**Contribution Title:** Verified Token Use Cases

**Source:** Jim McEachern, ATIS, [jmceachern@atis.org](mailto:jmceachern@atis.org)

**Abstract:** Many of the obvious use cases for STIR/Verified Token involve the call being signed either by the user of a phone number (classic STIR) or by the Service Provider the number is assigned to (Verified Token). However, there are a number of possible use cases where the number is signed by a third party. Depending on the use case, the third party may, or may not, have a relationship to the user or the originating service provider. This contribution outlines some of these use cases for consideration.

The material proposed in this contribution presents, as I understand the, ideas discussed during the IP-NNI call on Fevruary 24, 2016.

**Verified Token Use Case**

Many use cases for STIR / Verified Token involve the call being signed either by the user of a phone number (classic STIR) or by the Service Provider the phone number is assigned to (Verified Token). However, there are many use cases where it is necessary and appropriate for the number to be signed by a third party. In some cases, the third party will have a contractual trust relationship with the service provider the number is assigned to. (For example, …) In other cases, the third party will have a trust relationship with the end user, but not necessarily with the originating service provider. (For example…). In some cases, the third party may not have a trust relationship with either party. (e.g., GETS…?)

The following use cases involve calls being signed by someone other than the service provider the phone number has been assigned to.

* Customer has a VoIP line with Service Provider A but also has an arrangement with Service Provider B to provide backup IP service when there are failures. Under normal conditions, Service Provider A generates the verified token for the customer. However, under failure conditions, when traffic is routed through service provider B, it is not possible for Service Provider A to generate the verified token. Under these conditions, Service Provider B can generate the verified token. There are two possible sub-use cases.
  + Service provider B could have a contractual relationship with Service Provider A and could sign the verified token with a certificate issued to Service Provider A, but delegated to Service Provider B.
  + Service Provider B could sign the verified token with its own certificate, but with the authorization of the end user. In this case, the certificate would not be associated with the owner of the telephone number, and would implicitly rely on the certificate authority for the validity of the signature.
* A customer provisions their OTT voice service so that all outgoing calls show the user’s mobile phone number as the caller-ID. The OTT provider authenticates this by sending a code to the mobile phone and having the user enter that code before the provisioning takes effect. In this case, the OTT provider does not have a commercial relationship with the Service Provider the phone number was assigned to, but it does have a contractual relationship with the end user.
* A doctor returns a call to a patient, but wants the office phone number to appear as the caller-ID. In this case, there are two possibilities:
  + The doctor’s office phone and the doctor’s mobile phone could be provided by the same Service Provider. In this case, the service provider signing the verified token for calls from the doctor’s mobile phone would be the Service Provider the office number was assigned to.
  + The doctor’s office phone and the doctor’s mobile phone could be provided by different Service Providers. In this case, the service provider signing the verified token for calls from the doctor’s mobile phone would be different than the Service Provider the office number was assigned to. The two Service Providers might not have any commercial relationship.
* A school contracts with a third party to call parents when school is canceled due to bad weather. The third party offers this service nationally, and uses an intermediate service provider to “originate” the calls, while the schools use a variety of originating Service Providers. In this case, the party signing the verified tokens will have a relationship with the end user, but will not have a relationship with the Service Provider the number is assigned to.
* An international call center has a contract with a domestic company for a legitimate consumer recall initiative. The call center wants to sign the verified token for these calls, and has a commercial relationship with the end user, but not with the originating Service Provider(s).
* A VoIP Service Provider receives its telephone numbers from a CLEC, and wants to sign the verified token for calls even though it doesn't actually own the number.

Discussion

These use cases illustrate several things”

1. The entity in a position to sign a verified token does not necessarily have any defined relationship with the entity the phone number is assigned to.
2. Signing a verified token is not really providing “proof” of who owns the number, but is better thought of as “non-repudiation”. In other words, some entity is vouching for the authenticity of the call, and if the call proves to be illegitimate, the reputation of the entity that signs the call suffers.
3. For this system to work, it is critical that a highly reliable entity issues the certificates to entities that are authorized to sign verified tokens.
4. The process for obtaining certificates must be relatively onerous, so that it is not tempting for an entity to obtain a certificate for fraud, hoping to obtain benefit before the certificate is revoked.