

STIR/SHAKEN Implementation Guide

1. Introduction to STIR/SHAKEN

STIR/SHAKEN is a framework designed to combat illegal robocalls and caller ID spoofing. It uses digital certificates to authenticate caller ID information for IP-based voice calls.

2. Regulatory Background

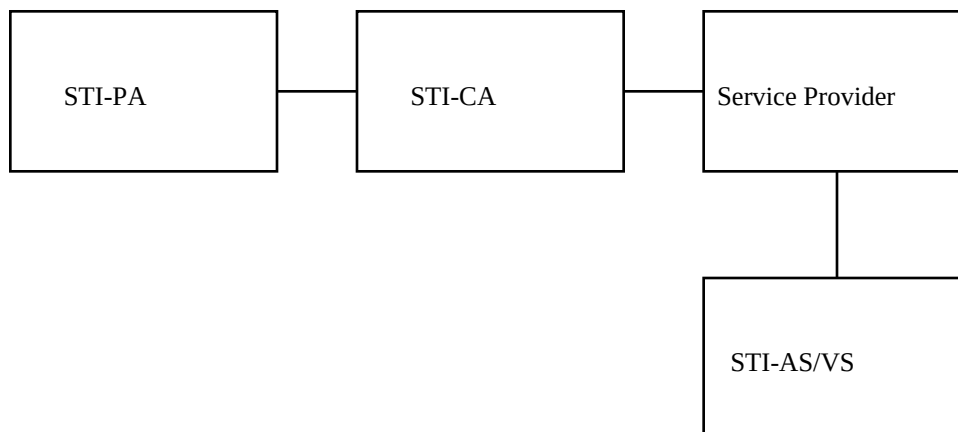
The FCC in the United States mandates STIR/SHAKEN for voice service providers. It is based on standards developed by ATIS and IETF (RFC 8224, 8588).

3. Architecture Overview

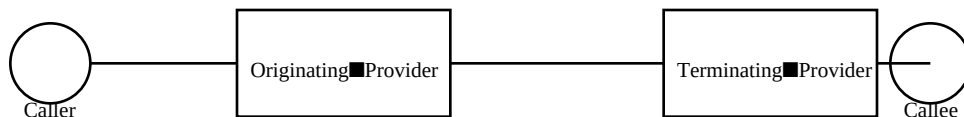
Key Components:

- STI-PA (Policy Administrator) – Approves providers for certificate access.
- STI-CA (Certification Authority) – Issues certificates to providers.
- STI-AS (Authentication Service) – Signs SIP INVITEs with PASSporT tokens.
- STI-VS (Verification Service) – Validates the authenticity of calls.

Architecture Diagram



Call Flow Diagram



4. Call Flow Example

1. Caller places a call through originating service provider. 2. STI-AS signs the SIP INVITE with a PASSporT token. 3. INVITE is sent with Identity header to terminating provider. 4. STI-VS verifies the PASSporT using public certificate. 5. Call is completed if verification succeeds.

5. Implementation Steps

- Obtain approval from STI-PA and get a certificate from STI-CA.
- Configure your SIP platform (e.g., OpenSIPS, Kamailio, FreeSWITCH) with STI-AS support.
- Implement SIP header signing for originating calls.
- Verify SIP Identity headers for terminating calls.
- Log verification results for analytics and compliance.

6. Sample SIP Identity Header

Example of an Identity header in SIP INVITE: Identity: eyJhbGciOiJFUzI1NiIsInR5cCI6IkpXVCJ9...;info=;alg=ES256

7. Testing & Validation

- Use test numbers provided by FCC or authorized labs.
- Validate PASSporT creation and signature with open-source tools.
- Ensure fallback for non-SHAKEN calls (e.g., TDM interconnects).

8. Deployment Considerations

- Certificate management and renewal automation.
- Integration with analytics to detect failed verifications.
- Handling of international calls not covered by STIR/SHAKEN.
- Scaling for high call volumes with optimized cryptographic operations.