VoIP Zero Trust Architecture Strategy

Presented By:

Netmaker Communications, LLC

Winchester, Virginia

2024

Company Overview

Veteran Owned Small Business
VOSB
cVE

Netmaker • Communications • LLC
Winchester • Virginia

Internet, Telecom, & WiFi Services

Surveillance Services

Cybersecurity Services

Commercial Services Division

Human Resources

Datacenter Facility

Accounting & Contracting

Marketing & Sales

Corporate Operations Division

Public Safety Communications Consulting

Unified Communications, IP Networking & Cybersecurity Consulting

Government Consulting Division

GTE
NORTEL NETWORKS

Netmaker • Communications • LLC

30+ Years Experience

GSA Schedule Contract
47QTCA22D002Z

Purpose

- Voice modernization initiatives represents the transition of legacy TDM voice services and technology to Voice over IP (VoIP). With the introduction of IP, combined with national attacks on public safety infrastructures, implementing a Zero Trust Architecture (ZTA) framework for VoIP could help mitigate these risks.
- Incorporating the ZTA framework within VoIP should be done within the Session Initiation Protocol (SIP) header. This is accomplished by utilizing secure keys; identity verification service; identity authentication service; certificate authority; certificate repository; and key management servers.

Data – Voice Cybersecurity Crosswalk

Familiar

DATA NETWORK SECURITY THREATS

Parallel

VOICE NETWORK SECURITY THREATS

Data Network Security Tools

Network Firewalls

Network Intrusion Prevention Systems (NIPS)

Network Authentication

Zero Trust

Unauthorized access & malicious activity	Unauthorized access & malicious activity
DDoS	TDoS
Harassing Traffic & Spam	Robocalls, Spam Harassing Calls
Man in the Middle Attacks	Social Engineering CC Fraud, & Theft
Phishing, Social Engineering	Vishing, Spoofing & AI-Generated Voice

Voice Network Security Tools

Voice Firewall

Voice IPS

Red List

Reporting & Analytics

FCC Requirement

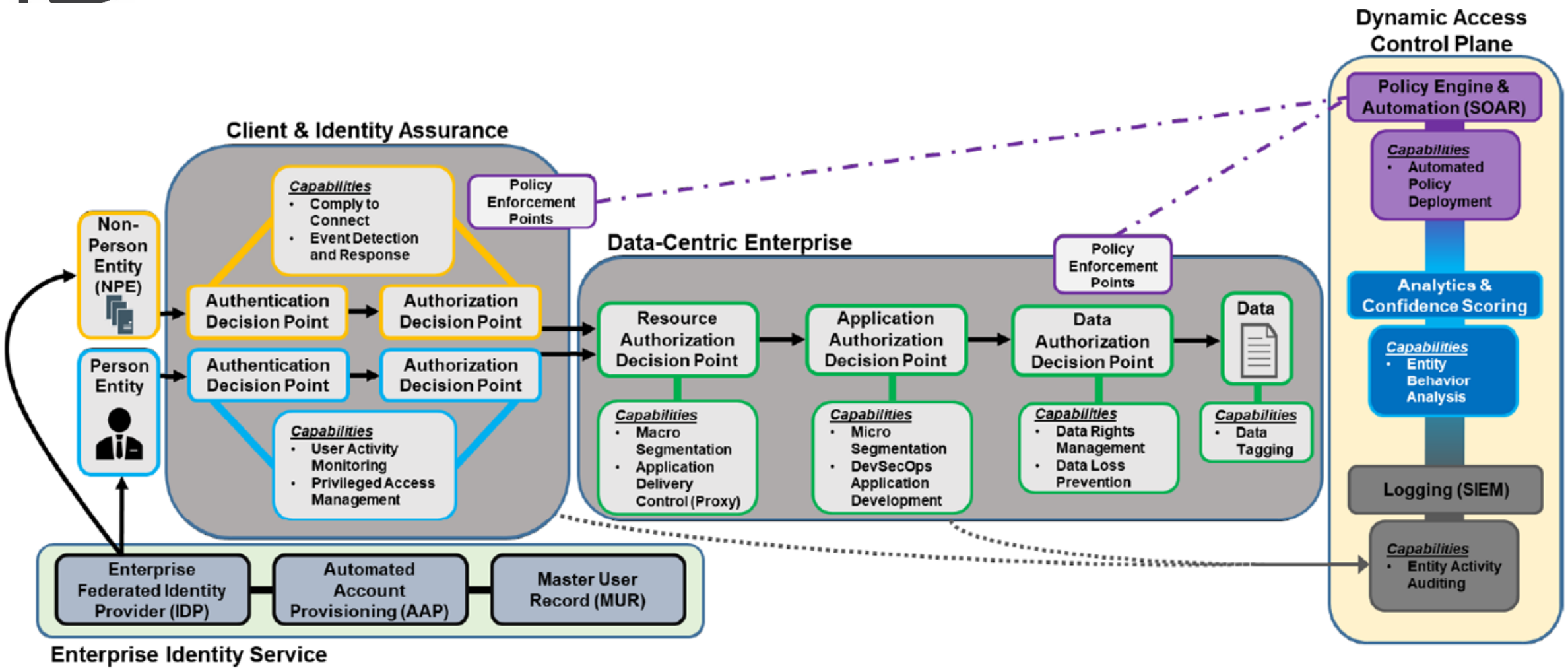
- In 2020, the FCC adopted rules requiring voice service providers to implement Secure Telephone Identity Revisited (STIR) and Signature-based Handling of Asserted Information Using toKENs (SHAKEN) in the IP portions of their voice networks by June 30, 2021.
- Commission rules require voice service providers to implement STIR/SHAKEN in the IP portions of their networks.
- Voice service providers must:

  (1) authenticate and verify caller ID information for all SIP calls that exclusively transit their networks;

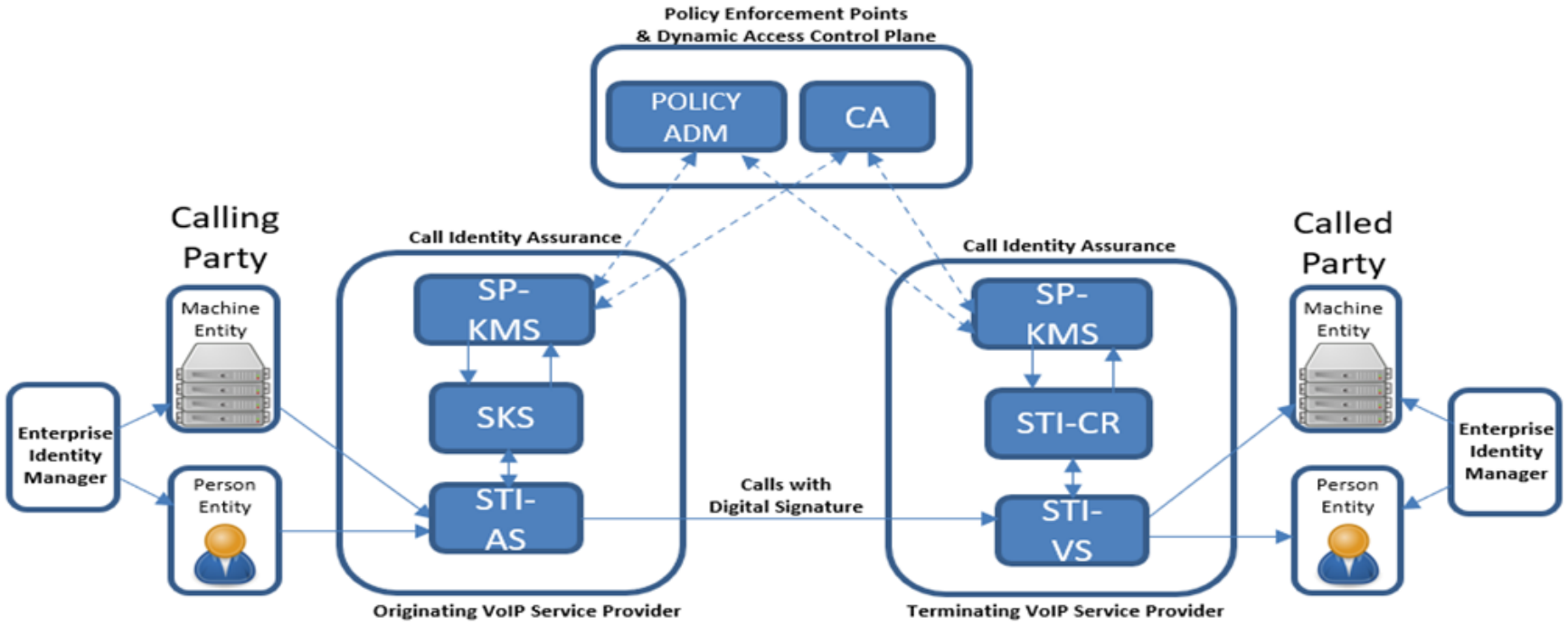
  (2) authenticate caller ID information for all SIP calls originating on their networks that they will pass to another voice service or intermediate provider and, to the extent technically feasible, transmit such calls with authenticated caller ID information to the next provider in the call path;

  (3) verify caller ID information for all SIP calls they receive from other providers that they terminate and for which caller ID information has been authenticated.

DoD Zero Trust OV-1



VoIP ZTA Framework

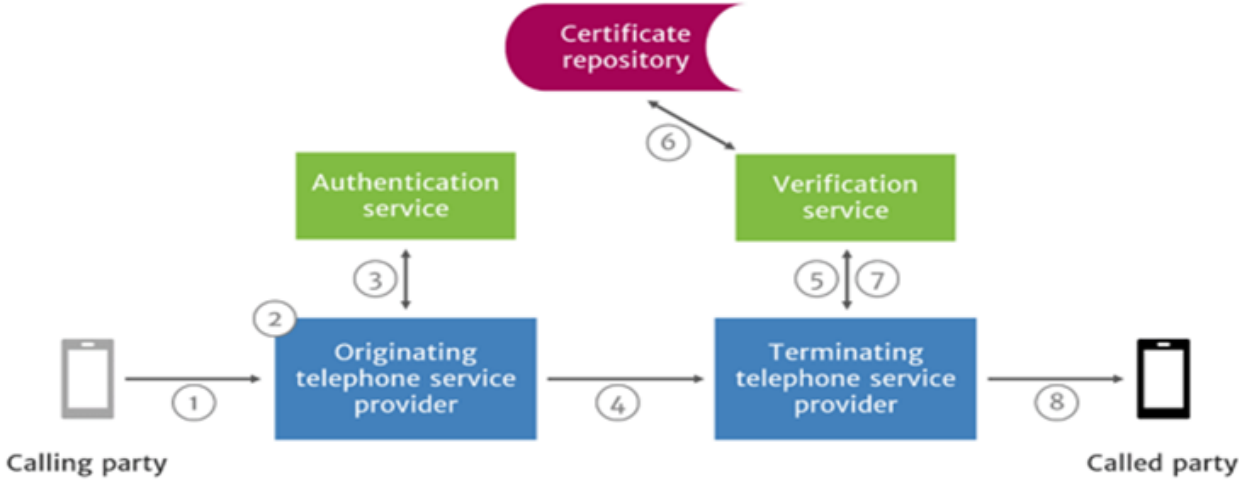


- Secure Key Store (SKS)
- Secure Telephony Identity - Authentication Service (STI-AS)
- Secure Telephony Identity - Verification Service (STI-VS)
- Service Provider – Key Management Server (SP-KMS)
- Secure Telephony Identity - Certificate Repository (STI-CR)
- Certificate Authority (CA)

Digital signature Inserted in SIP INVITE header

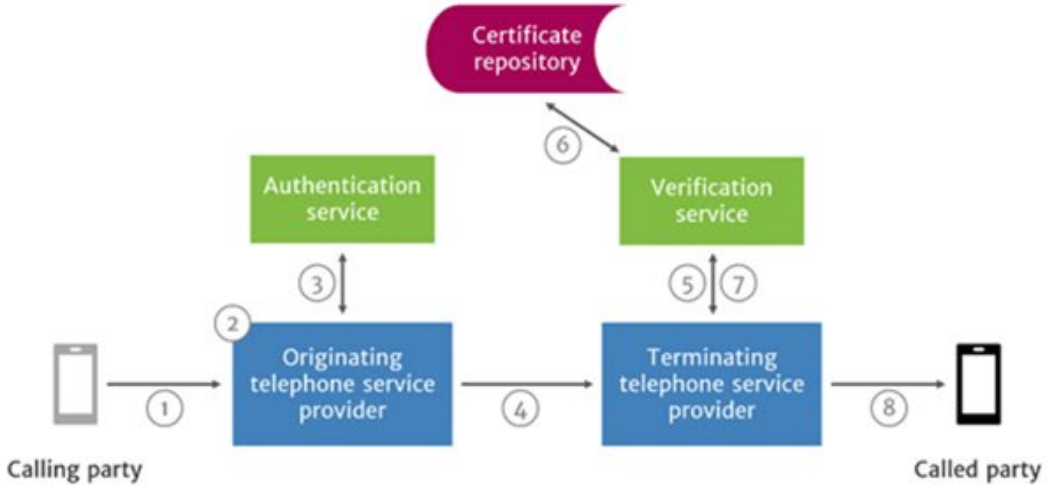

```
INVITE sip:18001234567@example.com:5060 SIP/2.0
Via: SIP/2.0/UDP example.com:5060
From: "Alice" <sip:14045266060@5.6.7.8:5060>;tag=123456789
To: "Bob" <sip:18001234567@1.2.3.4:5060>
Call-ID: 1-12345@5.6.7.8
CSeq: 1 INVITE
Max-Forwards: 70
Identity:
ey3hbGciOiAiRVMyNTYiLCJwcHQiOiAic2hha2VuIiwidHlwIjogInBhc3Nwb3J0IiwieOV1IjogImh0dHBzOi8vY2Vy
dGlmaWNhdGVzLmNsZWFyaXAuY29tL2IxNWQ3Y2M5LTBmMjYtNDZjMi04M2VhLWEzZTYzYTgyZWMzYS83Y2M0ZGI2OTVk
MTNlZGFkYTRkMWY5ODYxYjliODBmZS5jcnQifQ.ey3hdHRlc3QiOiAiQ5IsImRlc3QiOiB7InRuIjogWyIxNDA0NTI2N
jA2MCJdfSwiaWF0IjogMTU0ODg1OTk4Miwib3JpZyI6IHsidG4iOiAiMTgwMDEyMzQ1NjcifSwib3JpZ2lkIjogIjNhN
DdjYTIzLWQ3YWItNDQ2Yi04MjFkLTMzZDVkZWVkYmVkNCJ9.S_vqkgCk88ee9rtkB9P6a6ru0ncDfSrdb1GyK_mJj-
10hsiW-dMF7eCjDVARLR7EZSZwiu0fd4H_QD_9ZSU2bg;info=<https://certificates.clearip.com
/b15d7cc9-0f26-46c2-83ea-a3e63a82ec3a/7cc4db695d13edada4d1f9861b9b80fe.crt>;alg=ES256;
ppt=shaken
```

How it works



1. A SIP INVITE is received by the Calling Party's Carrier
2. The Calling Party's Carrier Checks the Call Source & DID to Determine how to Attest for the Validity of the DID
   - Full Attestation (Caller DID is Registered in Carrier Soft Switch)
   - Partial Attestation (Caller making Call Behind IP-PBX)
   - Gateway Attestation (Caller making Call from International Gateway)
3. Carrier Generates a SIP Identity Header from Data Received from Authentication Service

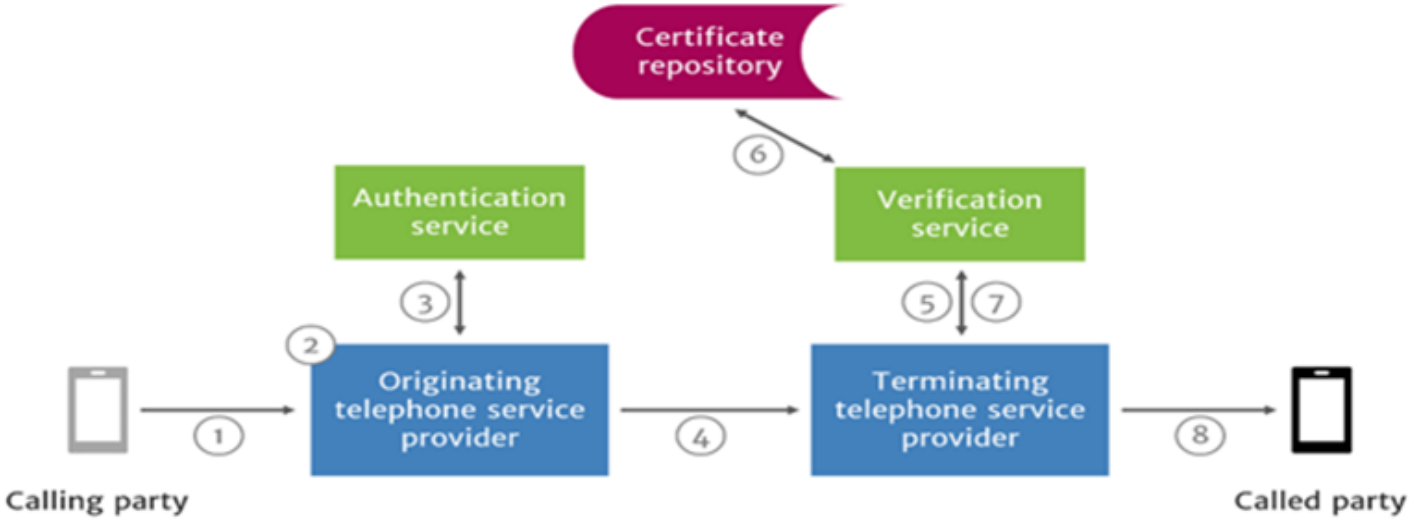
How it works




```
INVITE sip:18001234567@example.com:5060 SIP/2.0
Via: SIP/2.0/UDP example.com:5060
From: "Alice" <sip:14045266060@5.6.7.8:5060>;tag=123456789
To: "Bob" <sip:18001234567@1.2.3.4:5060>
Call-ID: 1-12345@5.6.7.8
CSeq: 1 INVITE
Max-Forwards: 70
Identity:
eyJhbGciOiAiRVMyNTYiLCJwcHQiOiAic2hha2VuIiwidHlwIjogInBhc3Nwb3J0IiwieDV1IjogImh0dHBzOi8vY2Vy
dGlmaWNhdGVzLmNsZWFyaXAuY29tL2IxNWQ3Y2M5LTBmMjYtNDZjMi04M2VhLWEzZTYzYTgyZWMzYS83Y2M0ZGI2OTVk
MTNlZGFkYTRkMWY5ODYxYjliODBmZS5jcnQifQ.eyJhdHRlc3QiOiAiQSIsImRlc3QiOiB7InRuIjogWyIxNDA0NTI2N
jA2MCJdfSwiaWF0IjogMTU0ODg1OTk4Miwib3JpZyI6IHsidG4iOiAiMTgwMDEyMzQ1NjcifSwib3JpZ2lkIjogIjNhN
DdjYTIzLWQ3YWItNDQ2Yi04MjFkLTMzZDVkZWVkYmVkNCJ9.S_vqkgCk88ee9rtk89P6a6ru0ncDfSrdb1GyK_mJj-
10hsLW-dMF7eCjDYARLR7EZSZwiu0fd4H_QD_9Z5U2bg;info=<https://certificates.clearip.com
/b15d7cc9-0f26-46c2-83ea-a3e63a82ec3a/7cc4db695d13edada4d1f9861b9b80fe.crt>alg=ES256;
ppt=shaken
```

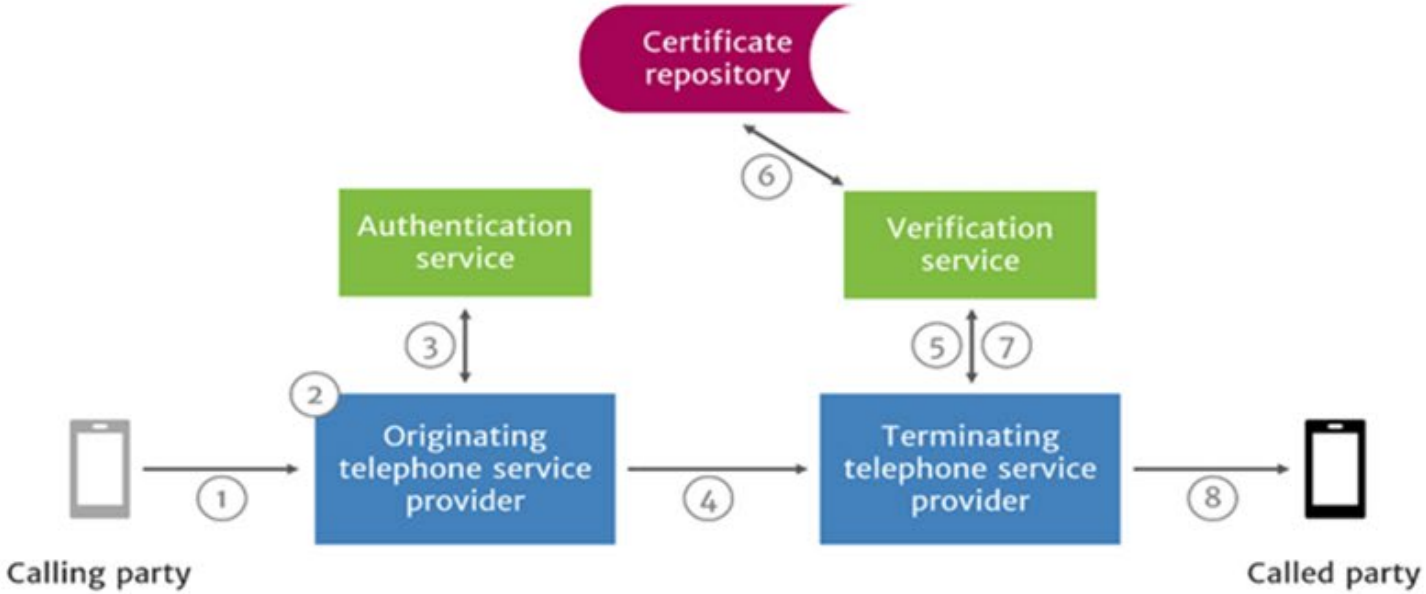

4. SIP INVITE with Inserted SIP Identity Header is Transmitted to Carrier Hosting Destination Party DID, with the ID Token being Sent over the Internet or Out-of-Band to the Destination Carrier's Call Placement Service
5. The SIP INVITE with Identity Header is Passed to the Verification Service

How it works



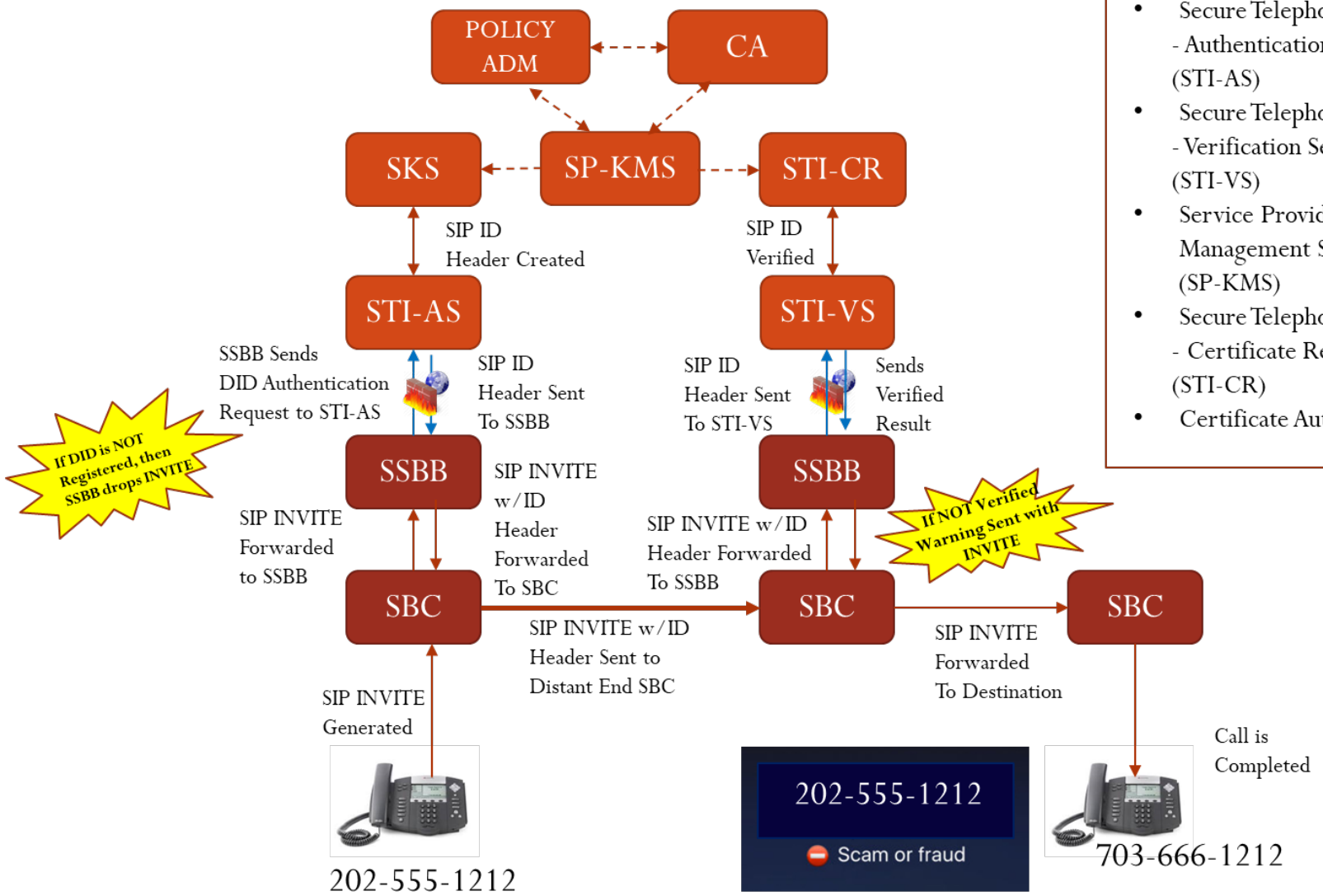
6. The Verification Service obtains the Digital Certificate of the Originating Carrier from the Public Certificate Repository and begins a multi-step verification process. If all verification steps are successful, then the calling number has not been spoofed.
   - The SIP Identity header is base64 URL decoded and the details are compared to the SIP INVITE message.
   - The public key of the certificate is used to verify the SIP Identity header signature.
   - The certificate chain of trust is verified.

How it works



7. The verification service returns the results to the terminating Carrier's Soft Switch or SBC.
8. The call is completed to the called party

Implemented within the DoD Environment



- Secure Key Store (SKS)
- Secure Telephony Identity - Authentication Service (STI-AS)
- Secure Telephony Identity - Verification Service (STI-VS)
- Service Provider – Key Management Server (SP-KMS)
- Secure Telephony Identity - Certificate Repository (STI-CR)
- Certificate Authority (CA)

Application Layer Security from SecureLogix

SecureLogix

Together

SBCs & Call Defense

=

Cyber Wrapper for Voice

Telephone Number Validation

- Outbound Call Trust Services:
  - Phone number reputation defense
  - Call branding
  - Spoofing protection

Data Analytics Vendors

SecureLogix established a relationship with key vendors

TNS

TNS has software in Verizon wireless network

TNS given responsibility to determine what will be displayed on Verizon wireless phone

TNS has algorithms and crowd source to evaluate source phone numbers calling Verizon wireless subscribers

TNS gives each source phone number a reputation

If phone number gets a negative reputation, then calls from that phone number are labeled as Spam or Fraud

verizon

Hiya

Hiya has software in AT&T wireless network

Hiya given responsibility to determine what will be displayed on AT&T wireless phone

Hiya has algorithms and crowd source to evaluate source phone numbers calling AT&T wireless subscribers

Hiya gives each source phone number a reputation

If phone number gets a negative reputation, then calls from that phone number are labeled as Spam or Fraud

AT&T

First Orion

First Orion has software in T-Mobile network

First Orion given responsibility to determine what will be displayed on T-Mobile phone

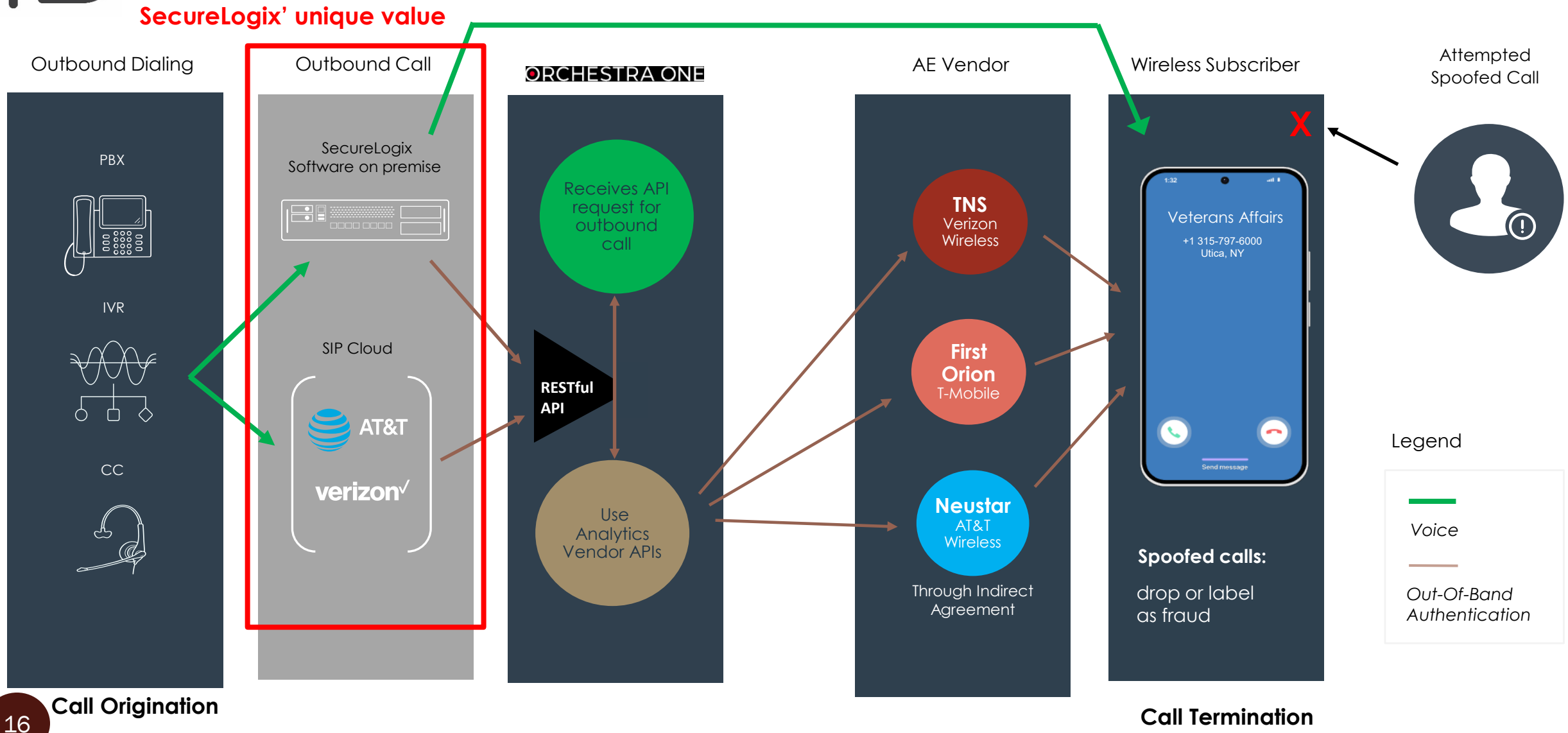
First Orion has algorithms to evaluate source phone numbers calling T-Mobile subscribers

First Orion gives each source phone number a reputation

If phone number gets a negative reputation, then calls from that phone number are labeled as Spam or Fraud

T-Mobile

TrueCall™ Spoofing Protection and Contact™ Branded Calling



Orchestra One – Inbound Call Authentication and Spoofing Protection

Authentication & Risk Scoring

Dynamically orchestrates the call authentication process using a variety of metadata services to assign a risk score to every call.

Scores from **-5 to +5**

Standard Authentication

Level I - low-cost metadata, industry and proprietary data sources, SIP Analysis

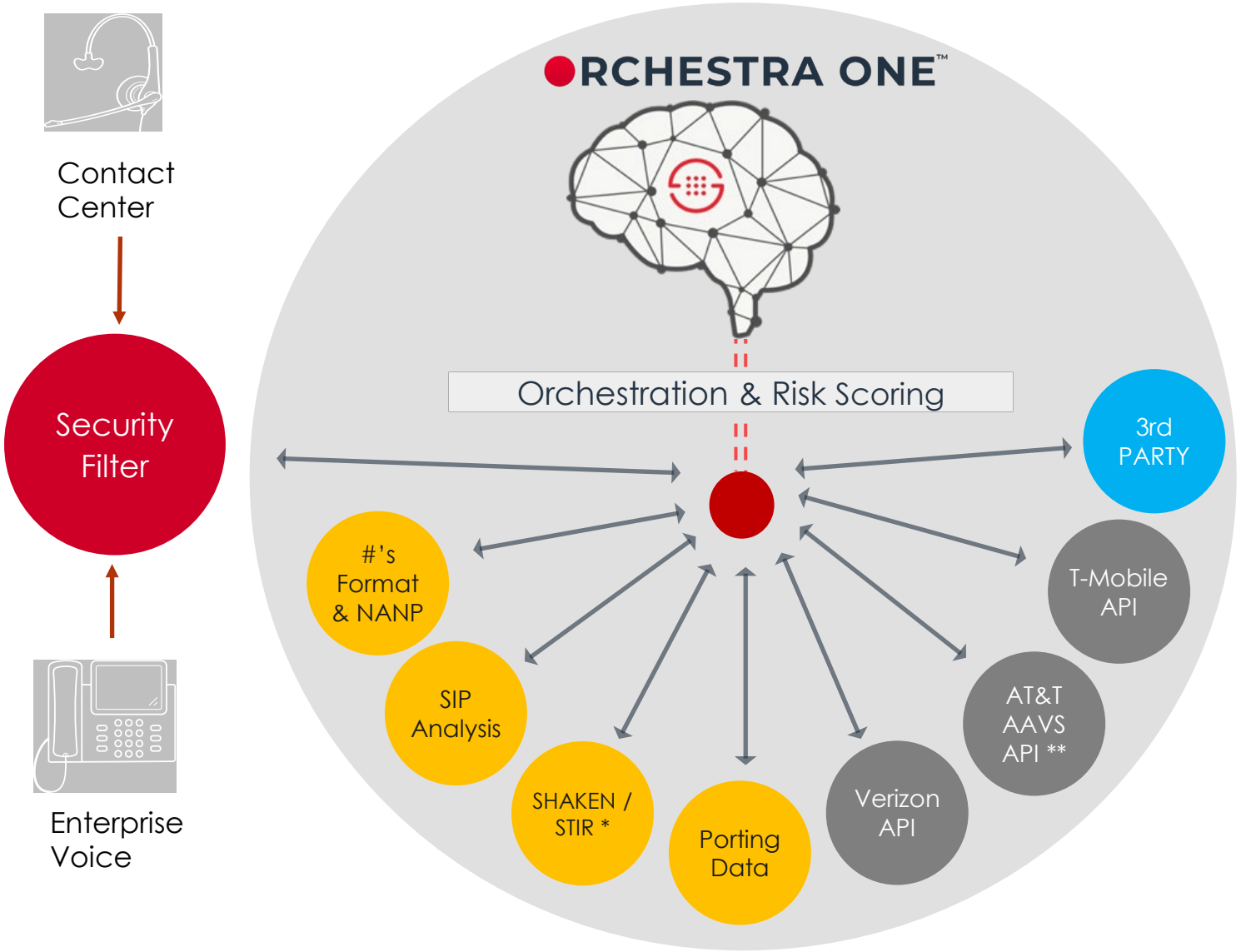
Level II – authentication through STIR/SHAKEN & Porting data

Advanced Authentication

Strong authentication real-time carrier network information with major US carriers.

3rd Party Authentication

Orchestrate the use of 3rd party solutions including media/voice analysis, audio deep fakes, etc.



Open Discussion

Questions / Comments