SIPNOC 2019
AT&T SHAKEN Deployment Case Study

Andy Jurczak
Principal Member of Technical Staff

12/03/2019

Agenda

- Current status of AT&T's SHAKEN Deployment
- Implementation Insights
- Display: Trust & Intent

AT&T

Current Status

AT&T STIR/SHAKEN Deployment Overview

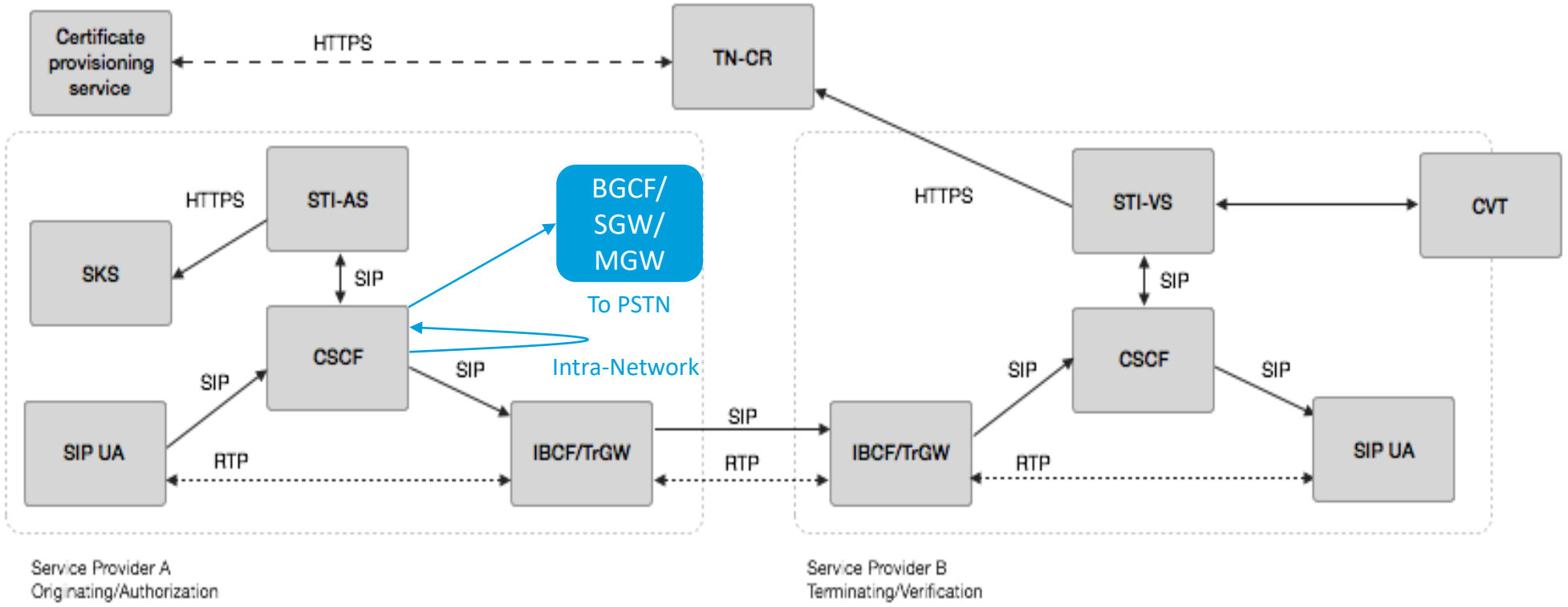
- STIR/SHAKEN is operational in AT&T's production network
  - Currently deployed on AT&T's VoLTE and Consumer VoIP (AT&T Phone) services
  - Authenticating/verifying 100% of intra-AT&T traffic for above services
  - Have begun the exchange of signed traffic with Comcast and T-Mobile
  - Ongoing testing and rollout with additional service providers
  - Tested with ATIS/Neustar Robocalling Testbed
- Manual exchange of self-signed root certificates
  - Will be interfacing with STI-PA/CA for certificates
- Support SHAKEN Error Responses
- In house development of STI-AS, STI-VS, TN-CR, SKS
  - 100% virtualized

AT&T

Implementation Insights

AT&T

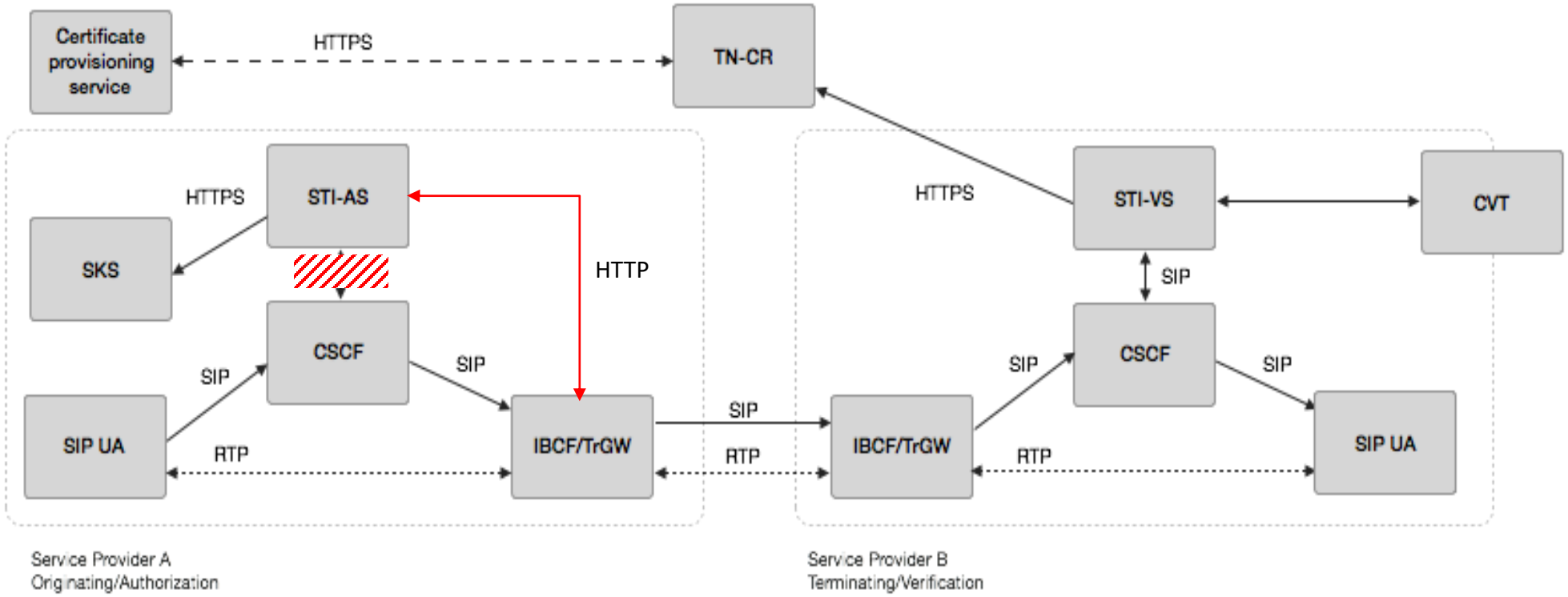
SHAKEN Reference Architecture (with additions)



- In reference model, signing is performed for all originating calls
- In practice, per call authentication is required, but per call signing is not
- Signing of intra-network calls result in unnecessary costs in terms of processing and call setup delay

AT&T

SHAKEN Reference Architecture: Signing at egress IBCF/SBC



- AT&T only signs calls sent to other SHAKEN-enabled service providers
  - Perform signing at the egress IBCF/SBC
  - Dramatic decrease in signing resources
- Makes use of ATIS-1000082 API (to be discussed later)

AT&T

Signing upon Egress for Inter-Network Calls: Issues

- Signing upon egress poses two issues:
  - Authentication is best performed upon origination
  - May not have origination information at egress (to be used in origid)
- If only signing inter-carrier calls, how are intra-carrier calls verified?

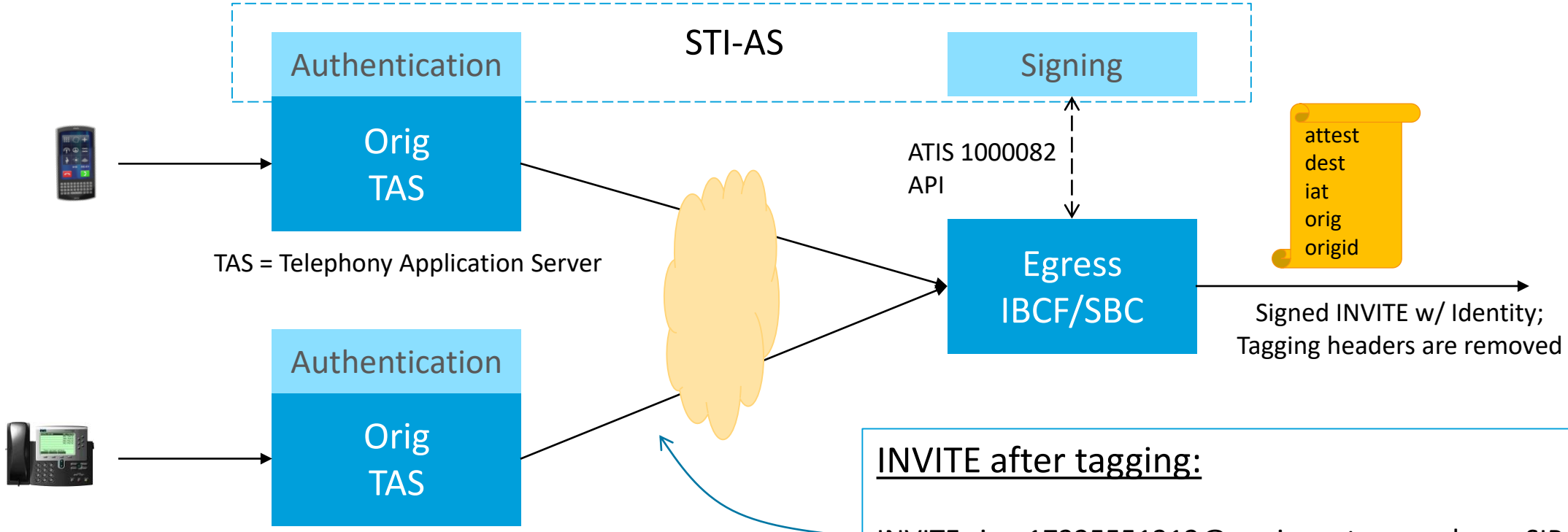
- Solution: “Tagging”

AT&T

Tagging

- Tagging adds information to SIP Signaling used to sign and/or verify calls
- Tagging performed upon origination, e.g. app server
- Tagging:
  - Inserts Attestation level based on Authentication results
  - Inserts Origid based on origination source
  - Inserts verstat
    - Verstat=TN-Validation-Passed (if successfully authenticated)
    - Verstat=No-TN-Validation (if unable to authenticate)
- SIP Headers used for Tagging are defined in 3GPP 24.229
  - Attestation-Info
  - Origination-Id

Tagging: Inter-carrier Call



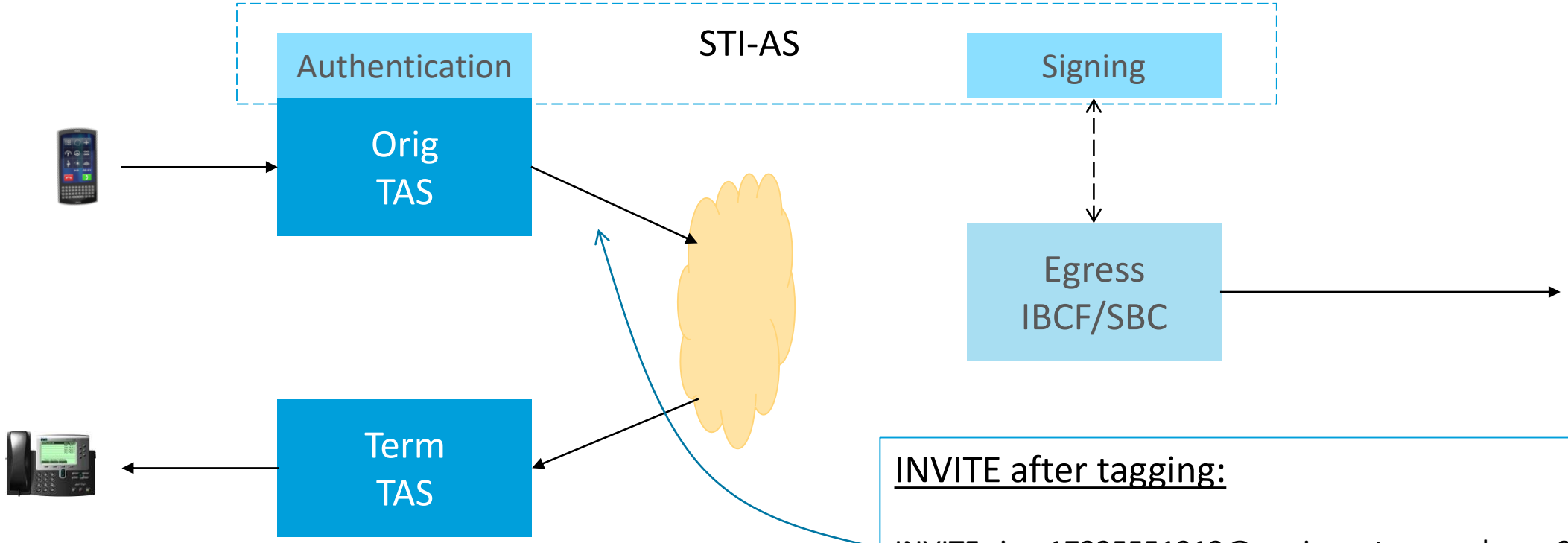
- Tagging provides “attest” and “origid” claim data to be used when call is signed
- Origination-Ids can be unique, per SHAKEN standards and recommendations

INVITE after tagging:

INVITE sip:+17325551212@carrier.net;user=phone SIP/2.0
…
…
Attestation-Info: A
Origination-Id: 2FB71193-D137-4DA1-9B34-E35CEA35498F
…

AT&T

Tagging: Intra-carrier Call



- Tagging provides “verstat”, used for intra-carrier calls in lieu of signing
- Verstat is removed by egress IBCF/SBC if call is routed to another carrier

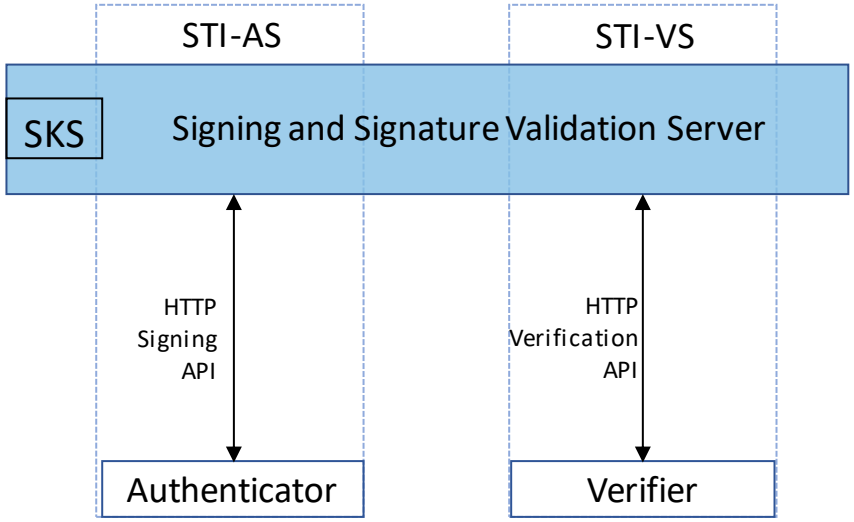
INVITE after tagging:

INVITE sip:+17325551212@carrier.net;user=phone SIP/2.0
…
…
Attestation-Info: A
Origination-Id: 2FB71193-D137-4DA1-9B34-E35CEA35498F
P-Asserted-Identity: <tel:+17325550123;verstat=TN-Validation-Passed>
…

AT&T

SHAKEN API for Signing and Verification

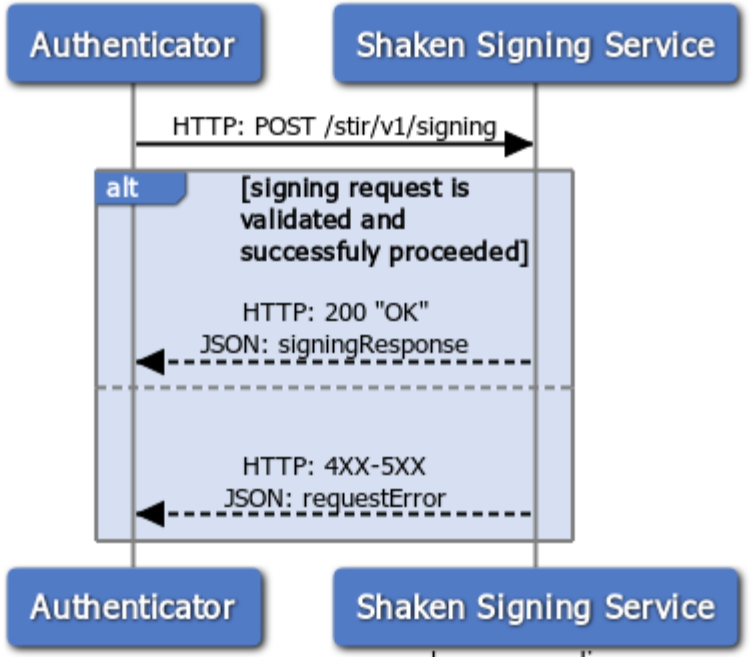
- Defined in ATIS-1000082 “Technical Report on SHAKEN APIs for a Centralized Signing and Signature Validation Server”
- Decomposes the STI-AS/VS functions
  - Particularly beneficial for call originations
- Supports centralized Signing/Verification resources along with distributed Authenticator/Verifier
- Authenticator can also be decomposed
  - Use Tagging to convey attestation and origid



- “Authenticator” determines the Attestation level and origid to be used for the call
- “Verifier” can perform syntax checking, canonicalization, etc. to screen pre-verification errors.

AT&T

SHAKEN API for Signing

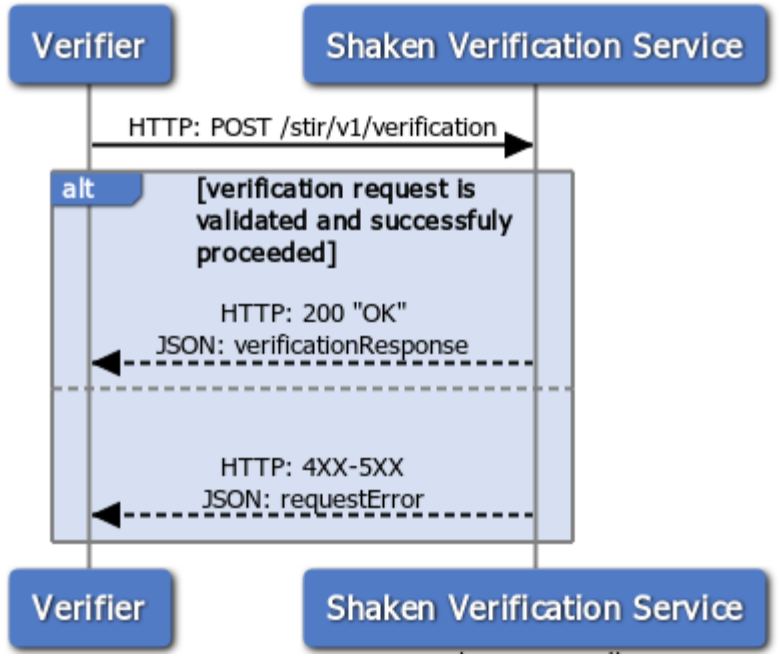



```
POST  /stir/v1/signing  HTTP/1.1
Host: stir.example.com
Accept: application/json
X-InstanceID : de305d54-75b4-431b-adb2-eb6b9e546014
X-RequestID: AA97B177-9383-4934-8543-0F91A7A02836
Content-Type: application/json
Content-Length: …
{
   "signingRequest”: {
              "attest": “A”,
              "orig”: {
                        “tn”: “12155551212”
                    },
               “dest”: {
                         “tn”: [
                                   “12355551212”
                                ]
                     },
               "iat”: “1443208345”,
               “origid”: “de305d54-75b4-431b-adb2-eb6b9e546014”
    }
}
```

```
HTTP/1.1 200 OK
X-RequestID: AA97B177-9383-4934-8543-0F91A7A02836
Content-Type: application/json
Content-Length: …
 {
   "signingResponse": {
    "identity":
“eyJhbGciOiJFUzI1NiIsInBwdCI6InNoYWtlbiIsInR5cCI6InBhc3Nwb3J0IiwieDV1IjoiaHR0cHM6Ly9
jZXJ0LmV4YW1wbGUyLm5ldC9leGFtcGxlLmNlciJ9.eyJhdHRlc3QiOiJBIiwiZGVzdCI6eyJ0biI6Wy
IxMjM1NTU1MTIxMiJdfSwiaWF0IjoiMTQ0MzIwODM0NSIsIm9yaWciOiJ0biI6MTIxNTU1NTEyMTI
ifSwib3JpZ2lkIjoiZGUzMDVkNTQtNzViNC00MzFiLWFkYjItZWI2YjllNTQ2MDE0In0=._28kAwRWn
heXyA6nY4MvmK5JKHZH9hSYkWI4g75mnq9Tj2lW4WPm0PlvudoGaj7wM5XujZUTb_3MA4mod
oDtCA;info=<https://cert.example2.net/example.cer>”
  }
}
```


AT&T

SHAKEN API for Verification




```
POST  /stir/v1/verification  HTTP/1.1
Host: stir.example.com
Accept: application/json
X-InstanceID : de305d54-75b4-431b-adb2-eb6b9e546014
X-RequestID: AA97B177-9383-4934-8543-0F91A7A02836
Content-Type: application/json
Content-Length: …
{
   “verificationRequest”: {
                “from”: {
                        “tn”: “12155551212”
                    },
                “to”: {
                        “tn”: [
                                “12355551212”
                            ]
                    },
                “time”: “1443208345”,
                “identity”:
“eyJhbGciOiJFUzI1NiIsInBwdCI6InNoYWtlbiIsInR5cCI6InBhc3Nwb3J0IiwieDV1IjoiaHR
0cHM6Ly9jZXJ0LmV4YW1wbGUyLm5ldC9leGFtcGxlLmNlciJ9.eyJhdHRlc3QiOiJBIiwiZ
GVzdCI6eyJ0biI6WyIxMjM1NTU1MTIxMiJdfSwiaWF0IjoiMTQ0MzIwODM0NSIsIm9ya
WciOiJ0biI6MTIxNTU1NTEyMTIifSwib3JpZ2lkIjoiZGUzMDVkNTQtNzViNC00MzFiLWF
kYjItZWI2YjllNTQ2MDE0In0=._28kAwRWnheXyA6nY4MvmK5JKHZH9hSYkWI4g75mn
q9Tj2lW4WPm0PlvudoGaj7wM5XujZUTb_3MA4modoDtCA;info=<https://cert.example2
.net/example.cer>”
   }
}
```

```
HTTP/1.1 200 OK
X-RequestID: AA97B177-9383-4934-8543-0F91A7A02836
Content-Type: application/json
Content-Length: …
{
   "verificationResponse": {
                “verstat”: “TN-Validation-Passed”
                                }
}
```


AT&T

Display: Trust & Intent

Trust – Reputation - Intent

Trust – Do we believe the calling number is correct?

Reputation

Every phone number has a Story…

Status – Is it connected? Valid?

Ownership – Who pays the bill?

Behavior – What does the number do?

Connections – How does it communicate?

Complaints – What others say about this number?

Reputation is the aggregated view of this Story. Analytics Engines use past reputation to predict **intent**.

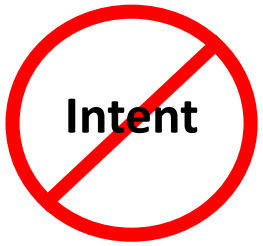
Trust combined with **intent** allow more accurate decisions whether call is to be blocked, flagged or allowed.

AT&T

When to display a Positive Indicator: Trust & Intent

Today

SHAKEN Only

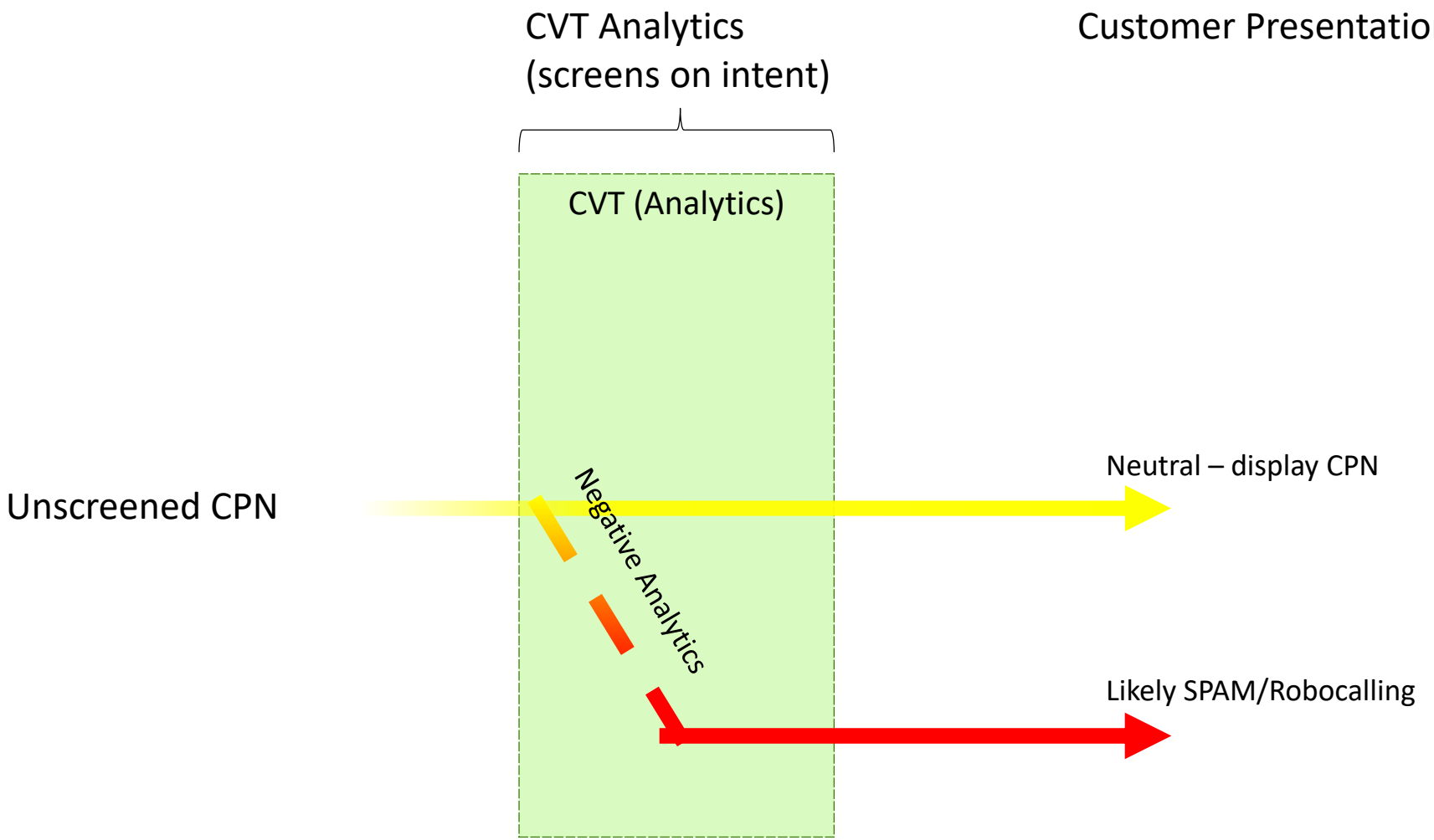


SHAKEN + Analytics

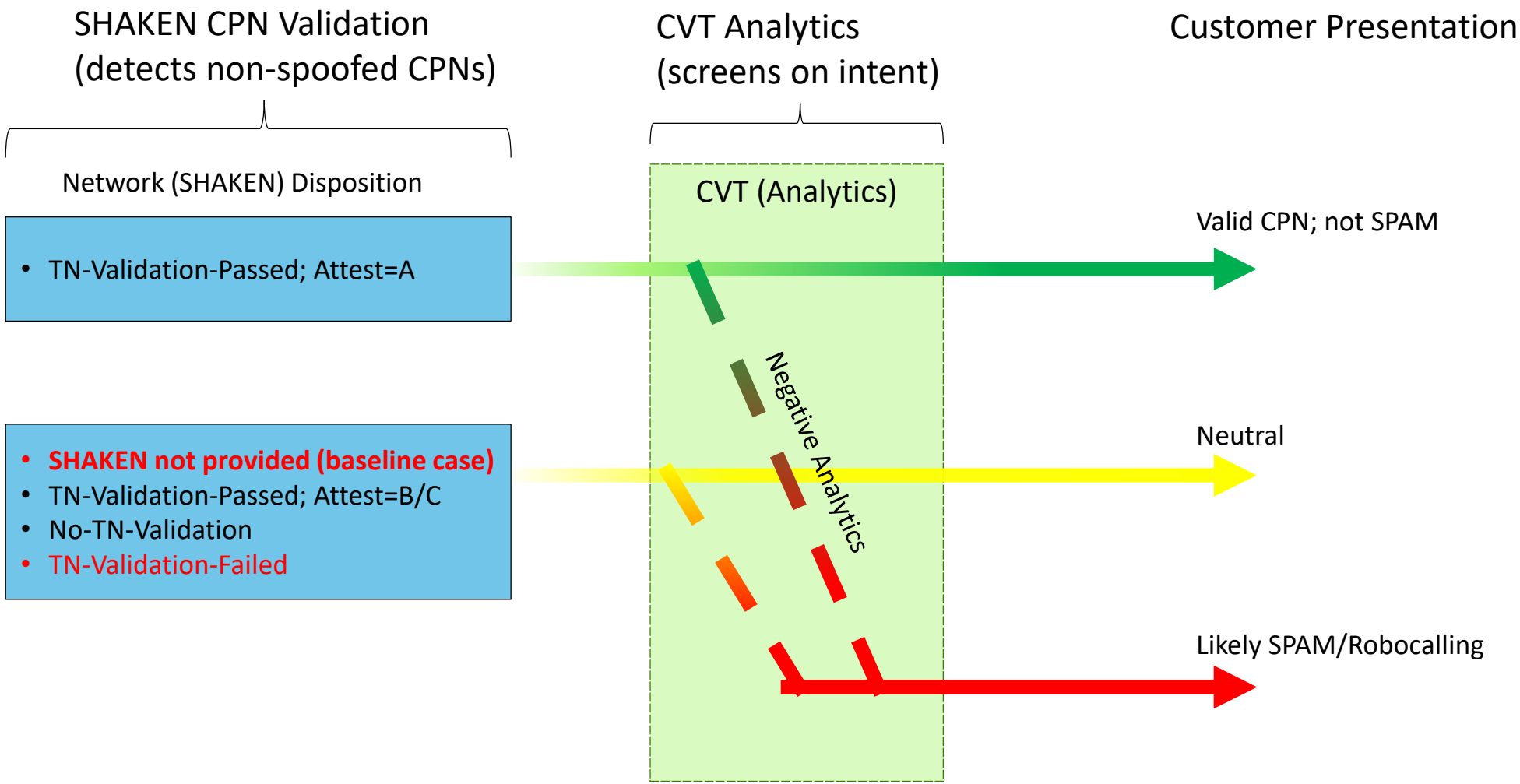
✓ Trust Identity of Number
✓ Predict Intent of Caller

AT&T

Display: Analytics Only

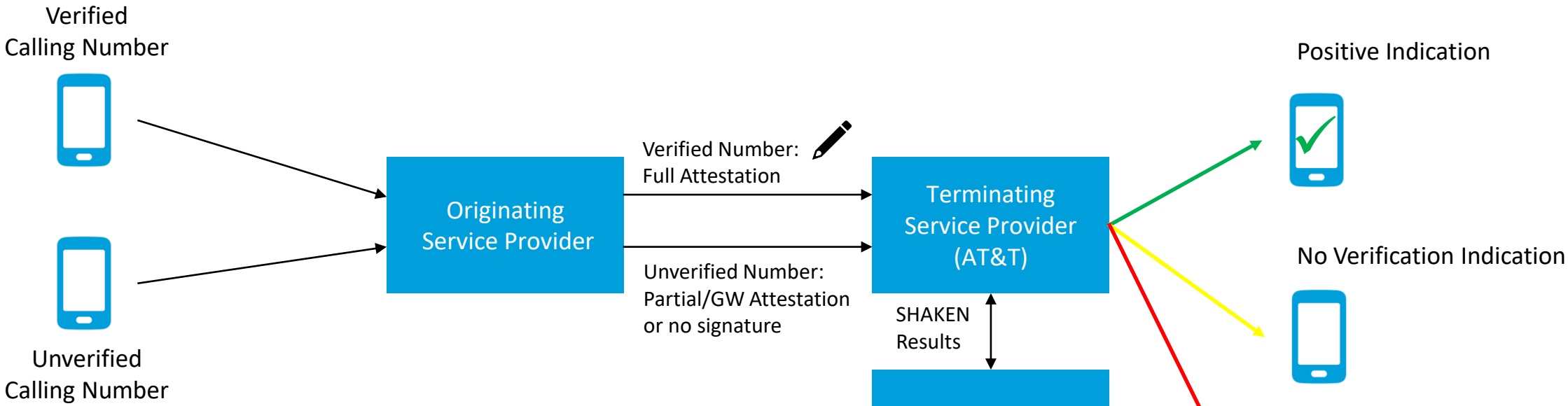


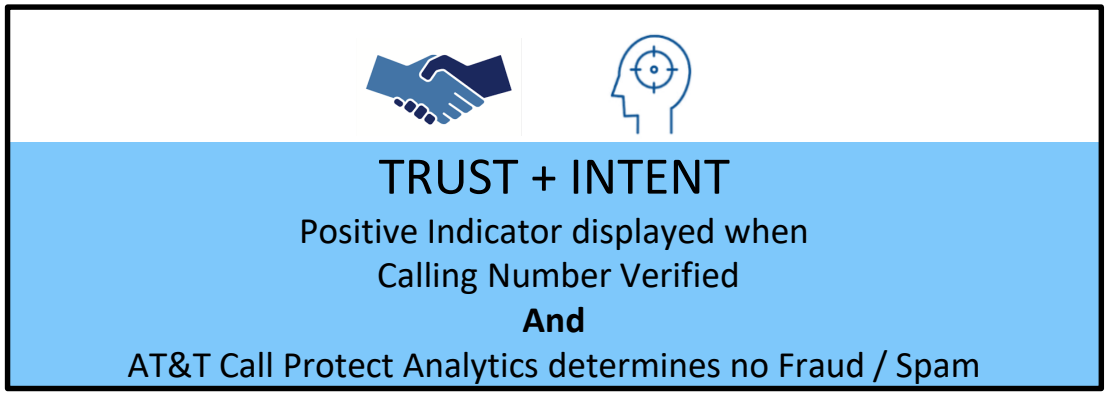
Display: SHAKEN + Analytics



AT&T

SHAKEN Display





AT&T


AT&T