certificates but this agreement need not include the 3rd country. So an STI-VS in the 3rd country might not be able to verify the Certificate.
   * For incoming international calls this can add significant delay (e.g. round trip to Australia) and PASSporTs may not available when the retrieve request arrives.

# If validation is allowed & fails then what?

If decide validation is allowed & define what is allowed to be validated, also need to specify what happens when validation fails.

Some possibilities

1. Ignore the error and pass the PASSporT
   * in which case why bother with validation
2. Discard all PASSporTs
   * Is this what you would expect an STI-VS to do?
   * E.g. if an rcd PASSporT failed validation should a valid shaken PASSporT be ignored?
3. Discard only the PASSporT(s) which failed validation

# If STI-CPSs do not perform validation what can go wrong?

Only one scenario has been identified where not performing validation could create a problem.

Scenario:

* SP Z with an STI Certificate for some reason wants to interfere with a call between parties A & B
* SP Z is not in the call path
* SP Z publishes Invalid PASSporTs to an STI-CPS with the objective of overwriting the legitimate PASSporTs for calls from A to B
* If successful, when the call arrives at B’s TSP it would fail validation and not get the appropriate Attestation.
* It would be very difficult to identify SP Z as the culprit because STI-CPS would not be able to keep logging information for any significant time – since call detail information is sensitive.

For this to have a chance to work SP Z must be publishing the invalid PASSporTs at a high rate – e.g. needs to arrive after the legitimate PASSporTs are published and before they are retrieved. And SP Z would have to willing to take the risk if caught.

A simple mechanism that would allow detection without have to maintain sensitive information is for the STI-CPS to simply log only a portion of the Called & Calling party phone numbers – e.g. the last 5 digits of the calling & called number. Given this information and the calling time the number of possible logs matching the call should be very small - except for those coming from SP Z in publishing the invalid PASSporTs.

Note such logging can also be useful for troubleshooting any real issues – e.g. if having intermittent failures of PASSporT delivery, could use these logs to identify the STI-CPSs involved (e.g. could be problem only occurs when a particular pair of STI-CPSs are involved in the publish/retrieve).

Given the unlikeliness of this scenario (little to no upside and serious down side) and the simple alternative for detection if this were considered serious, do not see this as a reason for validation.

# Inbound International Calls

Issues to consider regarding the transport of PASSporTs for international calls inbound to the USA:

* The call may be sent to the US International Gateway SP from a SP in Country A but the PASSporTs may be from a SP in Country B
* The call may be transiting but not terminating in the US
* If any country specific PASSporT processing is required should it be provided by a STI-CPS or by the International Gateway SP?
  + Since STI-CPS doesn’t perform routing it would not be able to differentiate between calls terminating in the US versus just transiting the US
* Any per country rules would likely be determined by the STI-GA and FCC.