**IP-NNI Task Force**

**Virtual**

**February 23, 2018**

**Contribution**

**TITLE:** Privacy / Display of STIR/ SHAKEN "Verstat" for Anonymous (CLIP/CLIR)

**SOURCE\*:** Verizon

**ISSUE NUMBER:**

**DOCUMENT:** Errata to ATIS-1000074 & Display of Verified Caller ID

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

**Abstract**

This contribution proposes a new section addressing the display of validated calls for Private and Anonymous calls (calling line identification restriction) to ATIS-1000074 and modifications to the Display Framework document. VERSTAT is not a PRIVACY PROTECTED parameter and provides value to the originating and terminating network without disclosing the originating identity and/or calling name or number. CVT MUST (1) handle the case for privacy and (2) use verstat properly in such cases.

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

**DISCUSSION:**

Maintaining legitimate uses of privacy should not interfere with the called party being notified that the call has been verified.  This concept should be documented as a requirement in the SHAKEN Standard and as guidance in the Display Framework.

In the case where an originating user has requested restricted presentation of Calling Name or Calling Number (either permanently or on a per-call basis), the originating network should perform Signing of a call (including sending an Identity Header). The Terminating network may use the Identity Header to generate a VERSTAT. While the terminating network MUST comply with the originating user request for PRIVACY (based upon proper SIP headers, and including not displaying the Calling Number), the uri parameter VERSTAT MAY be used and/or displayed to the terminating User. VERSTAT is not a PRIVACY PROTECTED parameter and provides value to the originating and terminating networks without disclosing the originating identity and/or calling name or number. CVT MUST (1) handle the case for privacy and (2) use verstat properly in such cases.

**Originating Network:**

P-Asserted-Identity: "Alice" <<sip:+12223334444@165.243.172.245>>

Privacy: id

Identity : asdfjashdflkjsdhfalkjsdhflakjfhalsdkjfhasdlkjh

**Terminating Network / After processing of Identity:**

**P-Asserted-Identity**: "Alice" <[sip:+12223334444; verstat=TN-Validation-Passed@101.251.151.139;user=phone](sip:+12223334444;%20verstat=TN-Validation-Passed@101.251.151.139;user=phone)>

**Privacy**: id

**Display on UE2 (Bob), including Terminating Network CVT for Analytics:**

“Unavailable”

“Validated ID” <Example>

**RECOMMENDATION:**

1. ATIS-1000074 - JOINT ATIS/SIP FORUM STANDARD – SIGNATURE-BASED HANDLING OF ASSERTED INFORMATION USING TOKENS (SHAKEN) does not currently include a requirement to explicitly present the call validation status to the called party independent of the calling party’s privacy preference. The following should be added as a new section:

**## - Privacy - Display of "Verstat" for calling line identification restricted (Private/Anonymous)**

*VERSTAT is not a PRIVACY PROTECTED parameter and provides value to the originating and terminating networks without disclosing the originating identity and/or calling name or number.*

*Device Display Framework along with CVT MUST provide this valuable information to end user.*

Use case for handling privacy and using VERSTAT for end user awareness:

**Originating Network**

*In the case where an originating user has requested restricted presentation of Calling Name or Calling Number either permanently or on a per-call basis (privacy header is included in INVITEs based on per subscriber data settings, i.e., both default privacy setting and allow per call override via \*67 (blocked) and \*82 (allowed)), the originating network should perform Signing of a call (including sending an Identity Header)*

**P-Asserted-Identity:** "Alice"<sip:+12155551212@tel.example2.net>,<tel:+12155551212>

**Privacy**: id

**Identity:**eyJhbGciOiJFUzI1NiIsInR5cCI6InBhc3Nwb3J0IiwicHB0Ijoic2hha2VuIiwieDV1IjoiaHR0cDovL2NlcnQtYXV0aC5wb2Muc3lzLmNvbWNhc3QubmV0L2V4YW1wbGUuY2VydCJ9eyJhdHRlc3QiOiJBIiwiZGVzdCI6eyJ0biI6IisxMjE1NTU1MTIxMyJ9LCJpYXQiOiIxNDcxMzc1NDE4Iiwib3JpZyI6eyJ0biI64oCdKzEyMTU1NTUxMjEyIn0sIm9yaWdpZCI6IjEyM2U0NTY3LWU4OWItMTJkMy1hNDU2LTQyNjY1NTQ0MDAwMCJ9.\_28kAwRWnheXyA6nY4MvmK5JKHZH9hSYkWI4g75mnq9Tj2lW4WPm0PlvudoGaj7wM5XujZUTb\_3MA4modoDtCA;info=<http://cert.example2.net/example.cert>;alg=ES256

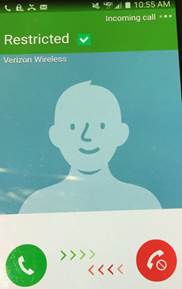
**Terminating Network**

*The Terminating network may use the Identity Header to generate a VERSTAT.    While the terminating network MUST comply with the originating user request for PRIVACY (based upon proper SIP headers, and including not displaying the Calling Number), the uri parameter VERSTAT MAY be used and/or displayed to the terminating User.*

**P-Asserted-Identity**: <[sip:+ 12155551212;verstat=TN-Validation-Passed@10.36.78.177:5060;transport=udp;user=phone](sip:+18174031887;verstat=TN-Validation-Passed@172.28.241.190:5060;transport=udp;user=phone)>

**From:** <<sip:anonymous@anonymous.invalid>>;tag=5a0bf135-5a8310bfd1ba84c-Not-lucentNGFS-128718

**Privacy**: id



1. Display Framework Section 5.2 assumption #4 reads as guidance for an analytics provider regarding adherence to the application of privacy rules.  An additional assumption should be added to echo the concern for maintaining privacy in cases where the network provider is providing the delivery of the final call information display.  Assumption #5 reference to “anonymizing ALL call information” should explicitly call out the fact that the determination of the authentication of the call is NOT “call information” in the traditional sense and should be presented to the user independent of legitimate privacy uses.  Section 5.2 of the Display Framework should be modified as shown:

## 5.2 Assumptions

…

1. It is expected that some service providers will delegate the delivery of the final call information display (including TN, calling name, and the results of verification) to an analytics provider. For those cases, the analytics provider is expected to adhere to the application of privacy rules for the calling number and name portions of the display; i.e., an "Anonymous" message would be displayed for name and TN.
   1. The terms of agreement between the service provider and the analytics provider are expected to require preservation of the caller's privacy.
   2. Further clarification and/or safe harbors are needed to determine whether the name and TN could be anonymized while additional call information, such as call category and potential fraud risk, could be delivered to help empower the end user.
2. Where delivery of the final call information display is not delegated to an analytics provider, the service provider is expected to adhere to the application of privacy rules for the calling number and name portions of the display; i.e., an "Anonymous" message would be displayed for name and TN.
3. In the absence of clarification or any special allowances on handling private calls, the guidelines herein call for anonymizing ALL call information if the received calling number is anonymous. The determination of the authentication of the call is NOT “call information” in the traditional sense and should be presented to the user independent of legitimate privacy uses.