An Introduction and Overview of the STIR / SHAKEN Framework

Martin Dolly
Lead Member of Technical Staff
Core Network & Gov't/Regulatory Standards
and Director, SIP Forum
md3135@att.com

12/4/2018

Spoofed Calls Versus Robo-Call

- **Spoofed calls**

The *Truth in Caller ID Act* prohibits spoofing, or deliberately falsifying the telephone number (TN) and/or name relayed as the caller ID information to disguise the identity of the caller ***for harmful or fraudulent purposes***. However, the law only applies to callers within the United States.

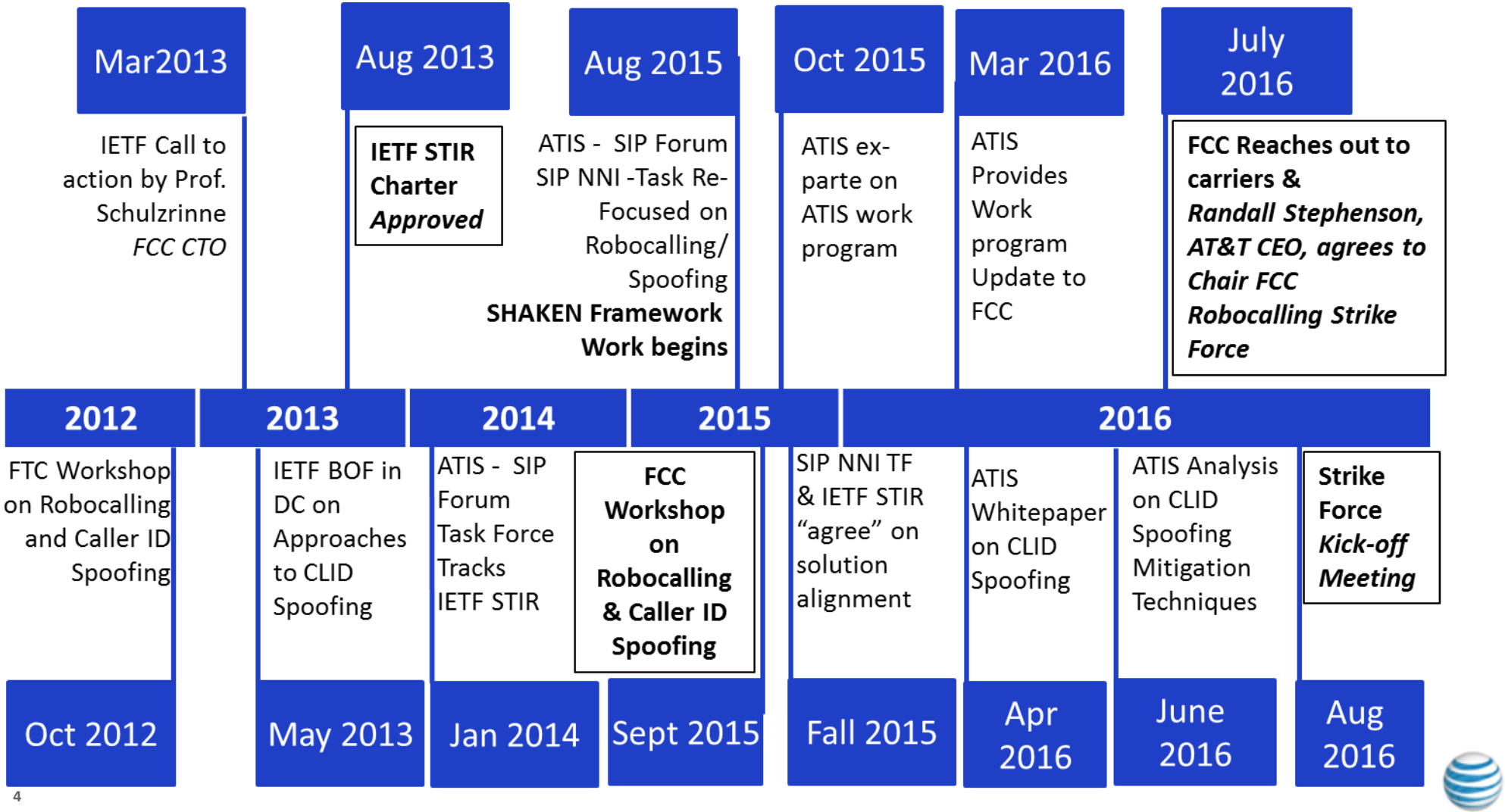
- **Robo-Calling**

A robocall is a phone call that uses a computerized autodialer to deliver a pre-recorded message, as if from a robot. Robocalls are often associated with political and telemarketing phone campaigns, but can also be used for public-service or emergency announcements.

We know how we got here

- Robocalls & Spoofing is the #1 complaint to the FCC and FTC.
  - https://consumercomplaints.fcc.gov/hc/en-us/articles/204009760-Consumer-Complaint-Charts-and-Data-Overview
- Robocalls & Spoofing is the #1 complaint to the CRTC in Canada
- Robocalls & Spoofing is the # 1 complaint to OFCOM and the UK ICO
  - https://ico.org.uk/action-weve-taken/nuisance-calls-and-messages/
- There have been 6-8 different bills in Congress looking at this. Hearings you name it.
  - FCC FTC CRTC [CA] OFCOM [UK] have held workshops. I wrote one of the reports.
  - http://stakeholders.ofcom.org.uk/binaries/market-data-research/Ofcom_VoIP_RPKI_Report.pdf
  - US Congress had endless hearings.
  - https://energycommerce.house.gov/hearings-and-votes/hearings/modernizing-telephone-consumer-protection-act
- The PSTN is undergoing a radical transition
  - With VoLTE IP based voice will be 75% of the market in 3 years in the US.
- Existing PSTN Class 5 TDM/SS7 equipment is at or near End of Life [EOL] and cannot be modified.
- All IP Interconnection now a reality US CA EU

Robocalling/ Spoofing Timeline



STIR & SHAKEN Work Program

IETF

- ***RFC 8224, Authenticated Identity Management in the Session Initiation Protocol (SIP)***
- ***RFC 8225, PASSporT: Personal Assertion Token***
- **RFC 8226, Secure Telephone Identity Credentials: Certificates**
- **RFC 8443, Personal Assertion Token (PASSporT) Extension for Resource Priority Authorization**
- ***PASSporT SHAKEN Extension (SHAKEN)***
- **PASSporT Extension for Diverted Calls**
- PASSporT Extension for Rich Call Data
- **TNAuthList profile of ACME Authority Token**

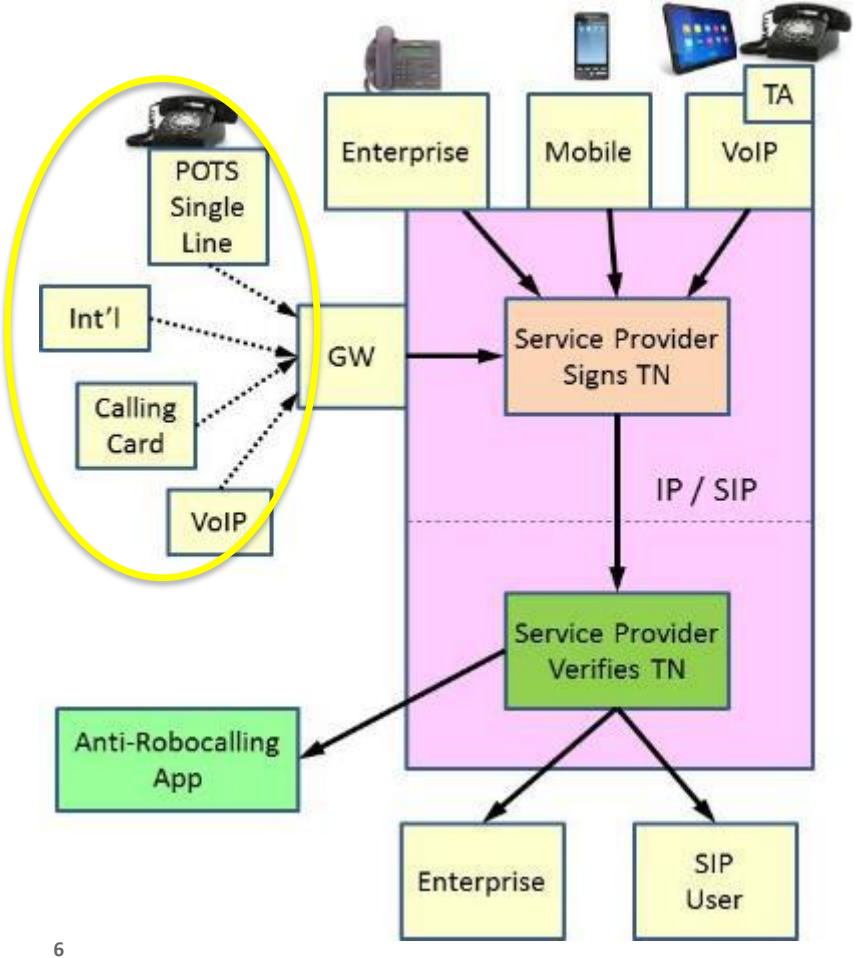
IPNNI

- IPNNI-2018-00038Rxxx, SHAKEN Roadmap
- ***ATIS-1000074, Signature-based Handling of Asserted information using toKENs (SHAKEN)***
- IPNNI-2018-00088Rxxx, SHAKEN Errata
- **ATIS-1000082, SHAKEN API for a Centralized Signing and Signature Validation Server**
- ***ATIS-1000080, Governance Model***
- **ATIS-1000084, Technical Report on Operational and Management Considerations for SHAKEN STI Certification Authorities**
- ATIS-1000081, Display Framework
- **IPNNI-2018-00084Rxxx, ATIS Standard on Signature-based Handling of SIP RPH Assertion using Tokens**
- **IPNNI-2018-00036Rxxx, SHAKEN Support of "div" PASSporT Token**
- IPNNI-2018-00018Rxxx, Signature-Based Handling of Asserted Information Using Tokens (SHAKEN): Proof-of-Possession of Telephone Numbers (TN-PoP)
- IPNNI-2018-00082Rxxx, ATIS Technical Report on a Framework for SHAKEN Attestation and Origination Identifier
- IPNNI-2017-00020Rxxx, Verification Token Use Cases (Living Document)
- IPNNI-2018-00048R000, Robo-Metrics

3GPP

- **3GPP TS 24.229**, Technical Specification Group Core Network and Terminals; IP Multimedia Call Control Protocol based on Session Initiation Protocol (SIP) and Session Description Protocol (SDP); Stage 3
- **3GPP TS 29.163,** Technical Specification Group Core Network and Terminals; Interworking between the IP Multimedia (IM) Core Network (CN) subsystem and Circuit Switched (CS) networks
- **3GPP TS 29.165,** Technical Specification Group Core Network and Terminals; Inter-IMS Network to Network Interface (NNI)
- **3GPP TS 29.292,** Technical Specification Group Core network and Terminals; Interworking between the IP Multimedia (IM) Core Network (CN) Subsystem (IMS) and MSC Server for IMS Centralized Services (ICS)

STIR/SHAKEN Limitations



- STIR can be used to validate SIP calls in real-time or to trace calls after the fact.
- GW may sign its identity for traceability purposes, without verifying calling number.
- Calls from outside SIP network cannot be verified.
  - Domestic SIP only
  - No support for TDM

Certificate Attestation Policy Indication

A. **Full Attestation:** The signing provider:

- is responsible for the origination of the call onto the IP based service provider voice network
- has a direct authenticated relationship with the customer and can identify the customer
- has established a verified association with the telephone number used for the call.

Note: The legitimacy of the telephone number(s) the originator of the call can use is subject to signer specific policy

B. **Partial Attestation:** The signing provider:

- is responsible for the origination of the call onto the telephone network
- has a direct authenticated relationship with the customer and can identify the customer
- has NOT established a verified association with the telephone number being used for the call

Note: Each customer will have a unique identifier, The unique identifier also provides a reliable mechanism to identify the customer for forensic analysis or legal action where appropriate.

C. **Gateway Attestation:** The signing provider:

- is the entry point of the call onto the telephone network
- has no relationship to the initiator of the call (e.g., international gateways).

Note: The signature will provide a unique identifier of the node. (The signer is not asserting anything other than “this is the point where the call entered my network”.)

The PASSporT “shaken” extension

The PASSporT “shaken” extension shall include both an attestation indicator (“attest”), as described in section 5.2.3 and an origination identifier (”origid”) as described in section 5.2.4. The SHAKEN PASSporT token would have the form given in the example below:

Protected Header


```
{
        "alg":"ES256",
        "typ":"passport",
        "ppt":"shaken",
        "x5u":"https://cert.example.org/passport.crt"
}
```


Payload


```
{
        "attest":"A",
        "dest":{"tn":["12125551213 "]},
        "iat":1443208345,
        "orig":{"tn":"12155551212"},
        "origid":"123e4567-e89b-12d3-a456-426655440000"
```

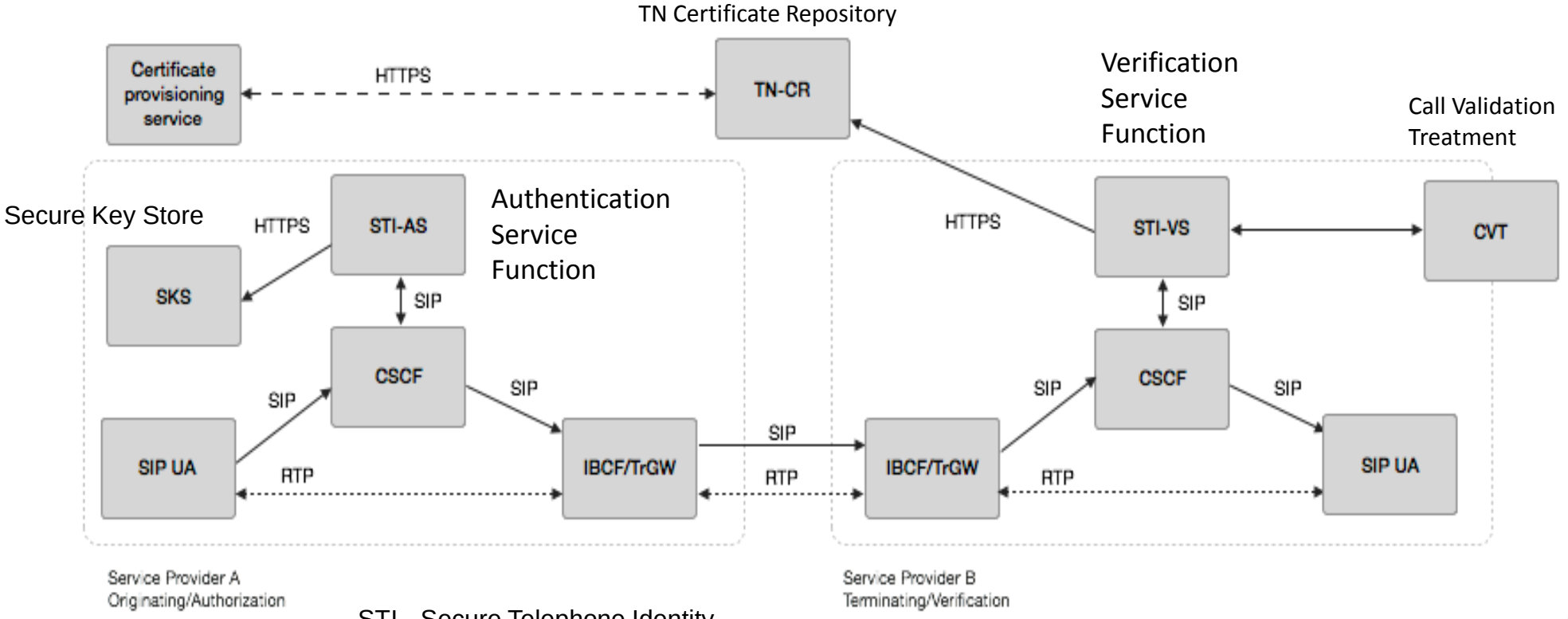

In addition to attestation, the unique origination identifier (“origid”) is defined as part of SHAKEN. This unique origination identifier should be a globally unique string corresponding to a Universally Unique Identifier (UUID) (RFC 4122). The origid will identify:

- Signing Carrier
- Carrier Customer/Access Carrier
- Entry Gateway

SIP Identity Header Example for SHAKEN

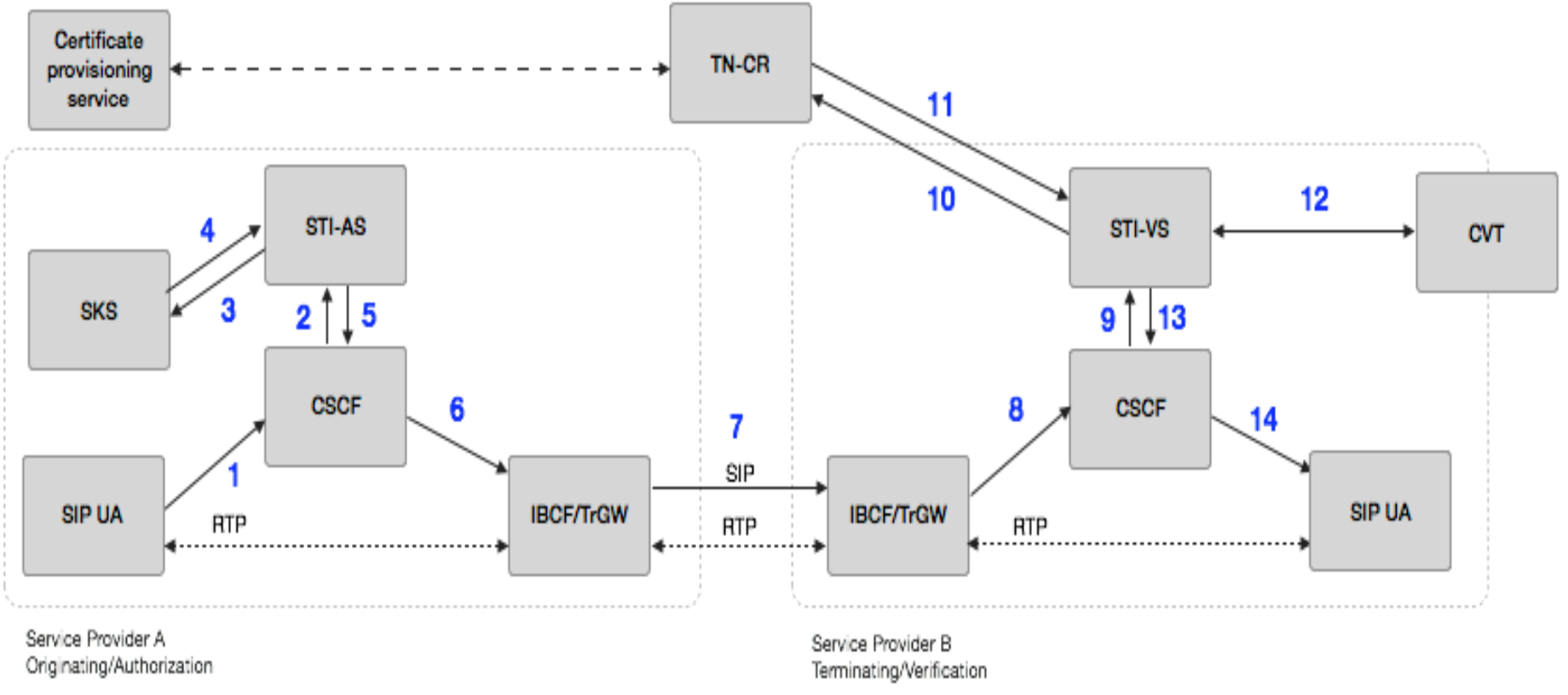
```
INVITE sip:+12155551213@tel.example1.net SIP/2.0
Via: SIP/2.0/UDP 10.36.78.177:60012;branch=z9hG4bK-524287-1---
77ba17085d60f141;rport
Max-Forwards: 69
Contact: <sip:+12155551212@69.241.19.12:50207;rinstance=9da3088f36cc528e>
To: <sip:+12155551213@tel.example1.net>
From: "Alice"<sip:+12155551212@tel.example2.net>;tag=614bdb40
Call-ID: 79048YzkxNDA5NTI1MzA0OWFjOTFkMmFlODhiNTI2OWQ1ZTI

P-Asserted-Identity: "Alice"<sip:+12155551212@tel.example2.net>,<tel:+12155551212>
CSeq: 2 INVITE
Allow: SUBSCRIBE, NOTIFY, INVITE, ACK, CANCEL, BYE, REFER, INFO, MESSAGE, OPTIONS
Content-Type: application/sdp
Date: Tue, 16 Aug 2016 19:23:38 GMT
Identity:
eyJhbGciOiJFUzI1NiIsInR5cCI6InBhc3Nwb3J0IiwicHB0Ijoic2hha2VuIiwieDV1IjoiaHR0cDovL2N
lcnQtYXV0aC5wb2Muc3lzLmNvbWNhc3QubmV0L2V4YW1wbGUuY2VydCJ9eyJhdHRlc3QiOiJBIiwiZGVzdC
I6eyJ0biI6IisxMjE1NTU1MTIxMyJ9LCJpYXQiOiIxNDcxMzc1NDE4Iiwib3JpZyI6eyJ0biI64oCdKzEyM
TU1NTUxMjEyIn0sIm9yaWdpZCI6IjEyM2U0NTY3LWU4OWItMTJkMy1hNDU2LTQyNjY1NTQ0MDAwMCJ9._28
kAwRWnheXyA6nY4MvmK5JKHZH9hSYkWI4g75mnq9Tj2lW4WPm0PlvudoGaj7wM5XujZUTb_3MA4modoDtCA
;info=<http://cert.example2.net/example.cert>;alg=ES256
Content-Length: 153
v=0
o=- 13103070023943130 1 IN IP4 10.36.78.177
c=IN IP4 10.36.78.177
t=0 0
m=audio 54242 RTP/AVP 0
a=sendrecv
```


SHAKEN reference architecture

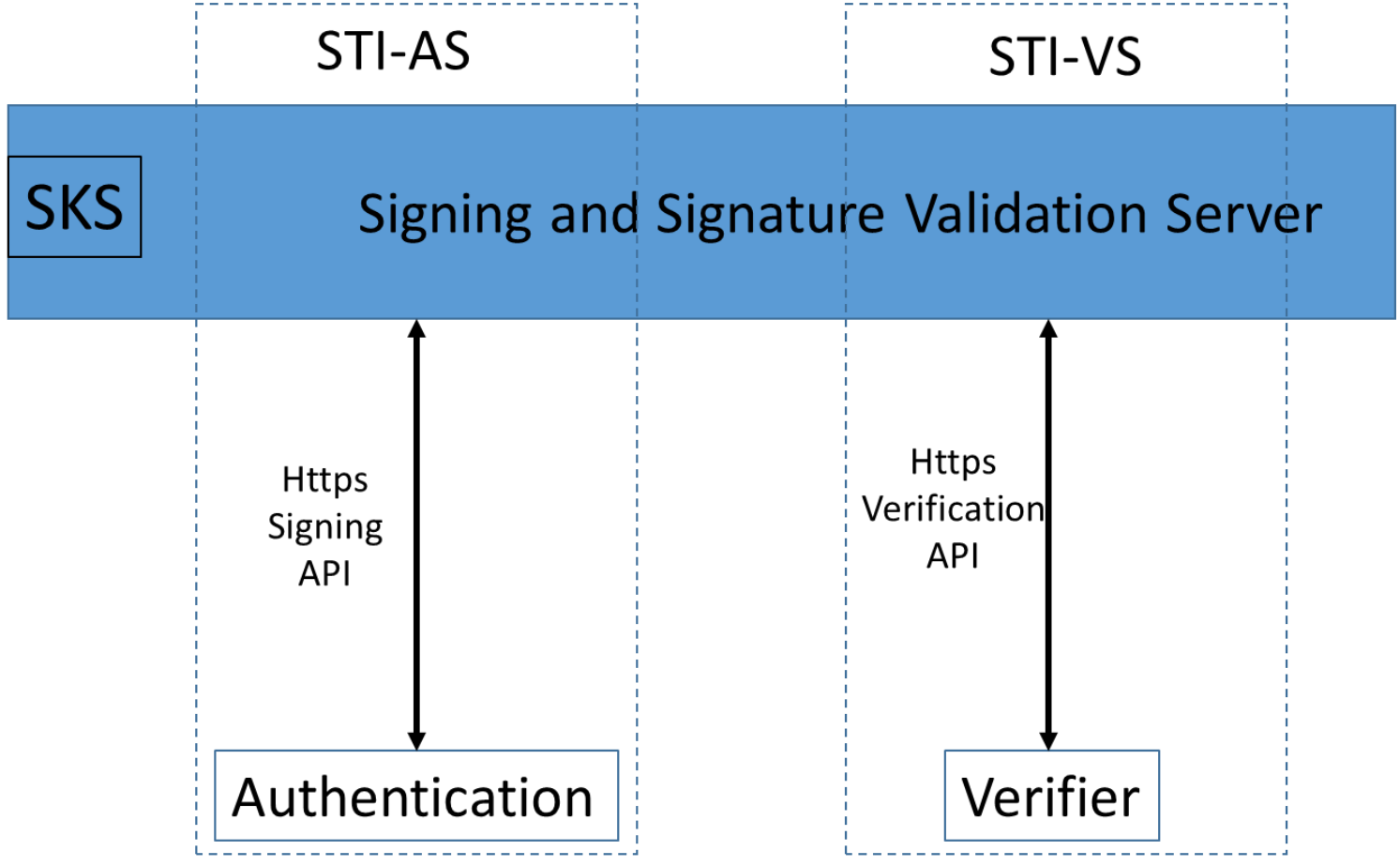


STI - Secure Telephone Identity

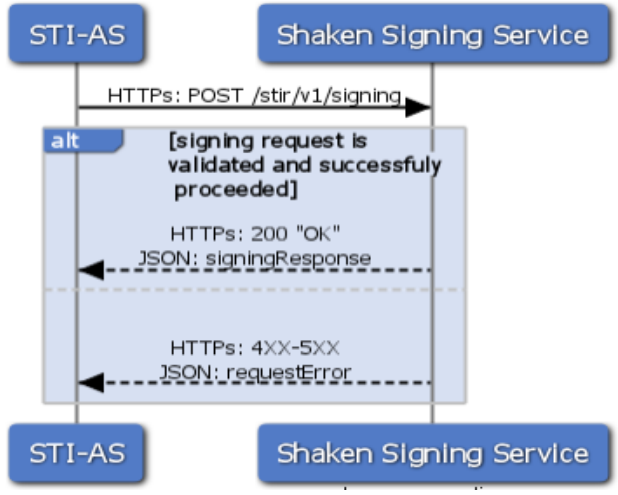
STIR/SHAKEN Basic Call Flow



Centralized Signing and Signature Validation Server



SHAKEN API for a Centralized Signing and Signature Validation Server



1. Request Sample

1. POST /stir/v1/signing HTTP/1.1
2. Host : stir.att.com
3. Accept : application/json
4. X-RequestID: AA97B177-9383-4934-8543-0F91A7A02836
5. Content-Type: application/json
6. Content-Length : …

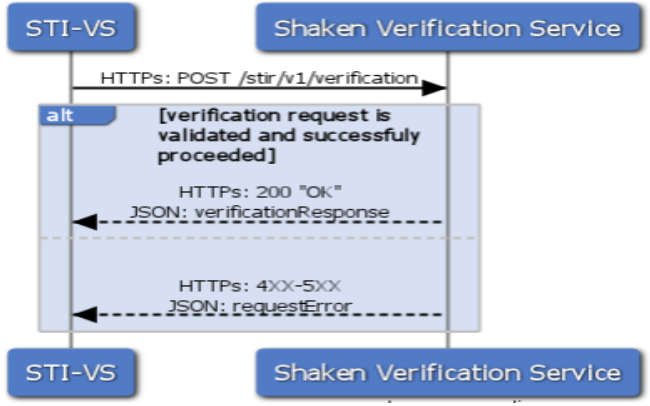
```
{
  "signingRequest": {
            "attest": "A",
            "orig": {
                    "tn": "12155551212"
                  },
             "dest": {
                     "tn" : [
                             "12355551212"
                            ]
                     },
            "iat":  1443208345,
            "origid": "de305d54-75b4-431b-adb2-eb6b9e546014"
    }
}
```

1. Response Sample (Success)

1. HTTP/1.1 200 Ok
2. X-RequestID: AA97B177-9383-4934-8543-0F91A7A02836
3. Content-Type : application/json
4. Content-Length : …

```
{
  "signingResponse": {
   "identity" :
"eyJhbGciOiJFUzI1NiIsInR5cCI6InBhc3Nwb3J0IiwicHB0Ijoic2hha2VuIiwieDV1IjoiaHR0cDov
L2NlcnQtYXV0aC5wb2Muc3lzLmNvbWNhc3QubmV0L2V4YW1wbGUuY2VydCJ9eyJhdHRlc3Qi
OiJBIiwiZGVzdCI6eyJ0biI6IisxMjE1NTU1MTIxMyJ9LCJpYXQiOiIxNDcxMzc1NDE4Iiwib3JpZyI6eyJ
0biI64oCdKzEyMTU1NTUxMjEyIn0sIm9yaWdpZCI6IjEyM2U0NTY3LWU4OWItMTJkMy1hNDU2
LTQyNjY1NTQ0MDAwMCJ9._28kAwRWnheXyA6nY4MvmK5JKHZH9hSYkWI4g75mnq9Tj2lW4
WPm0PlvudoGaj7wM5XujZUTb_3MA4modoDtCA;info=<https://cert.example2.net/example.c
ert>;alg=ES256"
  }
}
```

SHAKEN API for a Centralized Signing and Signature Validation Server



1. Request Sample

1. POST /stir/v1/verification HTTP/1.1
2. Host : stir.att.com
3. Accept : application/json
4. X-RequestID: AA97B177-9383-4934-8543-0F91A7A02836
5. Content-Type: application/json
6. Content-Length : …

```
{
  “verificationRequest”: {
            “from”: {
                    “tn”: “12155551212”
                  },
             “to”: {
                     “tn” : [
                             “12355551212”
                            ]
                     },
               “time”:  1443208345,
               “identity” : “eyJhbGciOiJFUzI1NiIsInR5cCI6InBhc3Nwb3J0IiwicHB0Ijoic2hha2VuIiwieDV1IjoiaHR0cDov
L2NlcnQtYXV0aC5wb2Muc3lzLmNvbWNhc3QubmV0L2V4YW1wbGUuY2VydCJ9eyJhdHRlc3QiOiJBIiwiZGVzdCI6eyJ0biI6
IisxMjE1NTU1MTIxMyJ9LCJpYXQiOiIxNDcxMzc1NDE4Iiwib3JpZyI6eyJ0biI64oCdKzEyMTU1NTUxMjEyIn0sIm9yaWdpZCI
6IjEyM2U0NTY3LWU4OWItMTJkMy1hNDU2LTQyNjY1NTQ0MDAwMCJ9._28kAwRWnheXyA6nY4MvmK5JKHZH9hSYk
WI4g75mnq9Tj2lW4WPm0PlvudoGaj7wM5XujZUTb_3MA4modoDtCA;info=<https://cert.example2.net/example.cert>
;alg=es256”
  }
}
```

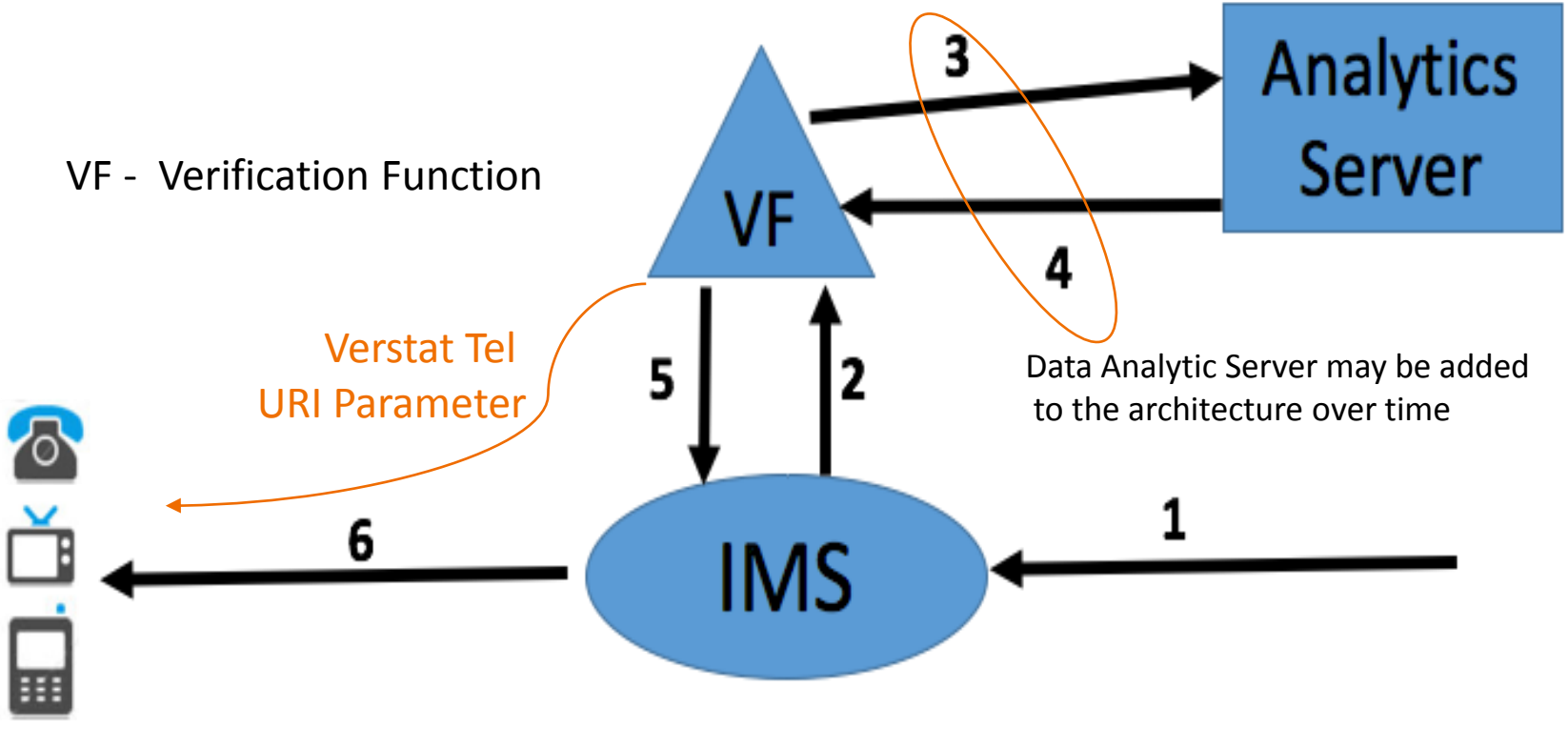
1. Response Sample (Success + Successful Validation)

1. HTTP/1.1 200 Ok
2. X-RequestID: AA97B177-9383-4934-8543-0F91A7A02836
3. Content-Type : application/json
4. Content-Length : …

```
{
  "verificationResponse": {
            “verstat”: “TN-Validation-Passed”
    }
}
```

Signaling Verification and Analytics Info

VF - Verification Function



Note: Interface between VF and Data Analytics Server is outside Industry Standards and may not be available in initial deployments
& Some Analytics may be performed in the network element that performs the VF

Signaling Verification

Verstat

- TN Validation Passed
- TN Validation Failed
- No TN Validation
- Future: same values above for CNAM

tel URI parameter in the P-Asserted-Identity
or FROM header field in a SIP requests
P-Asserted-Identity: tel:+14085264000;verstat=TN-Validation-Passed

Security Considerations

- The Verification Function must drop a verstat tel URI parameter received in an INVITE
- If the terminating UE does not support the "verstat" parameter value, it must discard the parameter
- The terminating UE will act on the "verstat" parameter value, if the 200 (OK) response to the UE REGISTER includes a Feature-Caps header field, as specified in RFC 6809° [190], with a "+g.3gpp.verstat" header field parameter

Thank you.