This contribution attempts to capture assumptions underlying the use of STIR/SHAKEN to provide a level of assurance for information pertaining to the calling party in a SIP session. It then proposes the levels of assurance that can be provided based on if/how a SIP call is signed using SHAKEN.

The proposals in this contribution are provided for consideration and revision as appropriate.

**Assumptions:**

1. STIR/SHAKEN can provide more than a simple binary yes / no indication about the calling party TN. It will be possible to define “levels of assurance” that can be assigned to the calling party information. The level of assurance can depend on a number of things:
	* Whether or not a call is signed and what information is signed (e.g., the actual TN, a unique identifier for traceback, or the GW id).
	* The level of assurance could also depend on confidence in the entity that signs the token.
2. It there were no restrictions on obtaining a certificate, or if it was not possible to unambiguously identify the owner of the certificate, then STIR/SHAKEN verification would bring little value.
3. To provide confidence in the authentication and signing of tokens for SHAKEN, and to ensure the entity that signs tokens can be unambiguously identified, SHAKEN certificates will only be issued to “carriers”. This means they must:
	* Have an OCN
	* Be entitled to directly obtain E.164 numbers

**Note**: *I am assuming that there are valid scenarios for legitimate spoofing where a carrier would sign a TN that they had not directly obtained or a TN that had been assigned to another carrier.*

1. SHAKEN certificates can be revoked if a carrier abuses the signing / verification process.

**Note**: *Criteria for revoking a certificate, the definition of what constitutes “abuse”, and the mechanism for revoking certificates is for further study. This assumption merely proposes that in principle it is possible.*

1. Only carriers can sign calls. Certificates are issued to the carrier for their own use. (This would allow the carrier to use a third party service to perform authentication of TNs, signing and verification, but in this case the carrier would be outsourcing the function and would remain responsible for the accuracy of the assertions.)
2. STIR/SHAKEN could potentially be used to provide input information to “reputation systems” to develop and refine white lists, black lists and grey lists. If these were used, it the reputation systems would be queried at the terminating end. The details of how reputation systems would be used are out of scope for SHAKEN.
3. Signing calls is optional. Even if a carrier has a certificate, and has authenticated the TN, there are valid scenarios where either the calling party or the originating carrier may choose not to sign the call. For example:
	* Some users will want their calling party information to remain private and therefore may not want to sign the call with their true TN.
	* Carriers may also have valid reasons to not want to reveal the true TN even to the terminating carrier, and therefore may not want to sign the call with the true TN.

Unsigned calls would display to the called party (or anti-telemarketing app) as “private”. It may (should?) be possible to use SHAKEN to enable traceback of these calls, even if they are not signed with the true TN. (Note: the mechanism to achieve this is for further study.)

1. The “levels of assurance” in the above points relate to the degree of confidence in what is being asserted about the calling party. If multi-factor authentication is applied by the originating service provider, it is also possible to introduce another type of “levels of assurance”. This could be viewed as a two dimensional description of “levels of assurance”. For example, this could include the following levels:
	* The calling party TN (basic STIR/SHAKEN functionality)
	* A specific individual associated with this TN (with biometric authentication at the beginning of the call)
	* A specific individual with multi-factor biometric authentication throughout the call.
2. SHAKEN can be used in two distinct ways:
	* “Forward Direction” allows real-time confirmation that the TN has been authenticated by the originating service provider, and which service provider authenticated the TN (i.e., the identity of the originating service provider). This information can be used by the end user, or by anti-telemarketing apps, to decide how to treat the call.
	* “Reverse Direction” allows calls that have been flagged, to be traced back (at least part way) toward the source. This traceback could identify:
		+ The actual TN (in some cases)
		+ The Gateway node (this can be done even if the actual TN wasn’t signed)
		+ The carrier who signed the call (if it is signed with a TN, this will be the originating carrier, but if it is signed with a GW-ID it could be an intermediate carrier).

**Proposal:**

Given the above assumptions, SHAKEN can be used to provide real-time information to the called party concerning the call and a level of assurance about this information. SHAKEN can also be used to provide information that can be used in a forensic traceback after the call is completed. The information available for these two purposes may be different, so they are treated separately here.

**Forward Direction**: real-time information to the called party and level of assurance possible:

* **Call is not signed**: no information is available. Call is from an unknown source with an unknown reputation.
* **GW is signed (for traceability):** Call is from an unknown number. Information may be available concerning the historical traffic through the gateway, and third party reputation services may use this to modify the “level of assurance” presented to the called party (perhaps). (Note: if “reputation services” are used, this information would be accessed at the terminating end.)
* **Call is signed (for traceability) but not with a TN:** Call is from a “private” number. No information is available about the TN (i.e., the level of assurance would be “private number”), but information may be available to anti-telemarketing apps concerning the carrier.
* **Call is signed with a TN:** Calling party account / TN has been verified, and originating carrier is known. Reputation systems may be able to use this information to modify the “level of assurance” assigned to the calling party information.
* **Call is signed with TN and additional multi-factor authentication**: Calling party account / TN has been verified, along with a degree of authentication of the actual user. The degree of personal authentication of the individual will depend on the specifics of the additional authentication (e.g., personal password, thumbprint, iris scan, first born, etc.). The originating carrier is also known.

**Reverse Direction**: traceback information to facilitate forensic analysis after the call:

* **Call is not signed**: no information is available to assist with traceback.
* **GW is signed (for traceability):** The call can be traced back to a gateway. It may also be possible to trace it back to a specific incoming connection (i.e., virtual trunk) into the gateway.
* **Call is signed (for traceability) but not with a TN:** If the call is signed with a unique identifier, it should be possible to trace the call back to the originating TN. It is definitely possible to trace it back to the originating carrier.
* **Call is signed with a TN:** Call can be traced back to the originating TN.
* **Call is signed with TN and additional multi-factor authentication**: Call can be traced back to the originating TN and the individual user, with a higher degree of non-repudiation.