**Contribution:** IP-NNI Task Force

**Source:** Jim McEachern, Principal Technologist, ATIS

**Title:** Considerations for International SHAKEN

**Introduction**

The SHAKEN standard specifies operation within the domain of a single national or regional regulatory authority, in most cases within a single country. This was a conscious decision by the IP-NNI TF in order to more quickly develop a solution that explicitly addressed U.S. requirements. However, SHAKEN does not assume unique U.S. attributes, and therefore should be equally applicable to other countries. It was generally recognized that future consideration would need to be given to calls that originate in one country and terminate in another country, but this is not explicitly addressed in the existing standard.

There are now two countries actively deploying SHAKEN; the U.S. and Canada. Therefore, it is appropriate to begin consideration of a recommended strategy to federate SHAKEN across two or more countries.

**Discussion**

Potential approaches for cross-border SHAKEN should be evaluated against objective criteria to identify the optimal approach and/or consider a phased or transition approach. It is proposed that the following items be considered for this evaluation.

**SHAKEN Specification**: Extending SHAKEN to handle cross-border traffic may require extensions or changes to the existing SHAKEN specifications. Proposals should be analyzed to determine if any changes are required and, if so, the impact of the necessary changes. Factors such as backward compatibility should be considered in this analysis.

**Scalability**: Near-term deployment of SHAKEN will likely be limited to a small number of countries, but over time it is expected this number will grow. The complexity of eventually incorporating all countries into the SHAKEN ecosystem should be considered.

**Post Dial Delay**: If we maintain the SHAKEN model of fetching the public certificate and CRL from the URL provided by the Originating SP before completing the call, then there could be significant implications to post-dial delay. A requirement to cache such data in various points around the world to reduce post dial delay may have a significant implication on cost.

**Trust model**: Within a single country, the trust anchor for the SHAKEN ecosystem is the STI-PA, which distributes the list of Trusted STI-CAs to all participating service providers. As SHAKEN is extended internationally this trust model will need to be enhanced. The implications of supporting cross-border SHAKEN should be assessed; will it be compatible with the existing trust model; will the logic be the same; will changes be required to the existing practices within a single country?

**Vulnerability**: The existing SHAKEN governance model assumes the STI-GA will be able to modify best practices to address any vulnerabilities that may emerge. Will extending SHAKEN internationally create new opportunities for entities to gain access to the ecosystem and begin to “fully attest” illegal calls? If such vulnerabilities do emerge, how will they be addressed?

**Gaps**: This analysis should identify additional work required to allow SHAKEN to cover cross-border traffic. This should include standards work, product implementation, system upgrades and/or new systems and processes.

**Evaluation**

Two broad approaches have been suggested to “internationalize” SHAKEN. These are:

1. **SHAKEN “Trusted STI-CA”**

SHAKEN specifications state that the STI-PA approves STI-CAs using criteria established by the Policy Management Authority and then distributes the list of “Trusted STI-CAs” to all service providers in the SHAKEN ecosystem. The SHAKEN governance model only considers a single country, but nothing in the existing technical specification precludes two STI-GAs agreeing they will recognize each other’s STI-CAs and instructing their respective STI-PAs to merge their “Trusted STI-CA” lists. The merged trusted STI-CA list could then be distributed to all service providers in each of the participating countries, using existing interfaces and procedures. Calls authenticated in one country would then be successfully verified in the other country.

Initial deployment of cross-border SHAKEN using this model is likely to be based on direct bilateral agreement between two STI-GAs, but as deployment increases, other mechanisms could be introduced. Several countries could appoint an entity (e.g., CEPT) to act on their behalf, with a single agreement covering all the countries. Alternatively, an industry association could act as a central clearing house, (e.g., similar to the CA/Browser Forum - <https://cabforum.org/>) allowing new participants to sign a single agreement with the association to gain access to all other members of the association. All these arrangements (i.e., bilateral agreements, regional organization, and industry association) could coexist, depending on the circumstances of the participating countries.

**Analysis for SHAKEN Trusted STI-CA model:**

**SHAKEN Specification**: This approach does not require any changes to the base SHAKEN specifications. Existing implementations of SHAKEN will be fully compatible with cross-border SHAKEN. Once the STI-PA creates a combined “Trusted STI-CA” list, it can be distributed to participating service providers using existing interfaces. The only addition is that STI-PAs will need to identify a mechanism to exchange information about trusted STI-CAs, but this could be accomplished by a variety of out-of-band mechanisms. Another approach would be to host the list of Trusted STI-CAs on a trusted server and the PAs could update the server when they add or delete a new STI-CA and then each STI-PA would periodically fetch the list.

**Scalability**: bilateral agreements will be adequate for initial deployments. But continuing with bilateral agreements to include all 195 countries implies nearly 20,000 agreements. (Each country would potentially require an explicit agreement with every other country, which would require (195\*\*2)/2 agreements.) Suitable regional entities and associations exist to improve the scaling, and in some cases are already active in SHAKEN governance. At some point where bilateral agreements become onerous, these associations could readily step in to simplify scaling.

**Post Dial Delay**: Fetching the public certificate and CRL for the originating jurisdiction could incur post-dial delay of up to one second if on the other side of the world. Given this approach involves bilateral STI-PA arrangements, then it may be practical for each STI-PA to cache the CRL of each peer. This may affect the cost of implementation and operation for each STI-PA. Furthermore, requiring the STI-CAs to host their public certificates in each jurisdiction or key geographic locations may also affect the price SPs will have to pay their STI-CA.

**Trust model**: No changes to the SHAKEN trust model would be required. Each country retains control, and only trusts another country after an explicit decision to trust.

**Vulnerability**: This approach is based on the SHAKEN governance model, and therefore does not introduce new vulnerabilities that might allow unwanted entities to sign calls. If vulnerabilities do emerge, they can be addressed in much the same way they would be addressed within a single country.

**Gaps**: the only additional interface required in this approach is a simple mechanism for STI-PAs to exchange information on trusted STI-CAs. There may be no need to specify this interface, or for everyone to use the same approach.

1. **Central registry**:

The second approach for cross-border SHAKEN is a central registry. The analysis in this contribution is based on an Internet Draft submitted by Dr. Eric Burger (<https://tools.ietf.org/pdf/draft-burger-stir-iana-cert-00.pdf>) proposing an IANA Registry for STIR. In this model, each country independently decides if/when they want to participate in the global SHAKEN ecosystem and populates the registry with information for their country. It should be noted that this was a first draft (expired) and may require further work to fully define the mechanism, but it can be used to evaluate the broad attributes of the approach. STIR/SHAKEN verification would begin with an analysis of the calling number to determine the appropriate IANA registry location to use as the trust anchor for verification. (The information stored in this registry still needs to be specified.) The analysis of the calling number is straightforward and well understood, but isn’t part of the existing SHAKEN specification.

Although this analysis is based on an IANA registry, the central registry could be hosted under other entities such as ITU-T, with similar technical considerations.

**Analysis for central registry model:**

**SHAKEN Specification**: This model would require changes to the SHAKEN verification function to analyse the calling number to determine the appropriate STI-CA. The changes appear simple, but would depend on the final specification of the central registry.

**Scalability**: This model would be easily scalable. Each country would independently decide to participate and populate the required information in the central registry.

**Post Dial Delay**: In this approach, we have an additional fetch of the IANA root certificate authority list for the country of origin. This is done to ensure the public certificate referred to is part of the trust framework in said jurisdiction. This might be done only after the cryptographic signature has proven to be untampered. In any case, this could add some amount of post-dial delay to the budget already expended fetching the two URLs in the Identity header which was covered in the first approach above, If the IANA registry was used by each STI-PA supporting cross-border SHAKEN in order to append the root certificate authority list to their own local list, this would incur some savings by taking the IANA query out of the call processing step. Presumably this could also allow the CRLs of each peer STI-PA to be exchanged which would further reduce post-dial delay impacts. This may affect the cost of implementation and operation for each STI-PA. Furthermore, we would still potentially require the STI-CAs to host their public certificates in each jurisdiction or key geographic locations per the first approach above.

**Trust model**: A central global registry implies a different trust model. With SHAKEN, all entities in the ecosystem meet criteria defined by the STI-GA and are therefore trusted equally. If entities abuse this trust, they can be excluded from the ecosystem. With the centralized registry model, a given STI-GA does not have a say in who joins the ecosystem. Additional analysis would be required to understand the implications of this new trust model. At a minimum, perhaps each entry in the list for an ISO country should be able to produce a letter of authorization (LOA) from the regulator to operate as one of that country’s root certificate authorities if there is no STI-PA that maintains said list in that jurisdiction. Perhaps each STI-PA then needs an LOA of its own from the national regulatory authority.

**Vulnerability**: with this approach an STI-GA in one country has no visibility into the policies in other countries and there isn’t an identified mechanism to address vulnerabilities that emerge. The implications should be analyzed in greater detail before proceeding with this model. (Note: Any ISO country codes subtending from another such as 7 for Russia or 1 for North America could have default NULL entries for the subtending national jurisdictional codes.)

**Gaps**: This approach would require additional work, including:

* Fully specify and establish the central registry
* Update existing SHAKEN specifications and product implementations
1. **Hybrid Model**:

A hybrid model would initially use the SHAKEN “Trusted STI-CA” mechanism between countries. The first phase could use any or all of the following techniques:

* Bilateral agreements and directly merging Trusted STI-CA lists can be used between countries with similar interests and concerns.
* A “SHAKEN Association” could be formed, if desired, and countries that meet the “terms of service” could join this SHAKEN Association, which would maintain the merged Trusted STI-CA list.  This could coexist with bilateral agreements.
* The list of Trusted STI-CAs could be hosted on a trusted server and the STI-PAs update the server when they add or delete an STI-CA. Each STI-PA would periodically fetch the list from the trusted server.

The initial phase, as described above, would not require changes to the existing SHAKEN standards nor updates to the initial products deployed. This is an important attribute.

The second phase of the hybrid model would allow a transition to a central registry model. Based on proposals to date, the central registry will require changes to the SHAKEN specifications. These changes may be limited, and it might be possible to minimize the impact to existing product implementations. But until a central registry mechanism is agreed and fully specified, it isn’t possible to fully assess the impact and devise the optimal transition strategy.

A phased hybrid approach should allow the industry to proceed quickly with initial cross-border SHAKEN using “merged Trusted STI-CA lists”. At the very least, merged Trusted STI-CA lists could be used for the U.S. and Canada, where SHAKEN deployment is already underway. This approach leaves open the option of adopting a centralized international registry once it is available.

**Recommendation**

It is recommended that:

* The IP-NNI TF adopt the hybrid model for cross-border SHAKEN.
* Initial cross-border SHAKEN deployments use the SHAKEN “Trusted STI-CA” model.
* No changes to existing functions, specifications or interfaces defined in SHAKEN are required at this time to support initial cross-border SHAKEN deployments.
* A new out-of-band mechanism to exchange information on trusted STI-CAs will be required, but does not need to be formally specified, and can be left up to individual STI-PAs. No changes to the SHAKEN specifications should be made at this time concerning this new mechanism.
* One evolutionary approach could be to host the list of Trusted STI-CAs on a trusted server that the STI-PAs would update when they add or delete an STI-CA and then each STI-PA periodically fetches the list. If this mechanism is adopted, it could be documented in future updates of the SHAKEN specification.
* Transitioning to a central repository for international SHAKEN should be recognized as a possible future development but should not be specified further in the SHAKEN specifications at this time. Once the central registry is available, this should be revisited.
* Although no changes to the core SHAKEN specifications are necessary, it may be appropriate to formally document this recommended approach for cross-border SHAKEN. This could be done by:
	+ An addendum to ATIS-1000080
	+ A separate document on “Cross-border SHAKEN”

**Acknowledgement**:

The following individuals reviewed drafts of this contribution and provided valuable comments and edits.

* Thomas Rumball, Bell Canada
* Eric Burger, Georgetown
* Mary Barnes, iconectiv
* Chris Drake, iconectiv
* Gary Richenaker, iconectiv
* Russ Penar, Microsoft
* Ken Politz, Neustar
* Pierce Gorman, Sprint
* Richard Polishak, Telus