An Introduction and Overview of the STIR / SHAKEN Framework and Topics to Consider for 911 use of SHAKEN

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

5/1/2019

Topics to Consider for 911 use of SHAKEN

- What is being Attested to?
- Is there a need to Attest to the Calling Party in addition to the Priority Attestation?
- Will a CVT be invoked?
- Are 911 calls ever diverted?
- Are new “Verstat” values needed?
- Other?

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

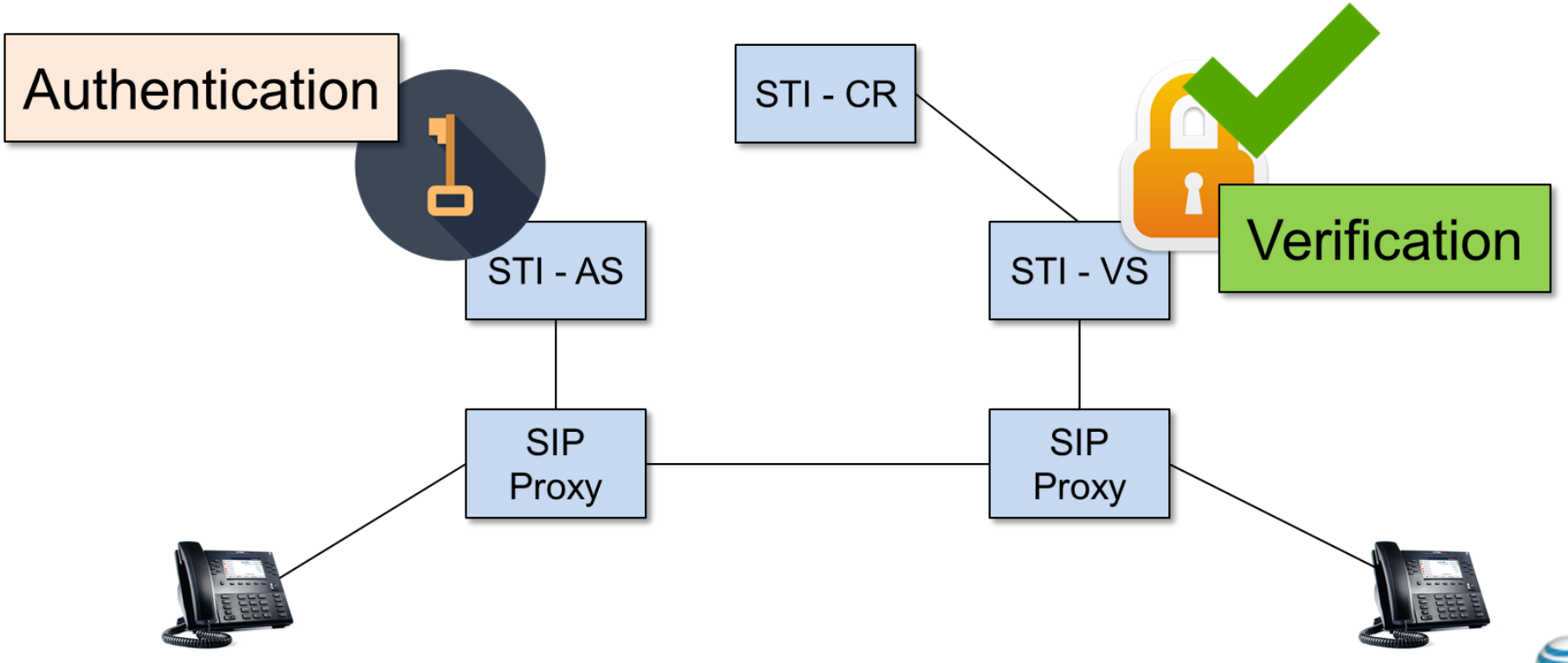
- **3GPP TS 24.229**, Technical Specification Group Core Network and Terminals; IP Multimedia Call Control Protocol based on Session Initiation Protocol (SIP) and Session Description Protocol (SDP); Stage 3
- **3GPP TS 29.163,** Technical Specification Group Core Network and Terminals; Interworking between 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)

SHAKEN 101

The essence of SHAKEN is:

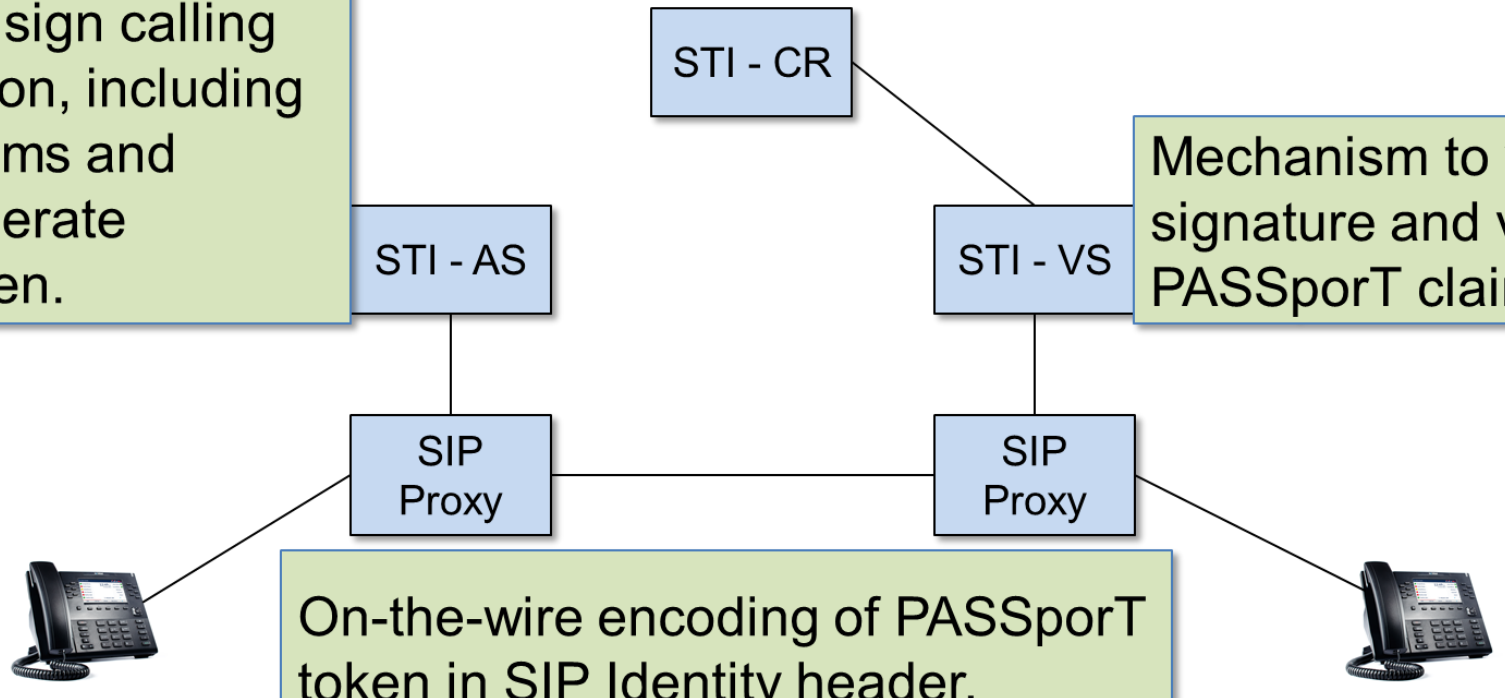
1. Originating service provider creates digital signature based on what it knows about the call origination:
   A. The customer and their right to use the number, or
   B. The customer (but not the number), or
   C. The point it enters their network
2. Assign “origid” to uniquely identify the call origination

SHAKEN Functions



Phase 1: SHAKEN – Published January 2017

Mechanism to sign calling party information, including attestation claims and “origid”, to generate PASSporT token.



Mechanism to verify signature and validate PASSporT claims.

On-the-wire encoding of PASSporT token in SIP Identity header.

ATIS-1000074: Signature based Handling of Asserted information using toKENs (i.e., SHAKEN)

SHAKEN Attestation Claims – Full Attestation

A. **Full Attestation**: The signing provider shall satisfy all of the following conditions:
   - 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 1**: The signing provider is asserting that their customer can "legitimately" use the number that appears as the calling party (i.e., the Caller ID). *…but they are not asserting that the call is actually from the number that appears as the calling party (i.e., SHAKEN allows "legitimate" spoofing)*
   - **NOTE 2**: Ultimately it is up to service provider policy to decide what constitutes "legitimate right to assert a telephone number"… *but it will impact "reputation"*

From ATIS-1000074

SHAKEN Attestation Claims – Partial Attestation

B. Partial Attestation: The signing provider shall satisfy all of the following conditions:

- Is responsible for the origination of the call onto its IP-based voice 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**: When Partial Attestation is used, each customer will have a unique origination identifier created and managed by the service provider, but the intention is that it will not be possible to reverse engineer the identity of the customer purely from the identifier or signature … allows data analytics to establish a reputation profile and assess the reliability of information asserted by the customer assigned this unique identifier. Also … for forensic analysis or legal action where appropriate.

From ATIS-1000074

SHAKEN Attestation Claims – Gateway Attestation

C. **Gateway Attestation**: The signing provider shall satisfy all of the following conditions:
   - Is the entry point of the call into its VoIP network
   - Has no relationship with the initiator of the call (e.g., international gateways)
   - **NOTE**: The token will provide a unique origination identifier of the node in the "origid" claim. (The signer is not asserting anything other than "this is the point where the call entered my network".)

From ATIS-1000074

Origination Identifier – (“origid”)

- **“origid”**: unique origination identifier (“origid”) is a globally unique opaque identifier corresponding to the service provider-initiated calls themselves, customers, classes of devices, or other groupings that a service provider might want to use for determining reputation or trace back identification of customers or gateways.
- For Full Attestation, in general, a single identifier will be used for all direct service provider-initiated calls on its VoIP network, but a service provider may also choose to have a pool of identifiers to differentiate geographic regions or classes of customers.
- For Partial Attestation, a single identifier per customer is required in order to differentiate calls both for trace back and reputation segmentation so that one customer’s reputation doesn’t affect other customers or the service provider’s call reputation.
- Best practices will likely develop as trace back and illegitimate call identification practices evolve.

From ATIS-1000074

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.cert"
}
```


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

Signing RPH for NS/EP

- This specification defines a new JSON Web Token claim for "rph", which provides an assertion for information in ’SIP Resource-Priority’ header field.

- The creator of a PASSporT object adds a "ppt" value of "rph" to the header of a PASSporT object, in which case the PASSporT claims MUST contain a "rph" claim, and any entities verifying the PASSporT object will be required to understand the "ppt" extension in order to process the PASSporT in question.

-

- A PASSPorT header with the "ppt“ included will look as follows:

```
{
"typ":"passport",
"ppt":"rph",
"alg":"ES256",
"x5u":"https://www.example.org/cert.cer"
}
```

Signing RPH for NS/EP

Specifically, the "rph" claim includes an assertion of the prioritylevel of the user to be used for a given communication session.

The value of the "rph" claim is an Object with one or more keys.

Each key is associated with a JSON Array. These arrays contain Strings that correspond to the r-values indicated in the ’SIP Resource- Priority’ header field.

```
{
"orig":{"tn":"12155550112"},
"dest":{["tn":"12125550113"]},
"iat":1443208345,
"rph":{"auth":["ets.0", "wps.0"]}
}
```

After the header and claims PASSporT objects have been constructed,

their signature is generated normally per the guidance in [RFC8225]

using the full form of PASSPorT.

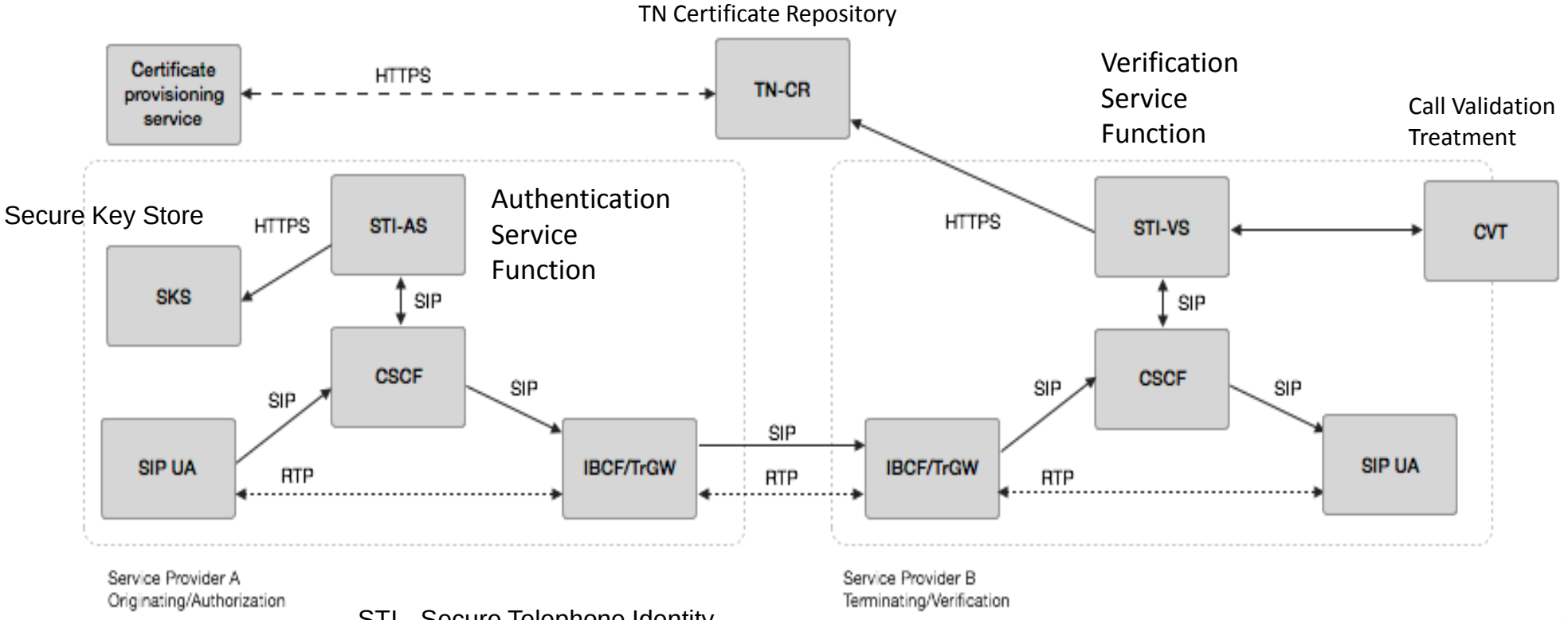
Deployment Assumptions for NS/EP

- RPH signing is only performed by the authenticating NS/EP service provider
- The authenticating NS/EP service provider will remove TN Identity Header prior to performing NS/EP authentication
- NS/EP call information will never be provided to a 3rd party CVT for data analytics
- An NS/EP carrier will use the same certificates for signing RPH, as they use for TN signing
- Based on local policy, an NS/EP service provider may choose to honor NS/EP calls without a signed RPH or process with normal priority
  - This may change over time taking into account maturity of signed PRH deployments and knowledge of the adjacent carrier
- As with TN siging, RPH signing will not survive if there is interworking with the PSTN

SIP Identity Header Example for SHAKEN

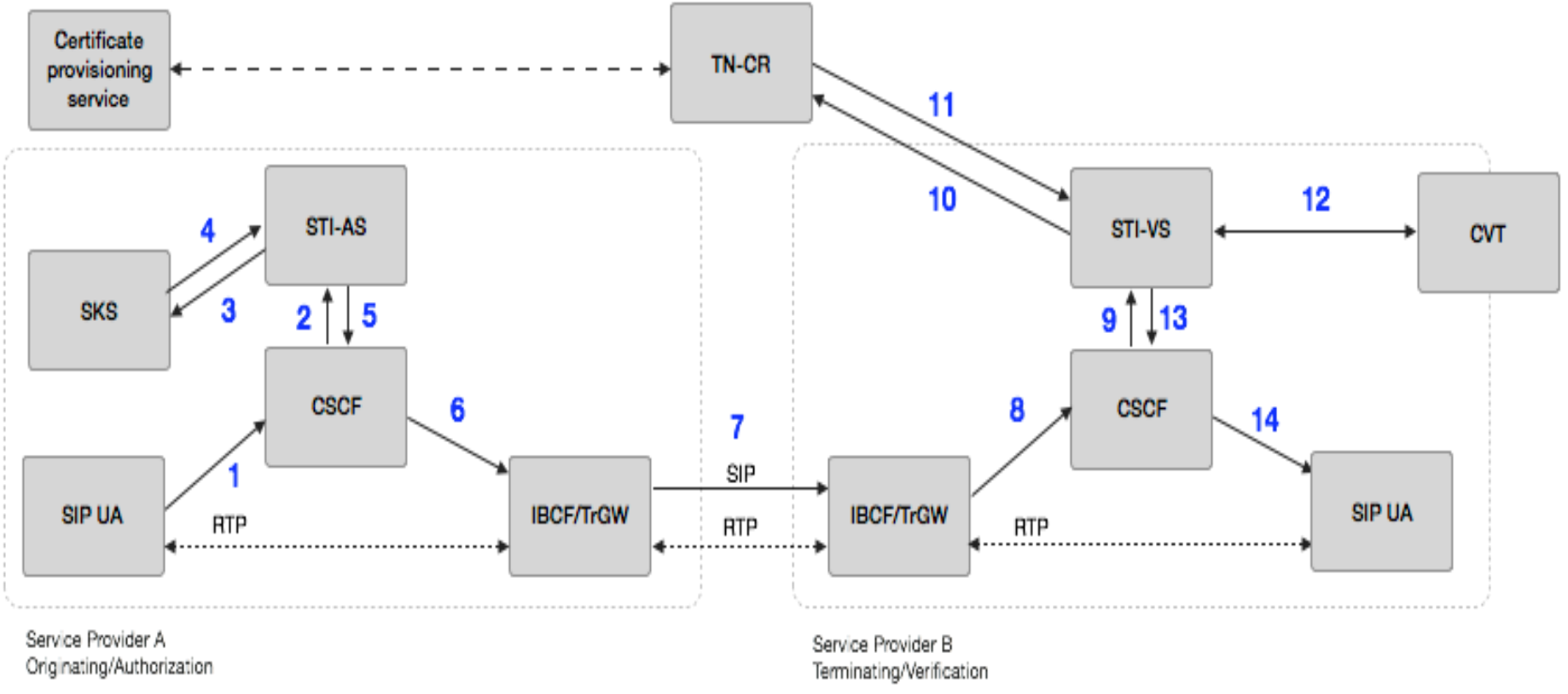
```
INVITE sip:+12155551213@tel.example1.net SIP/2.0
Via: SIP/2.0/UDP 10.36.78.177:60012;branch=z9hG4bK-524287-1---
77ba17085d60f141;rport
Max-Forwards: 69
Contact: <sip:+12155551212@69.241.19.12:50207;rinstance=9da3088f36cc528e>
To: <sip:+12155551213@tel.example1.net>
From: "Alice"<sip:+12155551212@tel.example2.net>;tag=614bdb40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

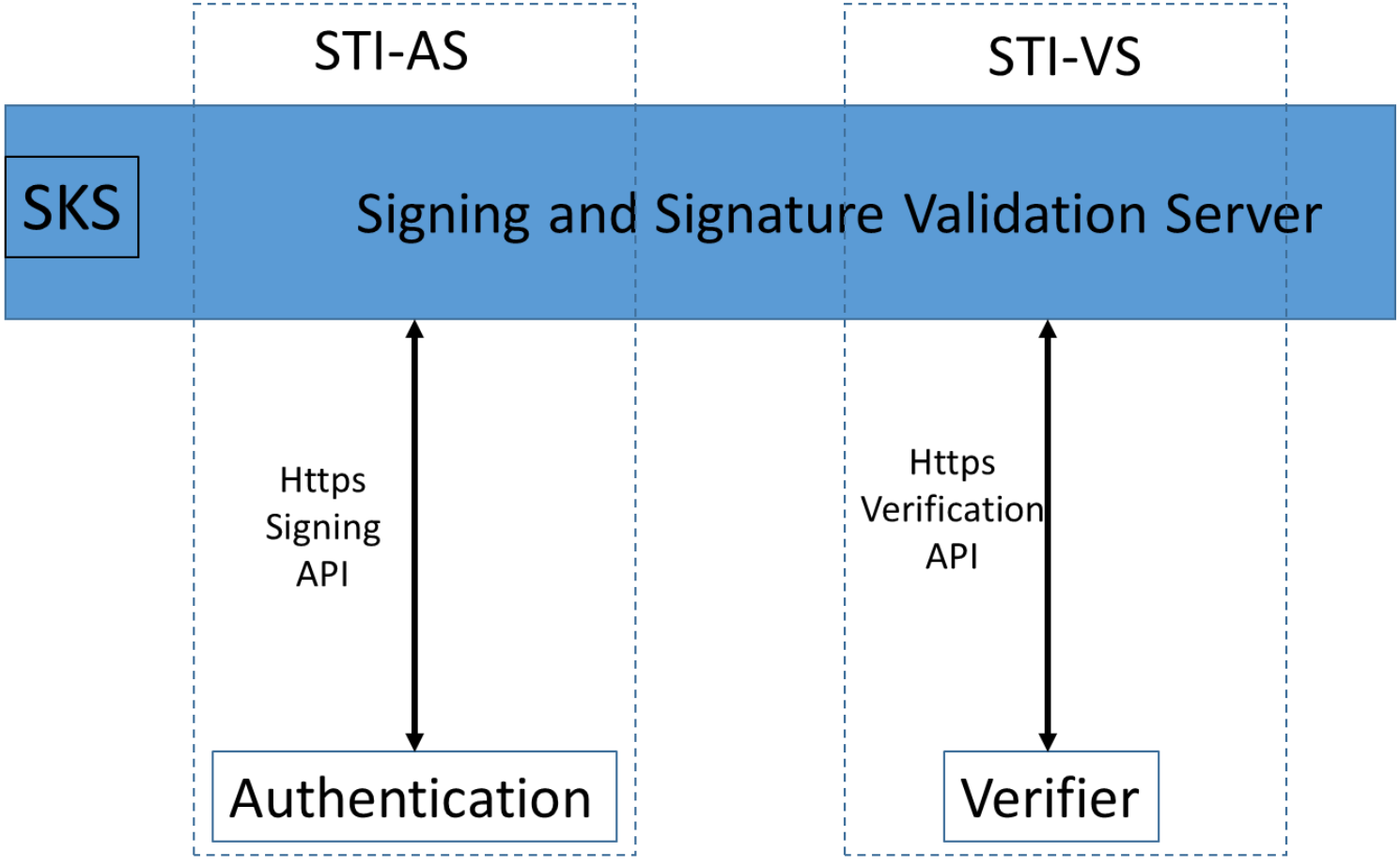


STI - Secure Telephone Identity

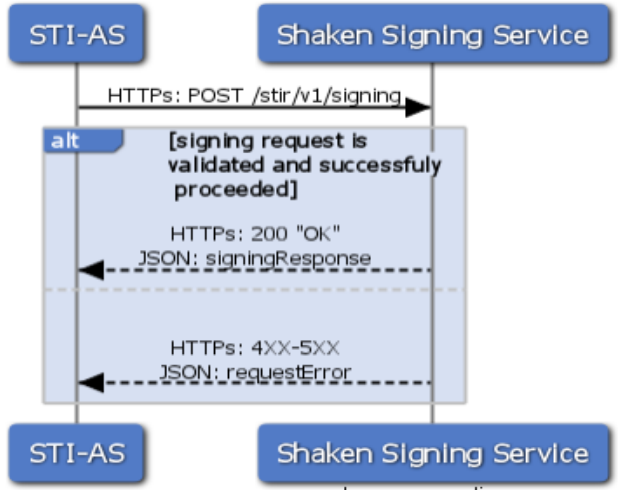
STIR/SHAKEN Basic Call Flow



Centralized Signing and Signature Validation Server



SHAKEN API for a Centralized Signing and Signature Validation Server



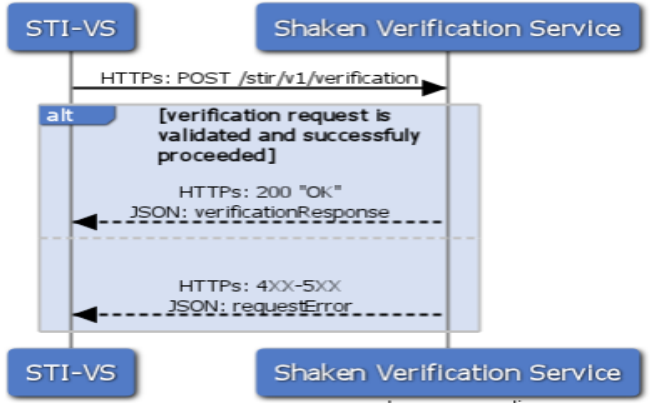
1. Request Sample

```
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”
  }
}
```

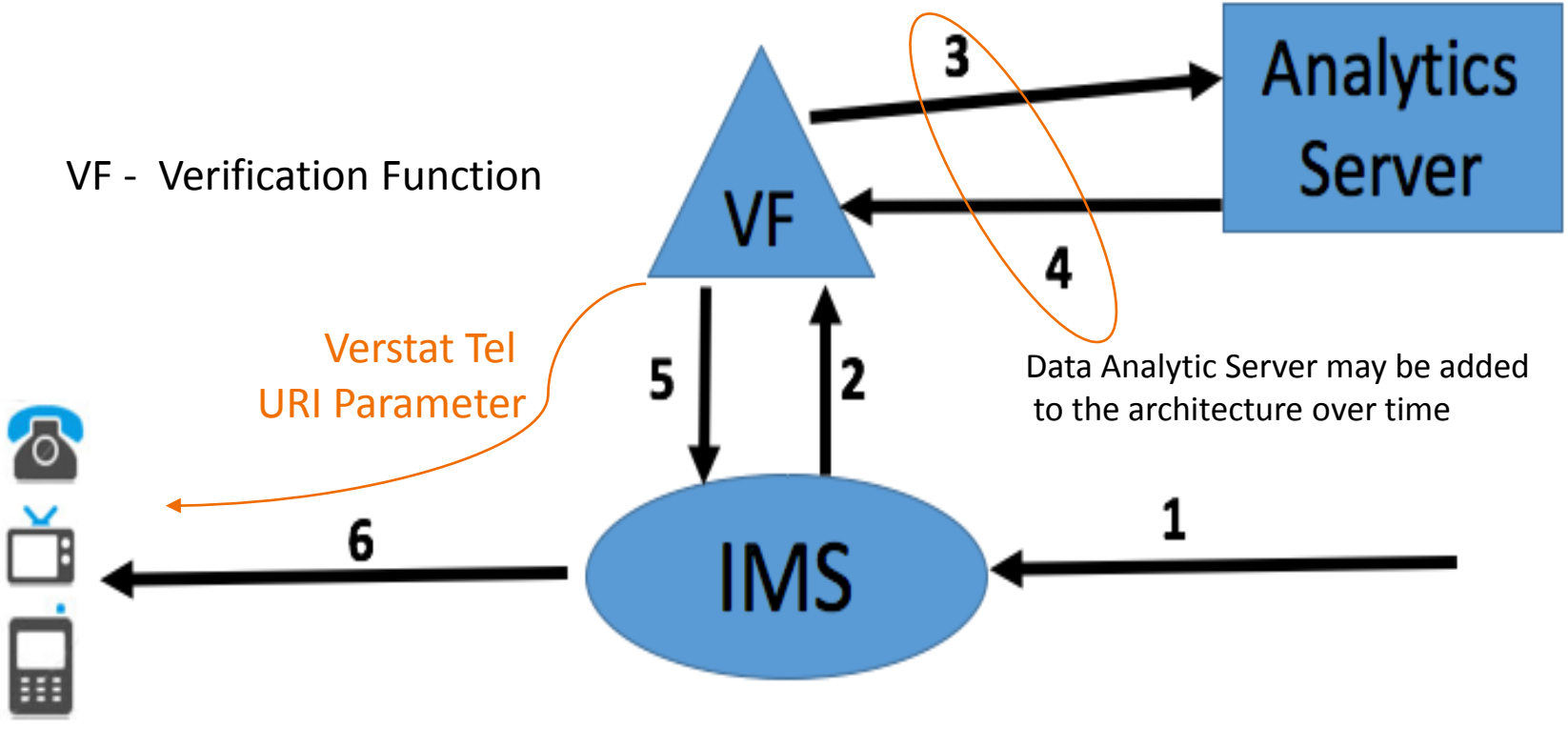
1. Response Sample (Success + Successful Validation)

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

Topics to Consider for 911 use of SHAKEN

- What is being Attested to?
- Is there a need to Attest to the Calling Party in addition to the Priority Attestation?
- Will a CVT be invoked?
- Are 911 calls ever diverted?
- Are new “Verstat” values needed?
- Other?

© 2015 AT&T Intellectual Property. All rights reserved. AT&T and the AT&T logo are trademarks of AT&T Intellectual Property.
AT&T Proprietary (Internal Use Only) Not for use or disclosure outside the AT&T companies except under written agreement.

Thank you.

© 2015 AT&T Intellectual Property. All rights reserved. AT&T and the AT&T logo are trademarks of AT&T Intellectual Property.
AT&T Proprietary (Internal Use Only) Not for use or disclosure outside the AT&T companies except under written agreement.