RSAConference2019
San Francisco | March 4–8 | Moscone Center

SESSION ID: STR-F01

STIR SHAKE'N SIP to Stop Robocalling

Daksha Bhasker

Senior Security Architect
Comcast NBC Universal

We’ve all been to the Islands

…For Free

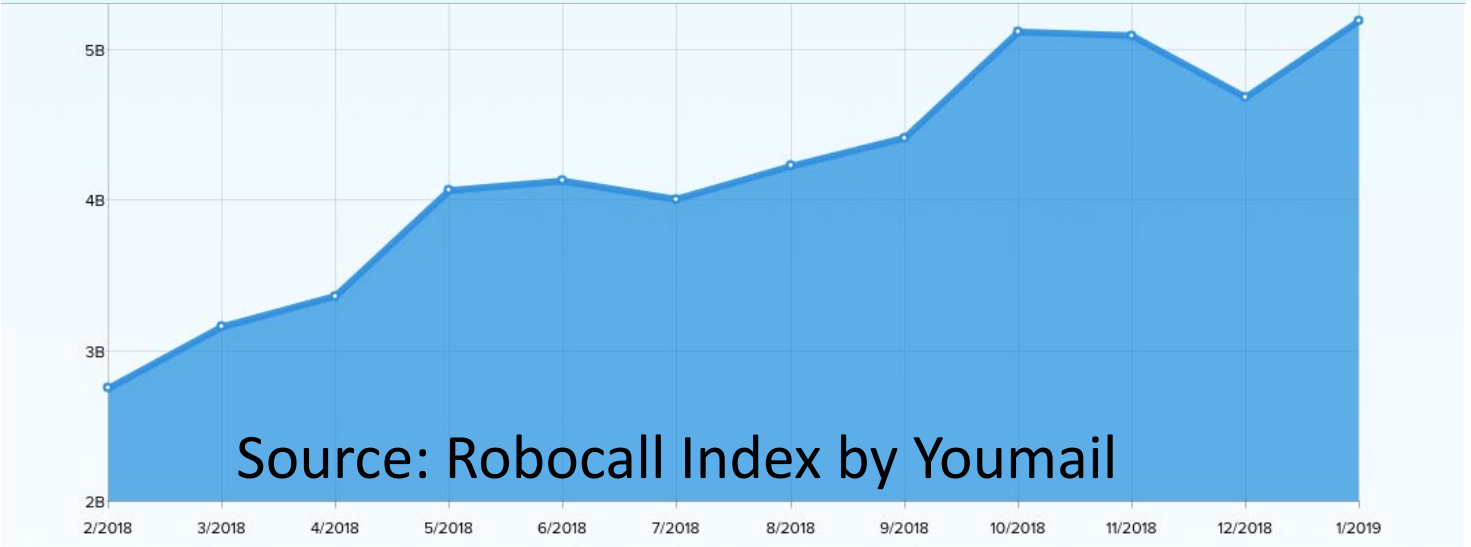
FREE

$9,700

Where Are We At in the US?

January 2019 Nationwide Robocall Data

CALLS PLACED	PER DAY	HOUR	SECOND	Avr. per Person
5.2B	167.3M	7.0M	1.9K	15.8



Robocalls by Category

Americans lost an estimated $9.5B in Phone scams in 2017

- Harris Poll/ Truecaller survey -

COMCAST

Source: https://blog.truecaller.com/2017/04/19/truecaller-us-spam-report-2017/
Youmail: https://robocallindex.com/

Caller ID Spoofing

Robocalling

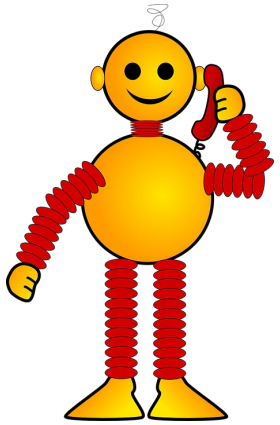
Not All Calls Are Equal

What Makes Spam Easier to Stop?

E-mail Spam

Illegal Robocalls

What's in it for (Illegal) Robocallers?



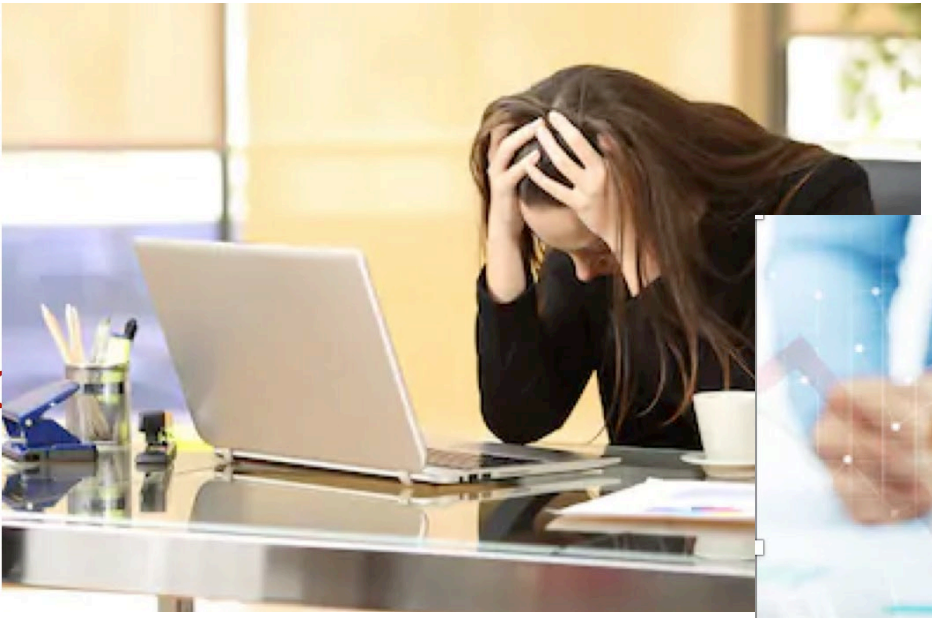
Payments from hire-a-Robocall Service

$$$ scammed from victims

Micropayments per Robocall

Robocallers make money even when calls are not answered.

Impacts Are Felt



Citizens/Consumers

Businesses

SP Networks

Business Case for Addressing the Issues

- Global VoIP market to grow to $190B by 2024
- TDM inching towards EOL
- Robocall and scams are one-third of all calls

RSAConference2019

2. One Cold STIR SHAKEN Framework Please

STIR

Secure
Telephone
Identity
Revisited

SHAKEN

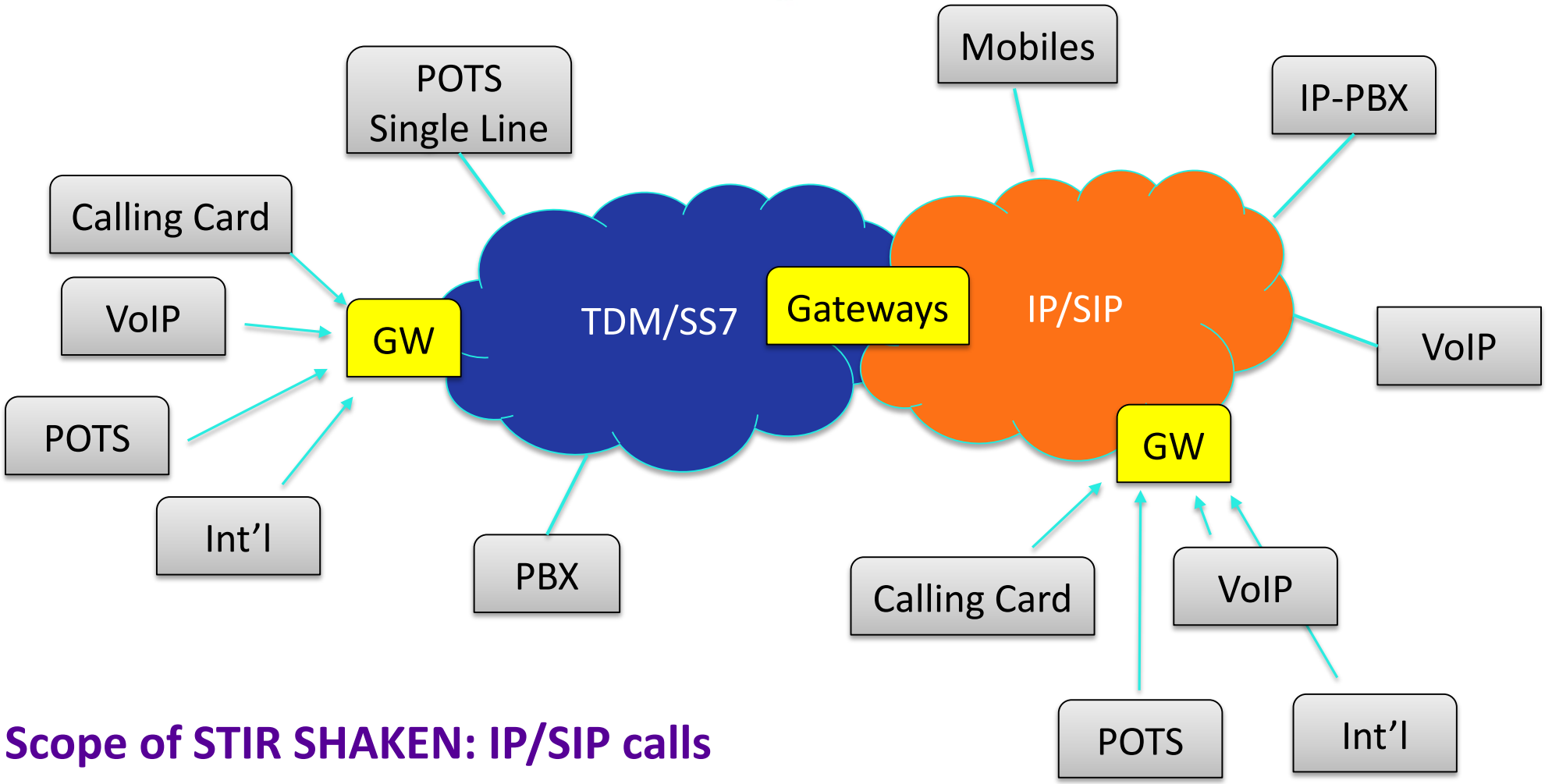
Signature-based
Handling of
Asserted
information using
to**KEN**s

STIR SHAKEN Authenticates Calls that Traverse SIP Networks

Industry

IETF | 3GPP | TSPs | ATIS | SIP Forum | Regulators | Int'l Partners | Others

Phone Technologies



ILEC

Cable ISPs

Wireless Carriers

Hosted/OTT VoIP

IP Backbone Providers

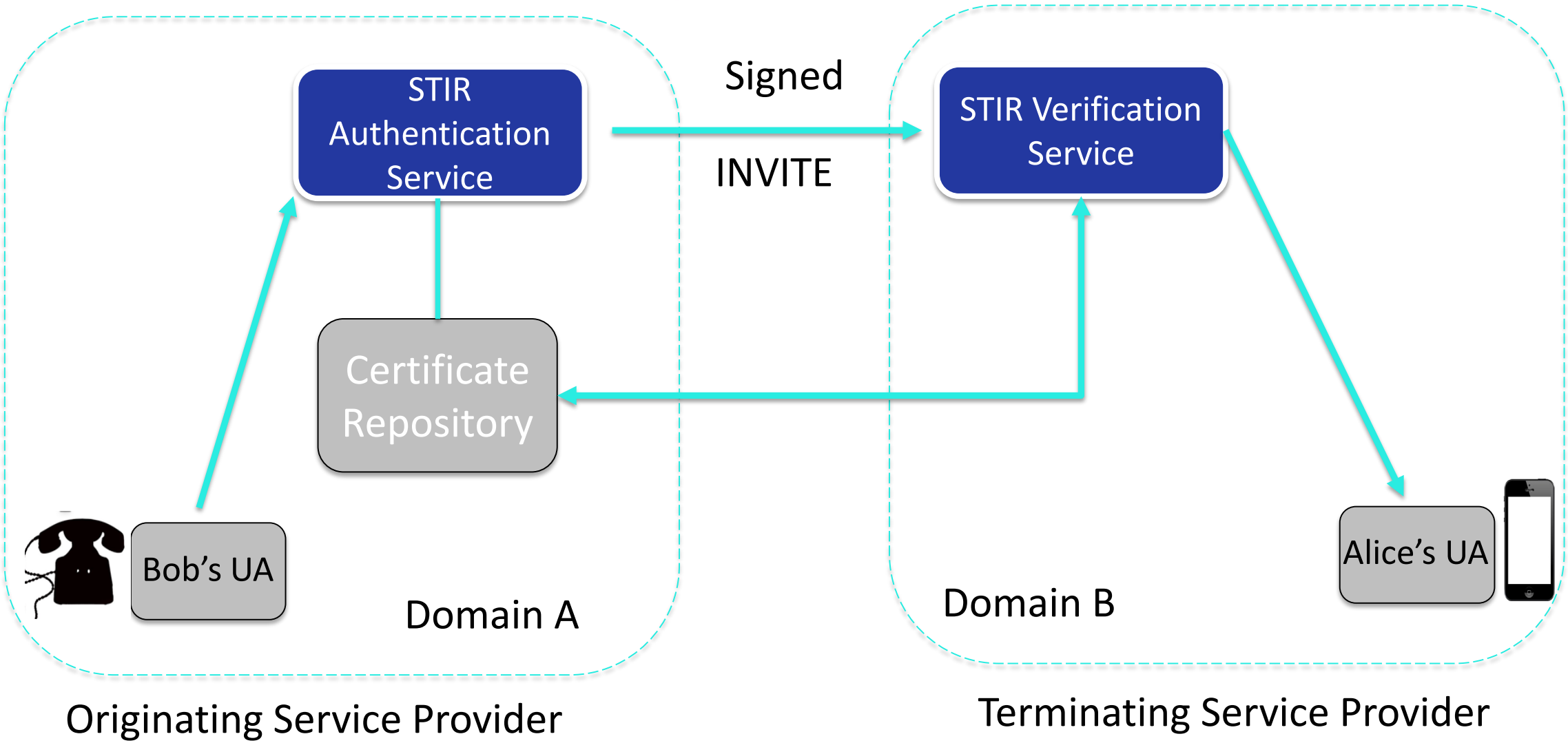
CLEC

Scope of STIR SHAKEN: IP/SIP calls

50% of suspect illegal Robocalls are IP based

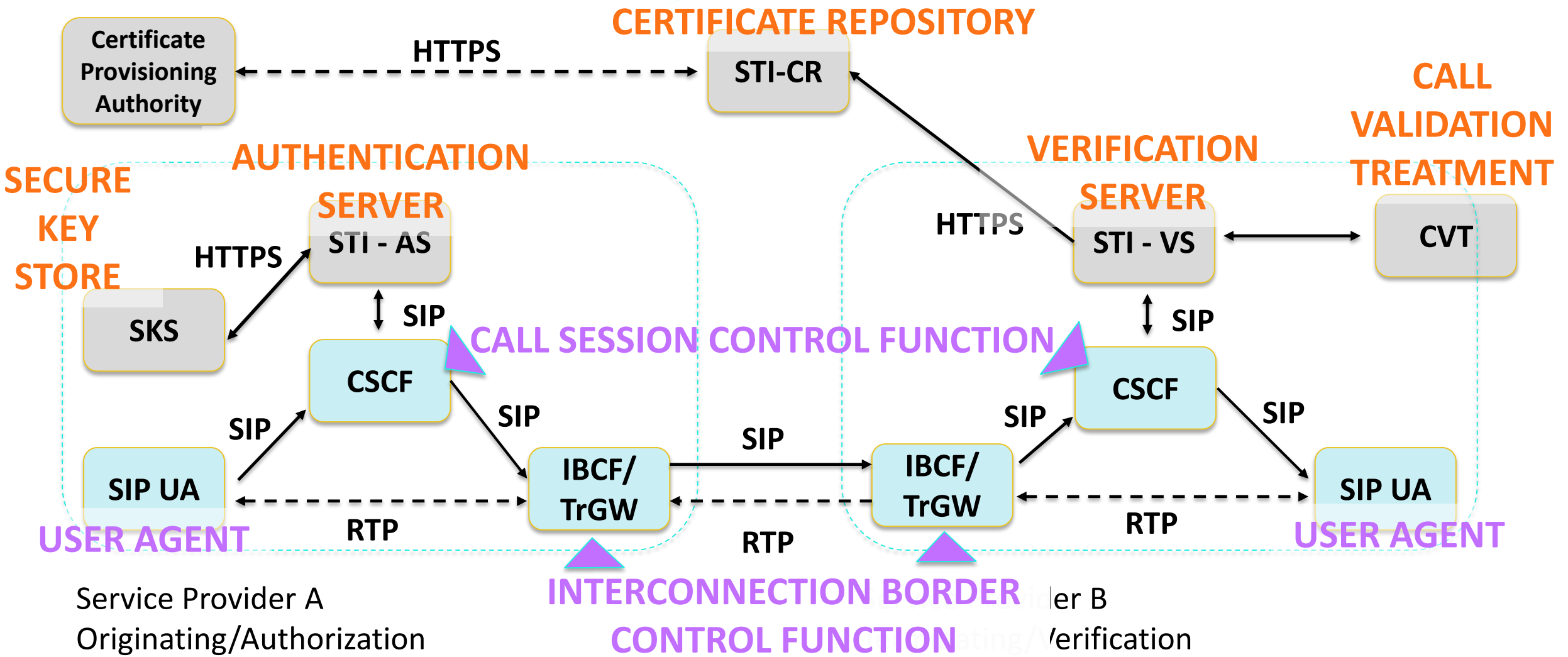
Source: 2018 Robocall Investigation Report – Transaction Network Services

STIR SHAKEN Framework Basic Flow



Source: ATIS, RFC 8224

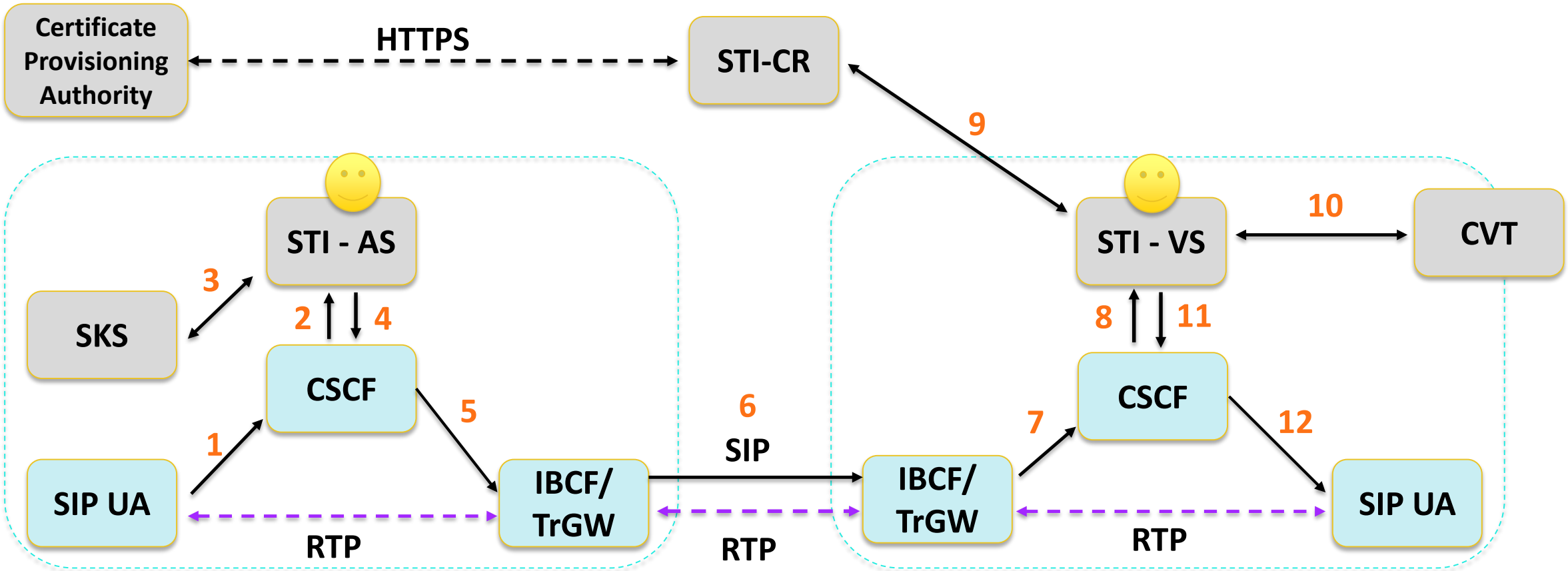
SHAKEN Reference Architecture



Logical view based on 3GPP IMS architecture

Source: ATIS1000074, ATIS0300116

SHAKEN Reference Call Flow



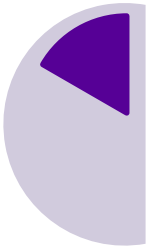
Service Provider A
Originating/Authorization

Service Provider B
Terminating/Verification

Logical view based on 3GPP IMS Architecture

Source: ATIS 1000074, ATIS0300116

Attestation Levels

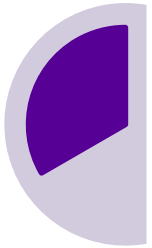


Gateway

Signing Provider

Has no relationship with the initiator of the call
e.g. International Gateway

C

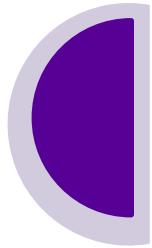


Partial

Signing Provider

Can authenticate the customer and has NOT verified association with the TN being used

B



Full

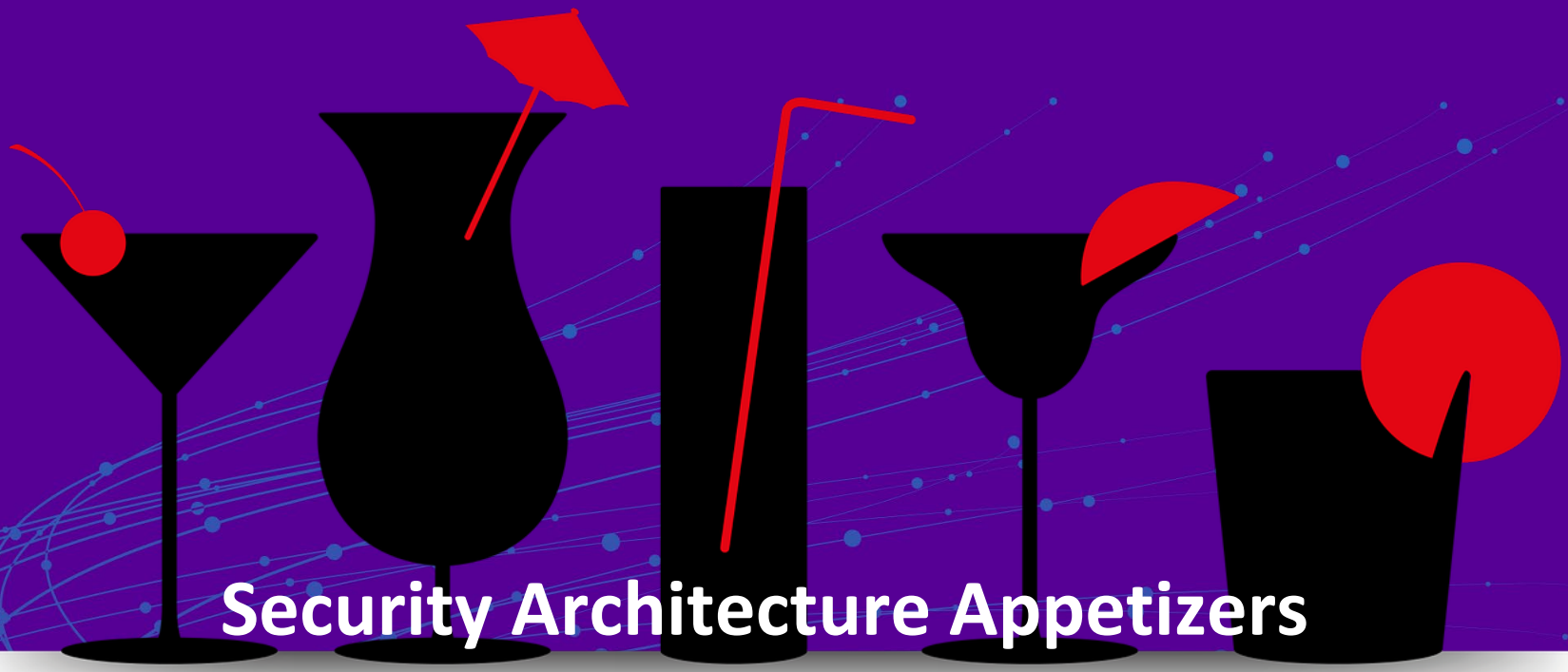
Signing Provider

Has direct authenticated relationship with customer and has verified the TN being used

A

RSAConference2019

3. A STIR & SHAKEN Mixer



Security Architecture Appetizers

Voice Attacks

Vishing

TN Impersonation

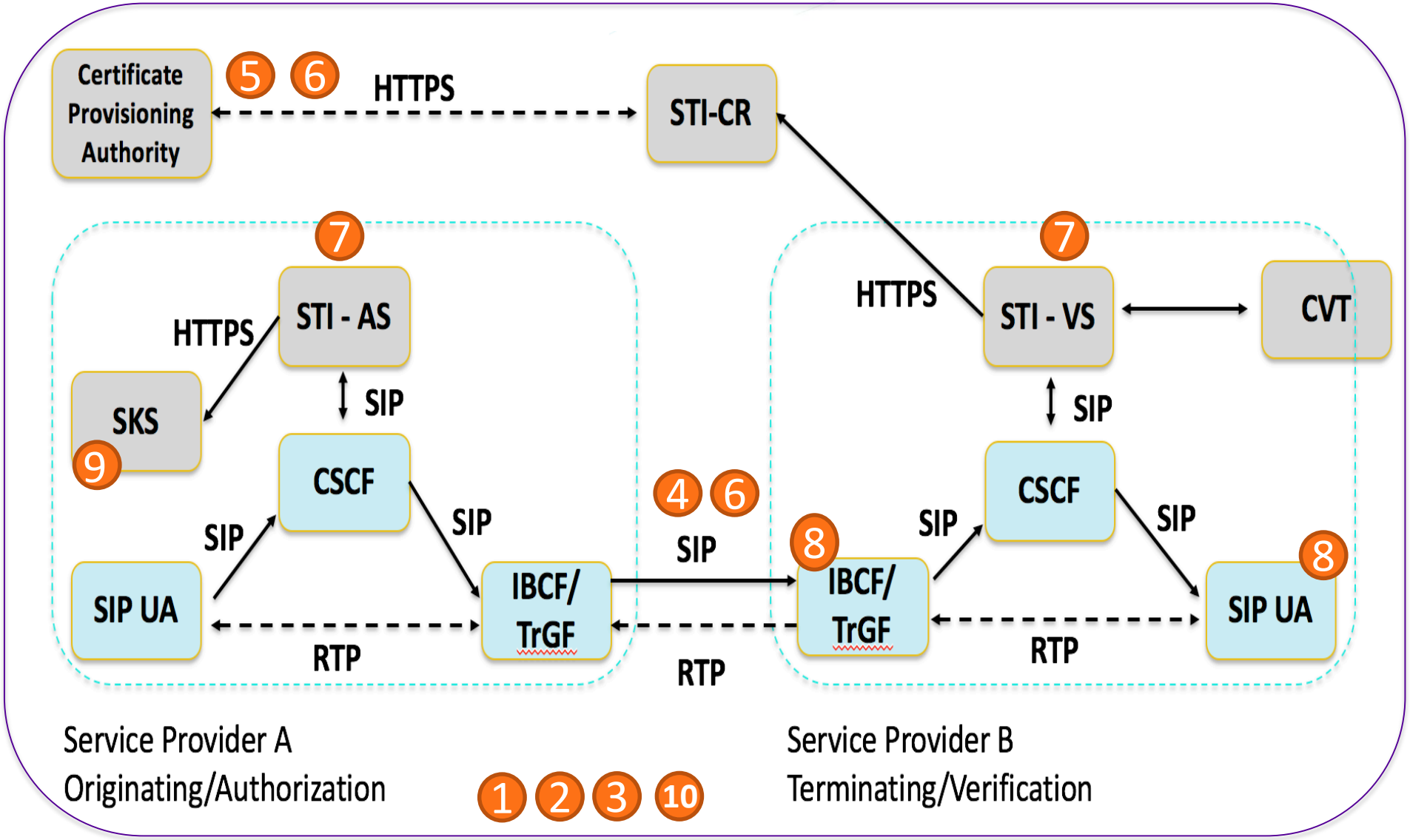
Invalid Unallocated Numbers

Voicemail Hacking

SPIT

Swatting

Security Architecture Considerations



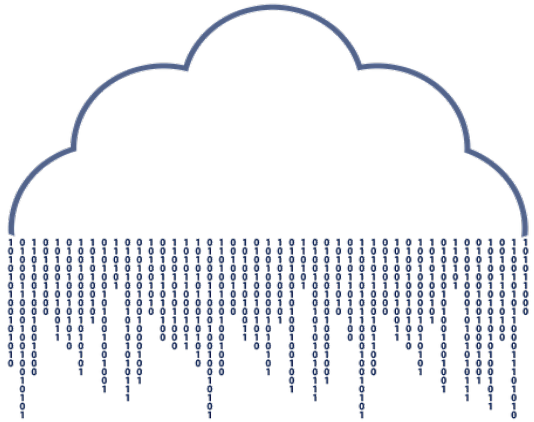
1. Infrastructure
2. Data Sensitivity
3. Security Zone
4. Protocols
5. SHAKEN Cert framework
6. Tokens
7. Caches
8. GWs and UAs
9. Key Management
10. Privacy

Appendix

1 Infrastructure

Is it a bird? plane? or cocktail?

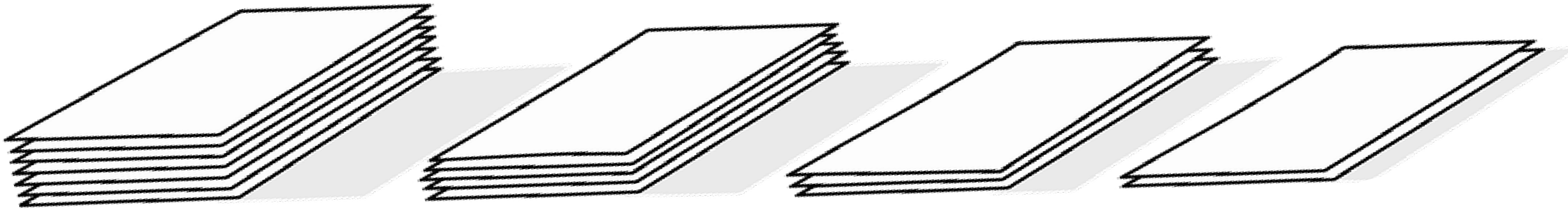
Physical Appliances



Private or Public Cloud Deployments

Availability: Scalability, Resiliency, Redundancy

② Data Sensitivity



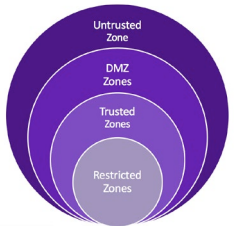
- Private Keys

- Customer Identifiers
- Customer Name
- Customer Address
- IP Address

- Infrastructure Specs
- System Config info

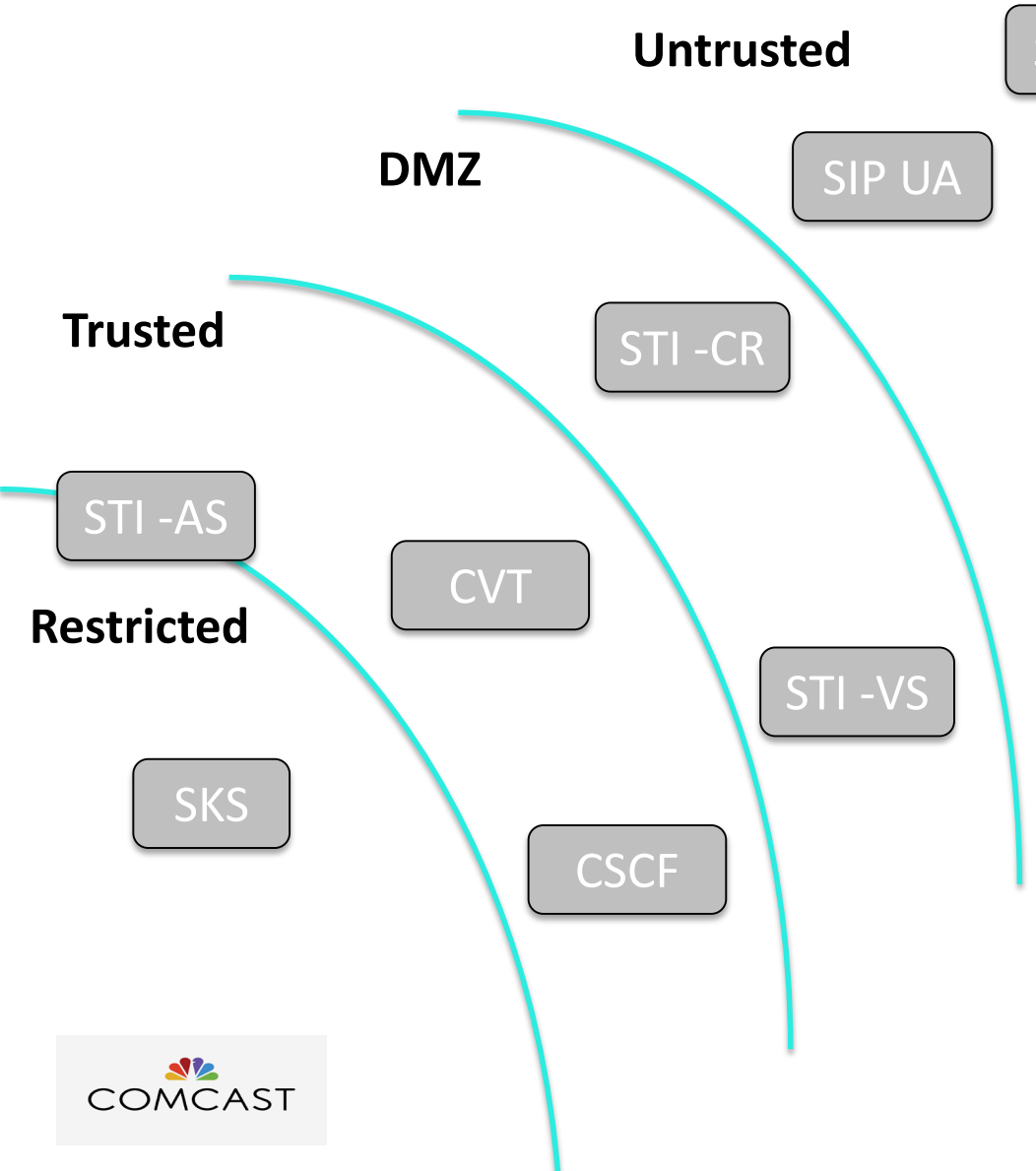
- Public Keys

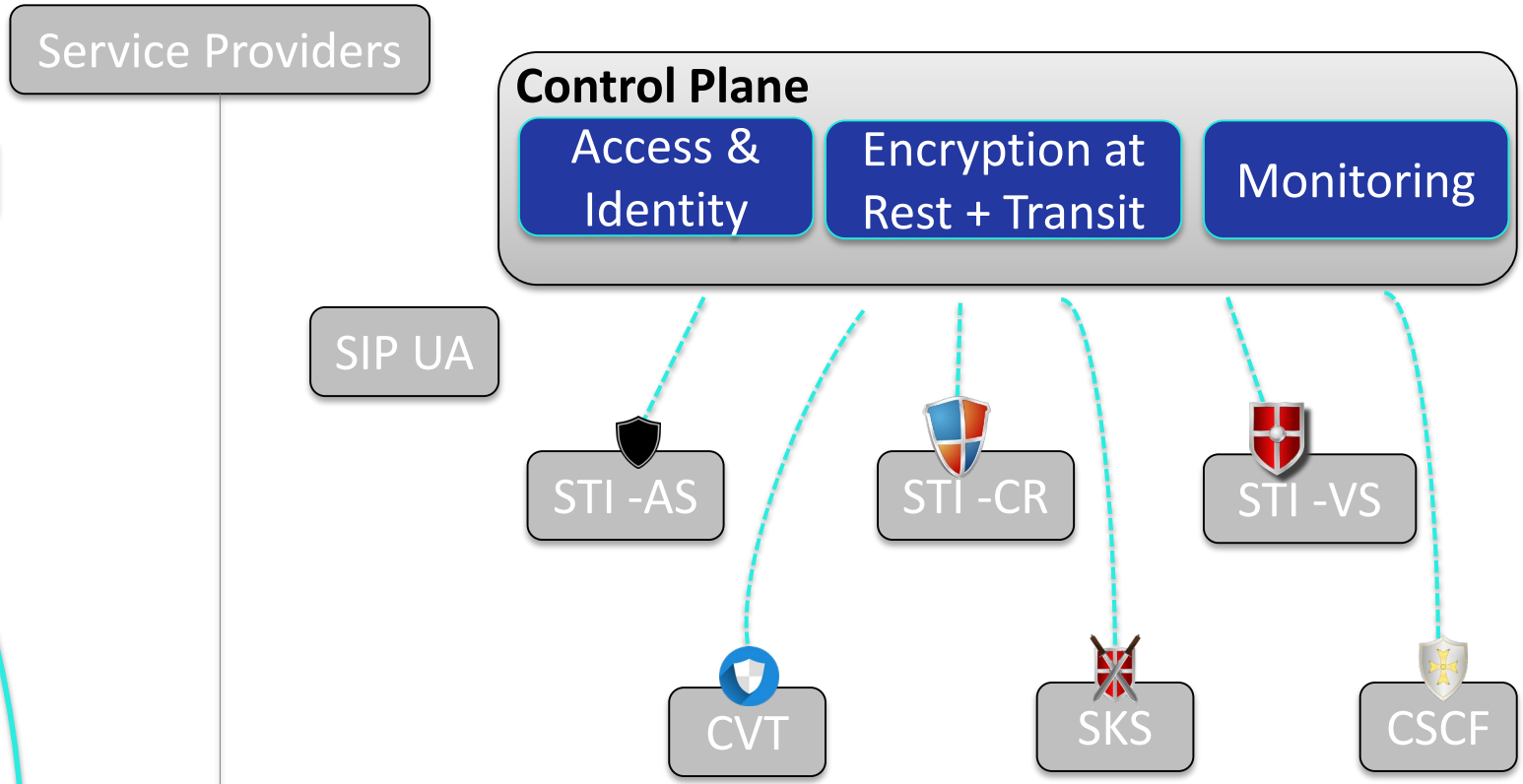
3



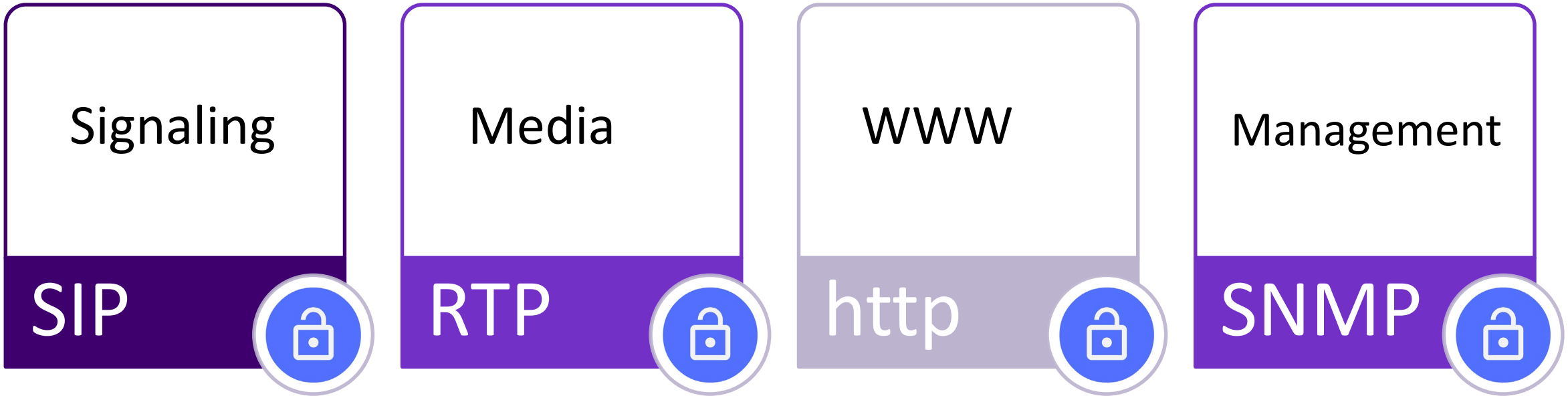
Security Zone

Zero Trust



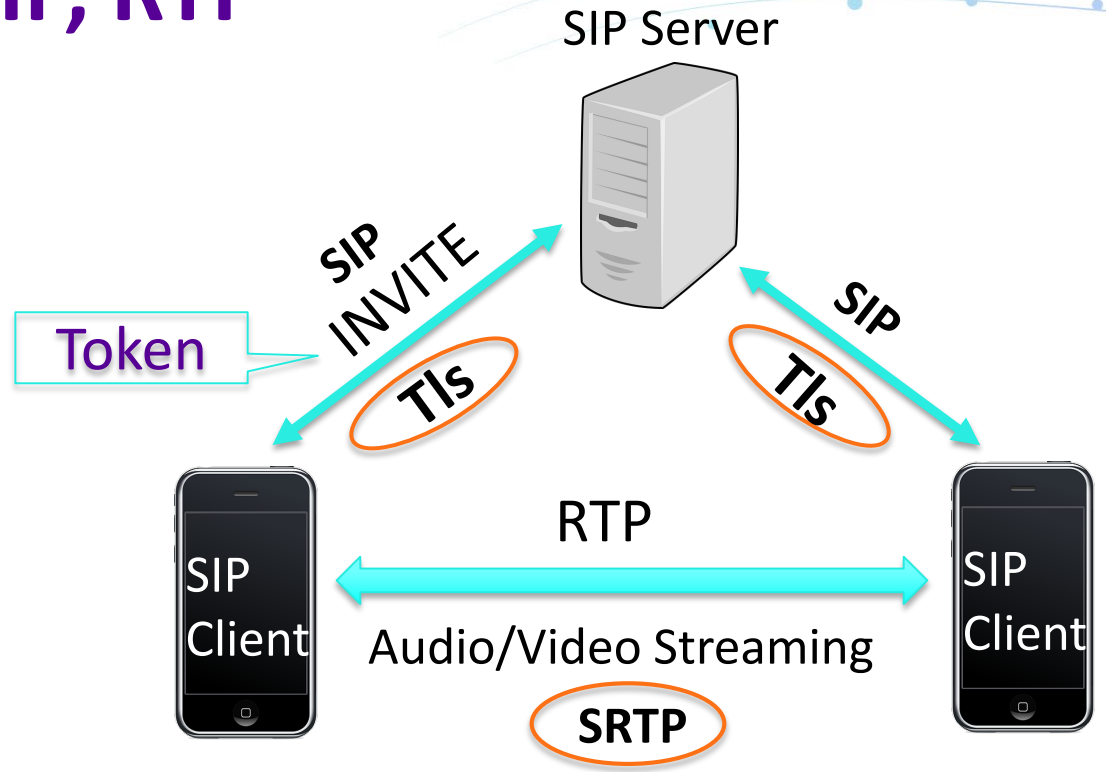


4 Protocols



Over UDP OR TCP?

4 Protocols: SIP, RTP



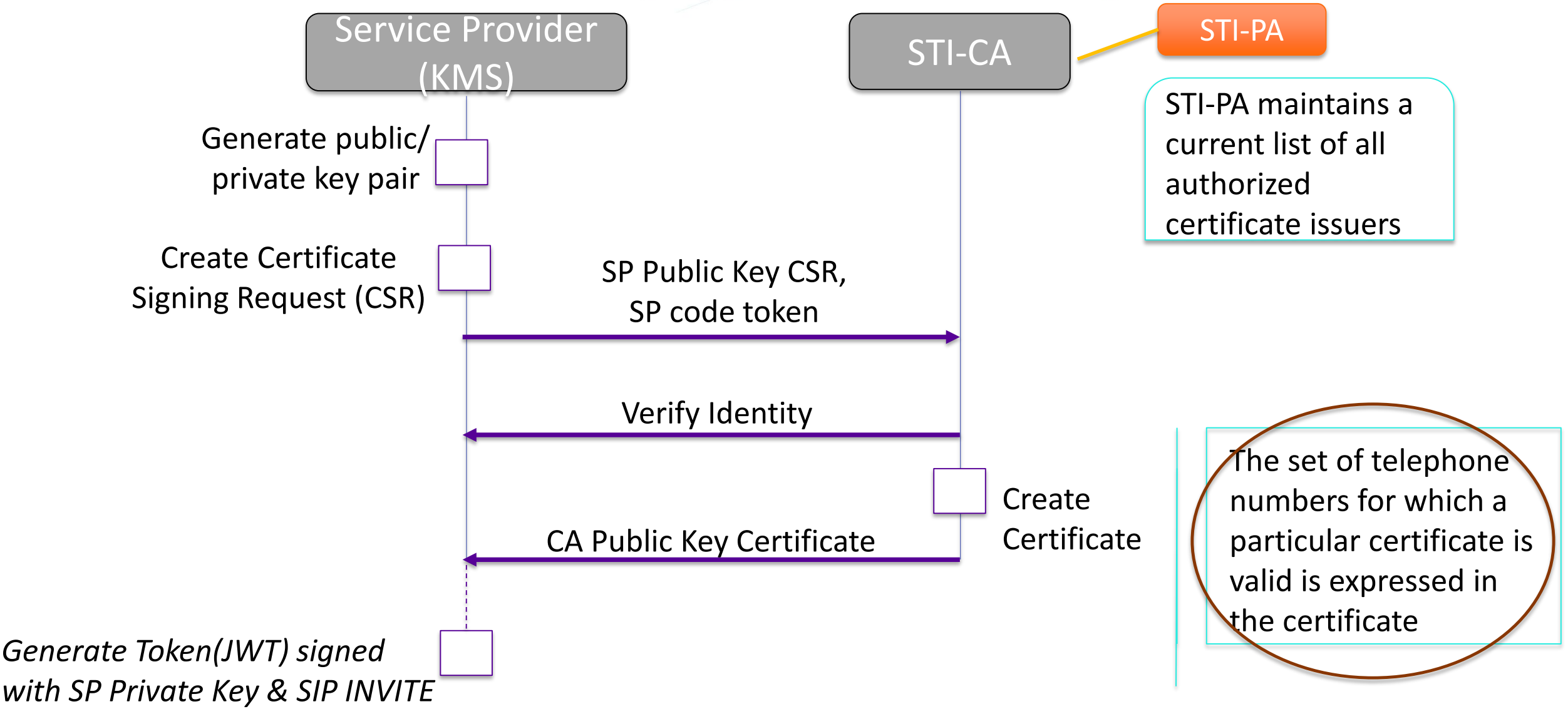
- Unauthorized Eavesdropping
- MiTM
- Call manipulation

- Encrypt the control plane
- Encrypt Real Time media transmission

Refer Reference Architecture to note SIP/RTP flows

Reference: RFC 3261, RFC 3550

5 SHAKEN Certificate Management Architecture (I)



5 Note Worthy Cert Specs for STIR SHAKEN Framework

- Every call is not necessarily uniquely signed
- STIR SHAKEN Certificates are short-lived
- CA charging model is TBD
- Solution may not deal with CRL or OCSP
- Validation that message is signed by Trusted Root CA is crucial

6 Tokens – Security Considerations

Service Provider Code Tokens

Persona Assertion Tokens
PASSporT

JSON Web Tokens
(JWT)

JWT Protected Header

```
{
  "alg" : "ES256",
  "typ": "JWT",
  "x5u": "https://sti-pa.com/sti-pa/cert.crt"
}
```

JWT Payload

```
{
  "sub": ["1234"]
  "iat": 14589234802,
  "nbf": 14782347239
  "exp": 15832948298
  "fingerprint":"SHA256
56:3E:CF:AE:83:CA:4D:15:B0:29:FF:1B:71:D3:BA:B9:19:81:F8:50:9B:DF:4A:D4:39:72:E2:B1:F0:B9
:38:E3"
}
```

JSON Web Token Signature

JWT Protected Header

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

JWT Payload

```
{
  "iat": "1443208345",
  "orig": {"tn":"12155551212"},
  "dest": {"tn":"12155551213"}
}
```

JSON Web Token Signature

6 Tokens – Security Considerations

Base64URL(UTF(JWS Protected Header)).Base64URL(JWS Payload).Base64URL(JWS Signature)

Characteristics

- JWTs maybe created without signature
- Support for encrypted JWTs is Optional

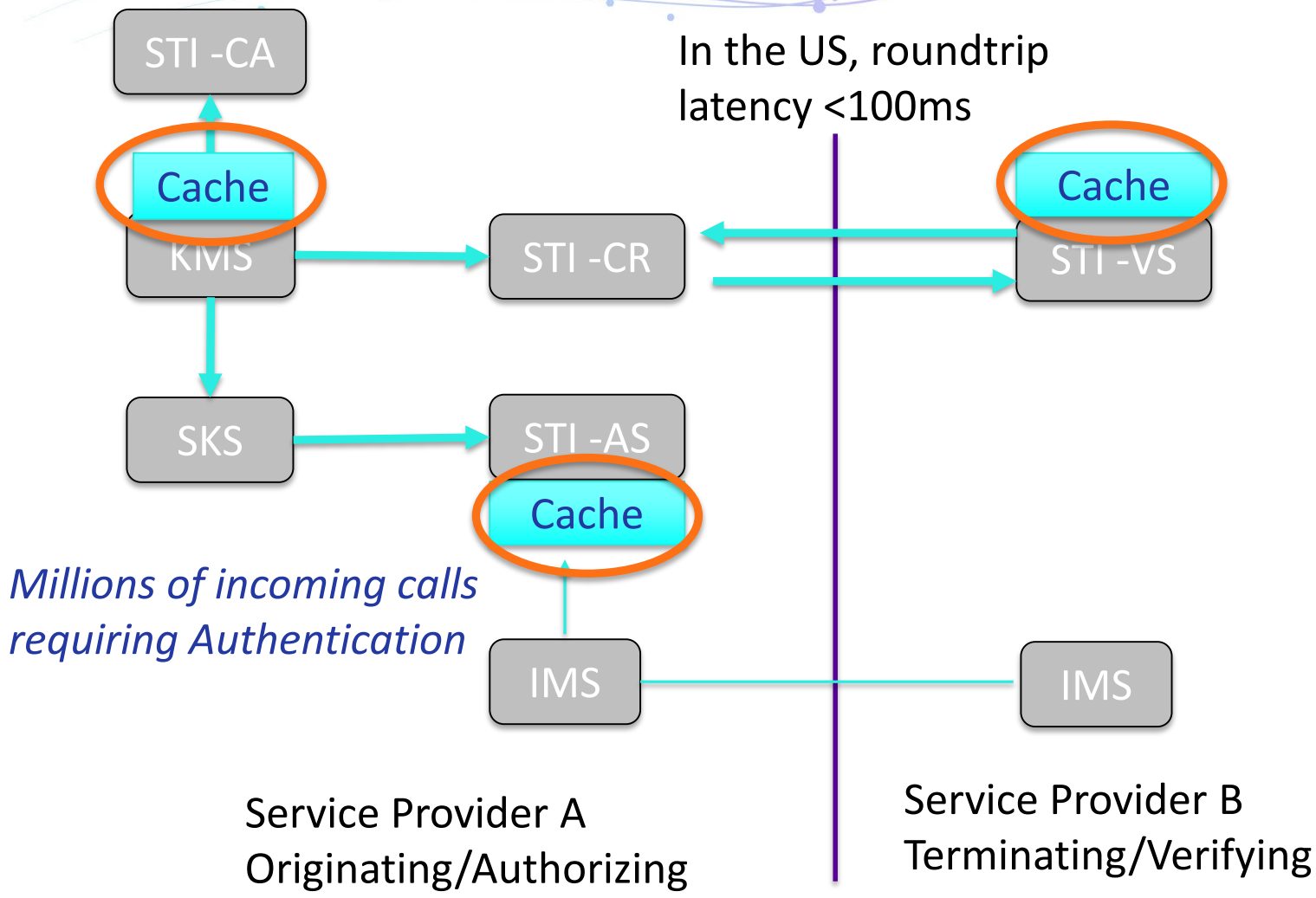
Exploits

- Replay Attacks
- Cut-and-paste Attacks

7 Cache Considerations

What happens when a Verification Service cannot reach the STI-CR?

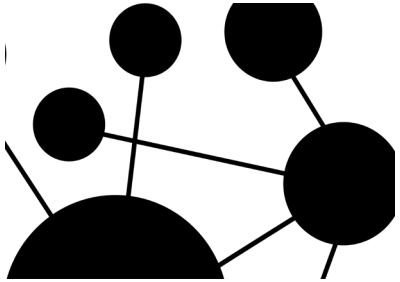
When large volumes of telephone calls need to be signed by the Authentication Service at high speed?



Caching of Public Keys (STI-SP CA), Private Keys (?!)

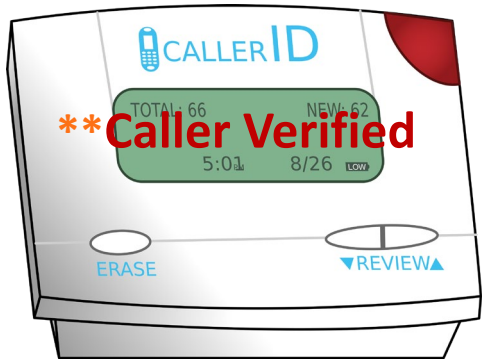
Reference: RFC 7234

8 Intermediaries/Gateways



- End to end retention of SIP headers
- No SIP header rewrites
- Equipment updates for above

9 UE



STIR Identity Support

- **Attestation:** Full, Partial, Gateway
- ‘Verstat’ tel URI parameter support

There is No Silver Bullet. Take a Multilayered Approach.

NATIONAL
DO NOT CALL
REGISTRY

Nomorobo
Hiya
Youmail

STIR SHAKEN
(IP/SIP only)

Voice Experts + Cybersecurity + Every Consumer
+
Industry

APPLY

In the Next 30 Days	
Consumers Enterprises Service Providers Equipment vendors	•Find out what voice technology you use? • What equipment is in place? E.g.: POTS, IP-PBX, TDM or SIP Note: Some VoIP applications use proprietary protocols •What solutions are used to address Robocalling? •Do you use contact centres? •What technologies are used there? •Consider participating in Standards Development: ATIS, SIP Forum, **IP-NNI joint task force**, IETFs, other

APPLY

In the Next 60 Days

Consumers	Leverage Services available to protect yourself from phone scams.
Enterprises	Inquire where your voice experts are with STIR SHAKEN • Will equipment in your environment need updates? • Are your suppliers engaged in STIR SHAKEN?
Service Providers	Inquire where your voice experts are with STIR SHAKEN • What kind of solution is being planned? • Vendor equipment? Inhouse development? Opensource? • What levels of attestation will you provide? • How will you present this to customers?
Equipment vendors	Inquire with your team where they are with STIR SHAKEN? • Do equipment features support STIR-SHAKEN? • Are there upgrades to Infrastructure being planned? • Gateways, SBCs, UEs

APPLY

In the Next 90 Days and BEYOND	
Consumers	• Leverage Services available to protect yourself from phone scams. • Lookout for signs of deployment of STIR SHAKEN • Your service provider *may* require you to opt-in for this feature • Are there new indicators of call attestation on your callerID display?
Enterprises Service Providers	• Partner with the voice experts to review security architectures for STIR SHAKEN
Equipment vendors	• Share your security expertise for secure implementation of STIR SHAKEN

Session Objectives

- Enhance your familiarity with the Robocalling problem and related voice crimes
- Review the STIR SHAKEN Framework
- Security Architecture considerations for STIR SHAKEN

Thank You!

CONTACT:
daksha_bhasker@comcast.com
Senior Cybersecurity Architect
Comcast
(215) 280-5216

Shout Out To Women in Cybersecurity

RSAConference2019

Daksha Bhasker, P.Eng(CIE), MBA, CISM, CISSP, CCSK
Senior Security Architect, Comcast

Daksha has over fifteen years experience in the telecommunications service provider industry with roles in both business management and technology development, accountable for complex solution architectures and security systems development. Her security work spans carrier scale voice, video, data and security solutions. Prior to joining Comcast she worked at Bell Canada developing their cyber threat intelligence platform, and securing cloud deployments. Daksha holds an M.S in computer systems engineering from Irkutsk State Technical University, Russia, and an MBA in electronic commerce from the University of New Brunswick, Canada. She has various publications in international security journals and contributes to security standards development. She is an advocate for women in cybersecurity.

RSAConference2019

APPENDIX

References, Standards, Documents

- ATIS-1000074, Signature-based Handling of Asserted Information using Tokens (SHAKEN)
- ATIS-1000080, Signature-based Handling of Asserted information using toKENs (SHAKEN): Governance Model and Certificate Management
- ATIS-0300251, Codes for Identification of Service Providers for Information Exchange
- ATIS-1000084, Technical Report on Operational and Management Considerations for SHAKEN STI Certification Authorities and Policy Administrators
- ATIS-1000081, Technical Report on a Framework for Display of Verified Caller ID
- RFC7340, Secure Telephone Identity problem statements and Requirements
- RFC8224, Authenticated Identity Management in the Session Initiation Protocol,
- RFC8225, Personal Assertion Token (PASSporT),
- RFC8226, Secure Telephone Identity Credentials: Certificates,
- RFC 3261, SIP: Session Initiation Protocol
- Industry Robocall Strike Force Report
- Martini Recipes

In Canada

- Rules for Robocalling have some differences

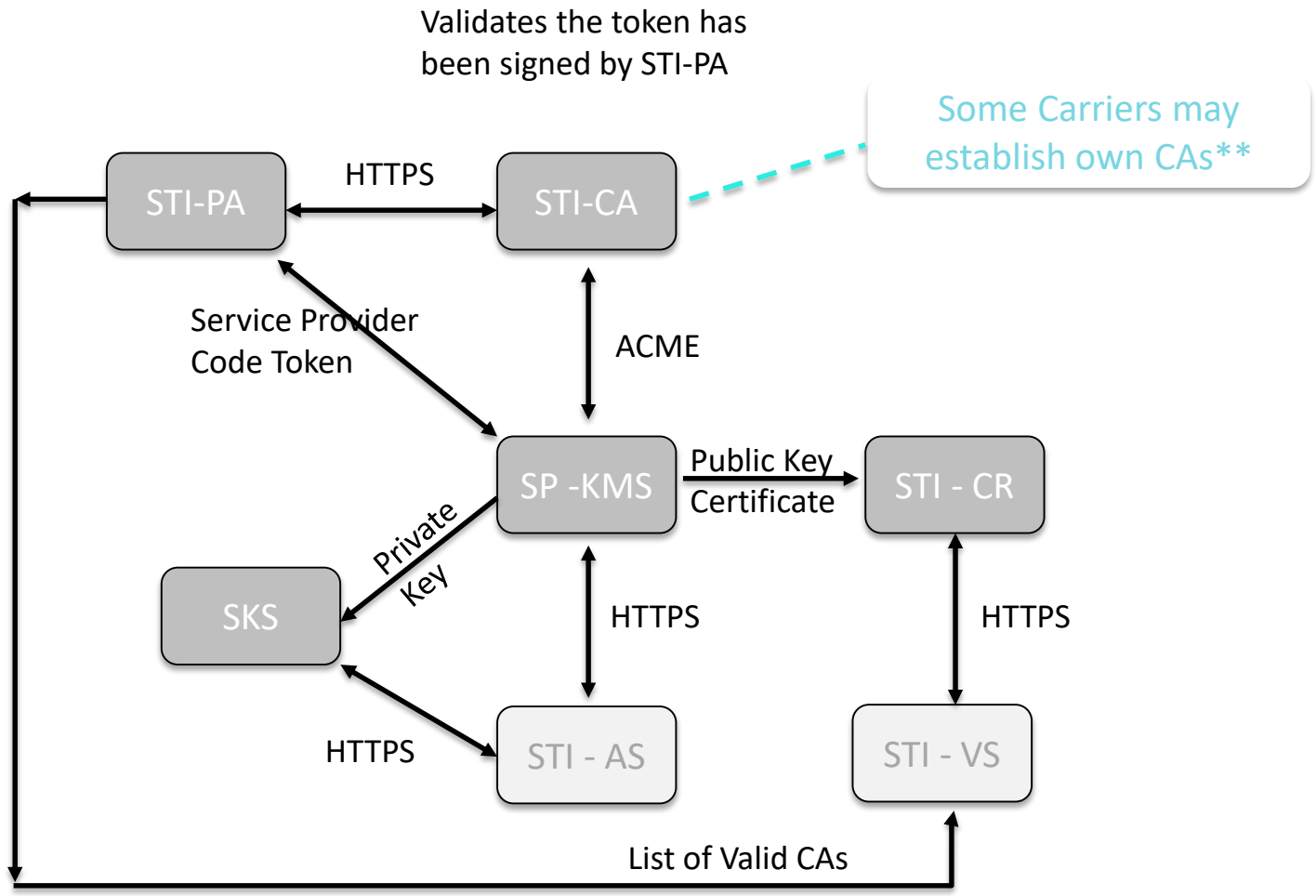
- And Yet…

In 2018 the BBB reported that Canadians lost >$100 million to scams most over the phone

5 SHAKEN Certificate Management Architecture (II)

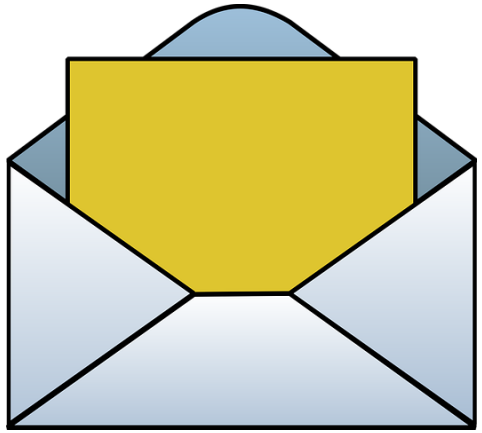
Governance

STI-PA is the trust anchor of the SHAKEN ecosystem



For the Authentication services (STI-AS) to sign calls they must hold a private key corresponding to a certificate with authority over the calling number.

9 Secure Key Store (SKS)



Envelope Encryption

Key Vault

HSM

10 Privacy Considerations

- Telephone Numbers
- CNAM

- Phone Directory
- Yellow Pages

Data Custodians and Data Owners have different responsibilities and privileges

Limitations

Scope of Impact

Originating Network	Terminating Network	Mitigation of Spoofing
PSTN	PSTN	No impact
SIP-Domestic	SIP-Domestic	Significant impact
SIP-Domestic	PSTN	Potential impact
PSTN	SIP-Domestic	No impact
SIP-International	PSTN	No impact
SIP-International	SIP-Domestic	Little impact

- SIP only scope
- International calls will have low attestation
- Testing is underway
- Differences in US/Canadian CNAM operations may cause interop issues.

Solutions itself continues to be developed and evolved

Shout Out To Women in Cybersecurity

HAPPY INTERNATIONAL WOMEN's DAY!

BERTHE MORISOT

WOMAN IMPRESSIONIST

"I don't think there has ever been a man who treated a woman as an equal, and that's all I would have asked for—I know I am worth as much as they are."

—Berthe Morisot, 1890

A stunning exhibit at the Barnes Foundation in Philadelphia