**ATIS IP-NNI**

**October 12, 2021**

**Contribution**

**Title: “div” transition**

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

**Issue Number:**

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

Abstract

Additional changes proposed for the transition to ubiquitous “div” support.

# Verstat when TN in To & r-uri are different

## Background

ATIS-1000074 specifies If the procedures in ATIS-1000085.v002 are not supported & the To & r-uri are different then the verifier shall skip verification.

Therefore the “div” specification should cover what to do whenever the To & r-uri are different.

One case that is not covered is when there are no “div” PASSporTs and the “shaken” PASSporT “dest” claim matches the r-uri.

One way this could happen is if the OSP implements Option-2 in 5.5.1 of “div”

**Option 2** Update the To header field TN to match the Request-URI TN and perform SHAKEN authentication as specified in ATIS-1000074 [Ref 1].

And if a transit provider changed the To header – e.g. some implementation derive the To header based on the top most diversion header (if present) or r-uri if not.

If do not specify what to do in this case presumably some implementations would treat this as a validation failure.

## Long Term

Before deciding what to do in the interim should consider what to do in the long term – i.e. when “div” PASSporTs are universally supported.

When receiving a “shaken” PASSporT and no “div” PASSporTs, two cases to consider

1. “dest” claim doesn’t match r-uri TN
* Set verstat= TN-Validation-Passed? No since would allow replay (change r-uri TN and leave To header TN and PAI TN unchanged).
* Set verstat=No-TN-Validation? Again would say no even though this is currently what ATIS-10000074 specifies, but the reason for this is the procedures for handling retargeting were not yet worked out.
* Set verstat= TN-Validation-Failed? Yes with universal support for “div” no reason to skip validation in this case.
1. “dest” claim matches r-uri TN
* Set verstat= TN-Validation-Passed? Yes since there is no replay scenario & technically there is a valid chain from the “dest” claim in the “shaken” PASSporT to the TN in the r-uri. (Note if r-uri TN is B, and “shaken” “dest” claim was B, adding a “div” PASSporT with “dest” & “div” claim equal to B would create a valid div chain.)
* Set verstat=No-TN-Validation? No even though this is currently what ATIS-10000074 specifies, but the reason for this is the procedures for handling retargeting were not yet worked out.
* Set verstat= TN-Validation-Failed? No since no replay scenario

## Transition

Now need to decide how to handle this during the transition phase, when the TSP supports “div” but “div” is not universally supported.

When receiving a “shaken” PASSporT and no “div” PASSporTs, two cases to consider

1. “dest” claim doesn’t match r-uri TN
	* Set verstat= TN-Validation-Passed? No since would allow replay (change r-uri TN and leave To header TN and PAI TN unchanged).
	* Set verstat=No-TN-Validation? Yes – since “div” not universally supported should allow for the case where call was retargeted by implementation not supporting “div” and continue applying the ATIS-10000074 treatment..
	* Set verstat= TN-Validation-Failed? No
2. “dest” claim matches r-uri TN
* Set verstat= TN-Validation-Passed? Yes since there is no replay scenario & technically there is a valid chain from the “dest” claim in the “shaken” PASSporT to the TN in the r-uri.
* Set verstat=No-TN-Validation? No even though this is currently what ATIS-10000074 specifies, but the reason for this is the procedures for handling retargeting were not yet worked out.
* Set verstat= TN-Validation-Failed? No since no replay scenario

## Text Proposal

At minimum should maintain the ATIS-1000074 behavior and set verstat=No-TN-Validation

Alternatively could treat as TN-Validation-Passed – since technically there is a valid chain from the “dest” claim in the “shaken” PASSporT to the TN in the r-uri.

## Text Proposal

Proposal text changes are diff marked against the text in 5.7 of IPNNI-2021-00094R000.docx

Proposal 1

The rules for setting verstat in the partial-support transition period are the same as stated above for the fully-supported case, with the exception that verstat shall be set to No-TN-Validation if the only verification failure is a broken chain of authority between the "shaken" PASSporT "dest" claim and the INVITE Request-URI. For example, consider the case where, during the transition period, a TSP receives an INVITE request that has been retargeted one or more times:

* If the TSP does not support "div" verification, then verstat is set as specified in clause 5.3.1 of ATIS-1000074 [Ref 1] and clause 7.2A.20.3 of TS 29.229 [Ref 10].
* If the TSP does support "div" verification, then the TSP shall set verstat to No-TN-Validation if any of the following conditions exist:
	+ The INVITE request contains one or more "div" PASSporTs and the only verification failure is a broken chain of authority between the "shaken" PASSporT "dest" claim and the INVITE Request-URI (e.g., when "div" authentication was not performed on all of the INVITE retargeting events), then the TSP shall set verstat to No-TN-Validation, or
	+ The INVITE request contains no "div" PASSporT, and the "shaken" PASSporT "dest" claim identifies a different destination than the INVITE Request-URI but the To header does not match the r-uri.
	+ The INVITE request contains no "div" PASSporT, and the "shaken" PASSporT "dest" claim identifies the same destination as the INVITE Request-URI but the To header does not match the r-uri

Proposal 2

The rules for setting verstat in the partial-support transition period are the same as stated above for the fully-supported case, with the exception that verstat shall be set to No-TN-Validation if the only verification failure is a broken chain of authority between the "shaken" PASSporT "dest" claim and the INVITE Request-URI. For example, consider the case where, during the transition period, a TSP receives an INVITE request that has been retargeted one or more times:

* If the TSP does not support "div" verification, then verstat is set as specified in clause 5.3.1 of ATIS-1000074 [Ref 1] and clause 7.2A.20.3 of TS 29.229 [Ref 10].
* If the TSP does support "div" verification, then the TSP shall set verstat to No-TN-Validation if any of the following conditions exist:
	+ The INVITE request contains one or more "div" PASSporTs and the only verification failure is a broken chain of authority between the "shaken" PASSporT "dest" claim and the INVITE Request-URI (e.g., when "div" authentication was not performed on all of the INVITE retargeting events), then the TSP shall set verstat to No-TN-Validation, or
	+ The INVITE request contains no "div" PASSporT, and the "shaken" PASSporT "dest" claim identifies a different destination than the INVITE Request-URI but the To header does not match the r-uri.
	+ The INVITE request contains no "div" PASSporT, and the "shaken" PASSporT "dest" claim identifies a the same destination as the INVITE Request-URI but the To header does not match the r-uri
* If the TSP does support "div" verification, then the TSP shall set verstat to TN-Validation-Passed if INVITE request contains no "div" PASSporT, and the "shaken" PASSporT "dest" claim identifies the same destination as the INVITE Request-URI.

# Recommendation on setting To header

If a “div” implementation sets the To header TN to be the same as the r-uri TN then a TSP that doesn’t support “div” would attempt verification using only the “shaken” PASSporT and the call would fail verification.

This can be avoided by having the To header & r-uri have different TNs. If this is done then the then a TSP that doesn’t support “div” would skip verification.

## Text Proposal

In section 5.3 propose adding the following new paragraph

Whenever an OSP adds an Identity header with a “div” PASSporT, the OSP should check if the TNS in the To header and r-uri have the same canonicalized value. If they have the same value, the OSP should change the TN in the To header (e.g. could align it with the “dest” claim in the “shaken” PASSporT. If these TNs are the same then the call could fail verification if the TSP does not support “div” PASSporT.