**ATIS/SIP Forum – IP-NNI**

**October, 2016**

**Arlington, VA**

**Contribution**

**TITLE: Clarifications to the handling of Identity header**

**SOURCE\*: Nokia**

**\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_**

**Abstract**

This contribution proposes changes to the SHAKEN Framework document to address handling of the Identity header.

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

Scenarios have been identified where the originating service provider could not fully attest the Caller-ID of a NS/EP Priority service call (e.g., call from an enterprise location). If the call was subsequently authorized as a NS/EP Priority Service (e.g., GETS) call, at that point we have actually verified the person making the call. In many ways this is a more stringent attestation than even “full attestation”, but the call would still only have “partial attestation”; this doesn’t seem sufficient.

For this scenario, an intermediate service provider effectively knows more about the caller than the originating service provider knew because of the GETS authorization. (Usually the originating service provider knows the most about the calling party, but not in this case.) It would seem appropriate for the intermediate (GETS) provider to also sign the call. The intermediate service provider would sign with their certificate and in effect be vouching for the call. In this case, the intermediate service provider should add another Identity header with this additional attestation – resulting in two Identity headers regarding the same claim.

Additionally, there are no clear statements regarding the handling of an Identity header in the case of a SIP B2BUA.

This contribution proposes text to be added to clarify the Identity header handling.

**5.2.1 PASSport and identity header construction**

For the SHAKEN framework, standard PASSporT base claims should be used as defined in both PASSporT and RFC4474bis documents.

The ‘orig’ claim and ‘dest’ claim MUST be of type ‘tn’.

The ‘orig’ claim ‘tn’ value should be derived using the following rules:

* The P-Asserted-ID header field MUST be used as the telephone identity, if present, otherwise the From header field MUST be used.
* If there is more than one P-Asserted-ID, Authentication service MUST have logic to choose the most appropriate based on service provider policy.

RFC4474bis allows the Identity header to be inserted by a SIP proxy or UA and for multiple instances of the Identity header to occur. The Identity header MUST be transited by SIP proxies and B2BUAs, unless otherwise prevented by local service provider policy. A SIP proxy or B2BUA MAY insert an additional Identity header in the event that the SIP node needs to make an additional claim or the SIP node has more specific knowledge regarding a claim in the received Identity header.

**5.3.1. PASSport and identity header verification**

The certificate referenced in the info parameter of the Identity header field MUST be validated by performing the following:

* check the validity dates
* check the certificate’s signature
* check chain of trust
* check certificate validity via CRLs and/or OCSP

The PASSporT token provided in the identity header of the INVITE MUST validate the presence of all of the baseline claims as well as SHAKEN extension claims. It MUST also follow RFC4474bis defined verification procedures to check the corresponding Date, Originating Identity and Destination Identities.

The ‘orig’ claim and ‘dest’ claim MUST be of type ‘tn’.

The ‘orig’ claim ‘tn’ value validation MUST be performed as follows:

* The P-Asserted-ID header field MUST be checked as the telephone identity to be validated if present, otherwise the From header field MUST also be checked.
* If there is more than one P-Asserted-ID, verification MUST check all P-Asserted-ID values.

In the event that multiple Identity headers exist regarding the same ‘orig’ claim ‘tn’ are present in the request, which claim is verified is based on local service provider policy.