



Outbound STIR/SHAKEN call flow & attestation

During an outbound call:

1. A SIP INVITE is received by the originating service provider (OSP).
2. The OSP looks at the call source (the customer) and the calling number to determine how best to sign (or attest) based on the validity of this information.
3. To sign calls, approved service providers (like Bandwidth) must be vetted by the STI Policy Administrator (STI-PA) and issued a digital STIR/SHAKEN certificate by a STI Certificate Authority (STI-CA).
4. Attestation is determined by the following parameters:



Attestation Level	Industry (ATIS) Standard	How Bandwidth Assigns Attestation
Full or “A”	The service provider knows the customer and their right to use the phone number.	You are a Bandwidth customer using a Bandwidth phone number
Partial or “B”	The service provider knows the customer, but not the source of the phone number.	You are a Bandwidth customer using another provider’s phone number • 3rd-party contact center using enterprise’s phone number • Calling-on-behalf-of (COBO) home device using mobile number • Legitimate number spoofing (caller ID appears from one phone number but call is originated from another number)
Gateway or “C”	The service provider has originated the call onto the network but can’t authenticate the call source e.g., international gateway.	Bandwidth does not currently attest any calls as “C”.



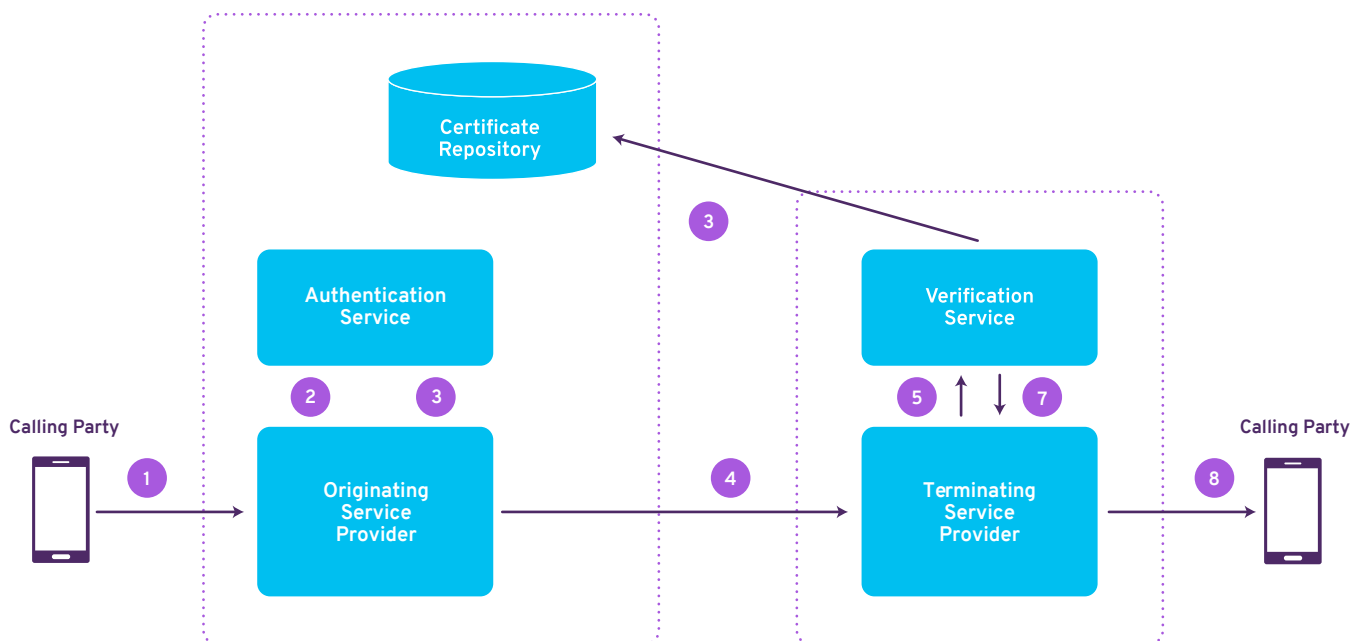
5. The originating service provider sends a SIP INVITE to an Authentication Service (STI-AS).
6. The Authentication Service returns the SIP INVITE with a SIP Identity Header containing a PASSporT header, PASSporT payload, PASSporT signature, encryption algorithm and location of Certificate Repository.
7. Included in the SIP INVITE is the:
 - Calling number
 - Number being called
 - Current date/timestamp
 - Attestation level
 - Unique originating identifier (Orig ID) for traceback

IDENTITY
HEADER

Identity:

```
eyJhbGciOiJFUzI1NiIsInBwdCI6InNoYWtlbiIsInR5cCI6InBhc3Nwb3J0IiwieDV1IjoiaHR0cHM6Ly9iYW5kd2lkdgGgtc2hha2VuLXRlc3QtY2VydHMuczMuYW1hem9uYXdzLmNvbS9id3NoYWtlbmVuZHVzZXJjZXJ0LnBlbSJ9.eyJhdHRlc3QiOiJBIAwiZGVzdCI6eyJ0biI6WyIxMjA2MzUwMSJdfSwiaWF0IjoxNTgwODQ1OTI3LCJvcmlnIjpw7InRuIjoimTk4NDM4OTE5MjgifSwib3JpZ2lkIjoimjkyNGU2MDMtODFkOC0zNmE5LWExNTItYTc3YmE3MDY1NmYyIn0Lq4T-fdajsWBNFtHiBd6xYErgY7natC0VCbXz7ZjqZh91j8v9NSduwyqP72YJ35jH2ZHh9sRuaX8m67wkReFLw;info=<https://bandwidth-shaken-test-certs.s3.amazonaws.com/bwshakenendusercert.pem>;alg=ES256;ppt=shaken
```

8. The SIP INVITE with the Identity Header is sent to the terminating service provider (TSP)





Inbound call flow & verification

For inbound calls to the terminating service provider (TSP), the SHAKEN framework outlines the steps to decode and validate the call:

1. The TSP sends the SIP INVITE with the Identity Header to a Verification Service (STI-VS)
2. The Verification Service obtains the digital certificate using a public key from a Certificate Repository
3. The Verification Service decrypts the SIP Identity Header and compares it to the SIP INVITE using the public key of the certificate from the Certificate Repository
4. The call is reviewed using several validation parameters to confirm:
 - The digital signature is valid
 - The caller ID matches information the SIP header
 - The originating service provider has a valid certificate
 - The originating service provider has the right to use the telephone number
5. Freshness check on date/timestamp
 - This information is conveyed as a verification status or VERSTAT with three potential results:
 - TN-Validation-Passed: the call met all the validation conditions
 - TN-Validation-Failed: the identity header failed the verification step
 - No-TN-Validation: the identity header was valid but the call did not have "A" level attestation

The SIP validation information appears as:

```
sip:+19843891928;verstat=TN-Validation-Passed@67.231.3.4 3:5060;user=phone
```

