STIR/SHAKEN: A Looming Privacy Disaster

Josh Brown & Paul Grubbs
University of Michigan

Presented by Josh Brown

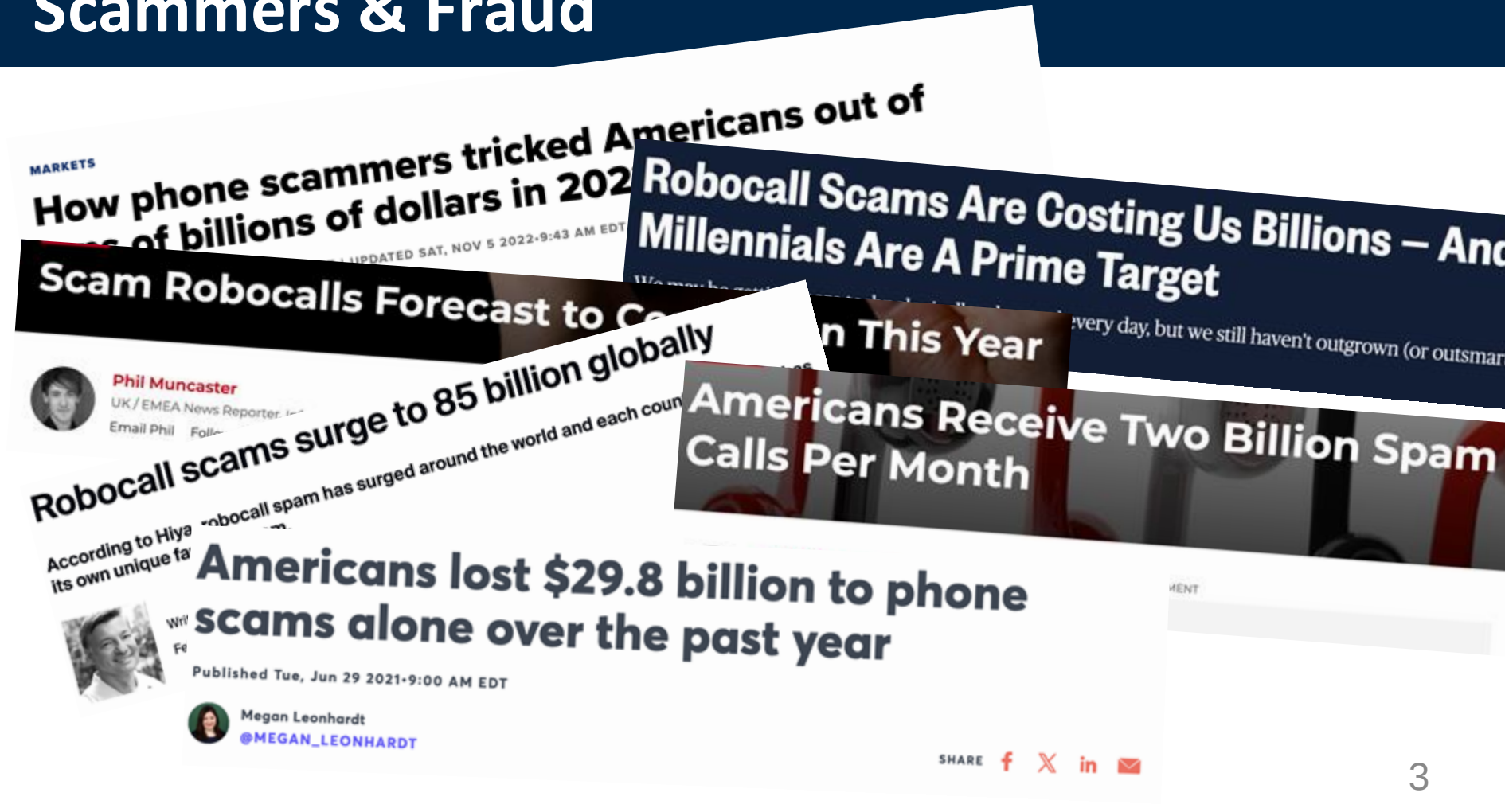
Robocalls & Fraud

We've been trying to reach you about your car's extended warranty!

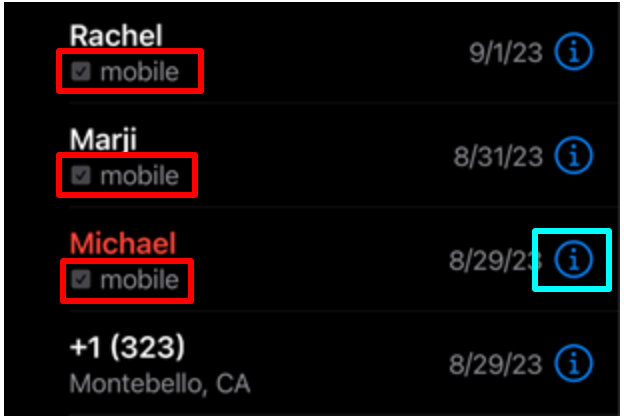
You've won a free cruise to the Bahamas!

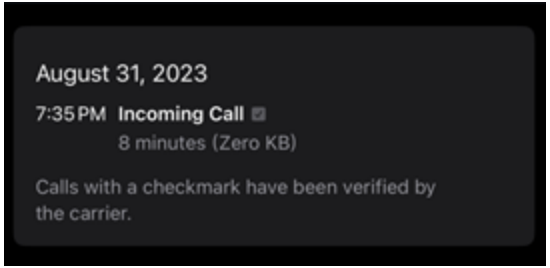
This is Microsoft Technical support.

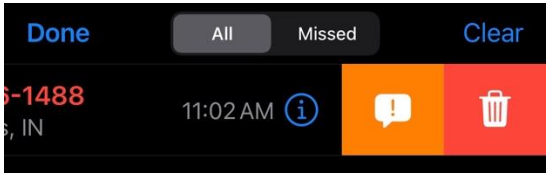
Scammers & Fraud

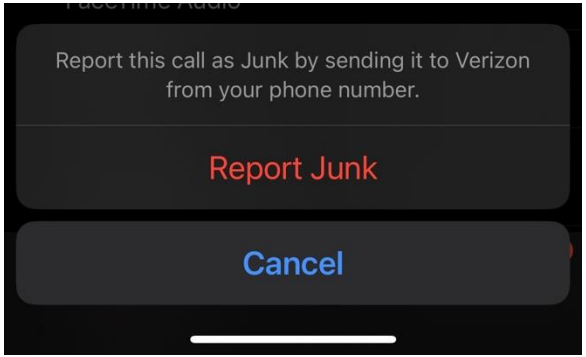


Familiar Screens









STIR/SHAKEN

Public Law 116–105
116th Congress

An Act

Dec. 30, 2019
[S. 151]

To deter criminal robocall violations and improve enforcement of section 227(b) of the Communications Act of 1934, and for other purposes.

Be it enacted by the Senate and House of Representatives of the United States of America in Congress assembled,

Pallone-Thune Telephone Robocall Abuse Criminal Enforcement and Deterrence Act
47 USC 609 note.

SECTION 1. SHORT TITLE.

This Act may be cited as the "Pallone-Thune Telephone Robocall Abuse Criminal Enforcement and Deterrence Act" or the "Pallone-Thune TRACED Act".

Trump signs the TRACED Act, the first federal anti-robocall law

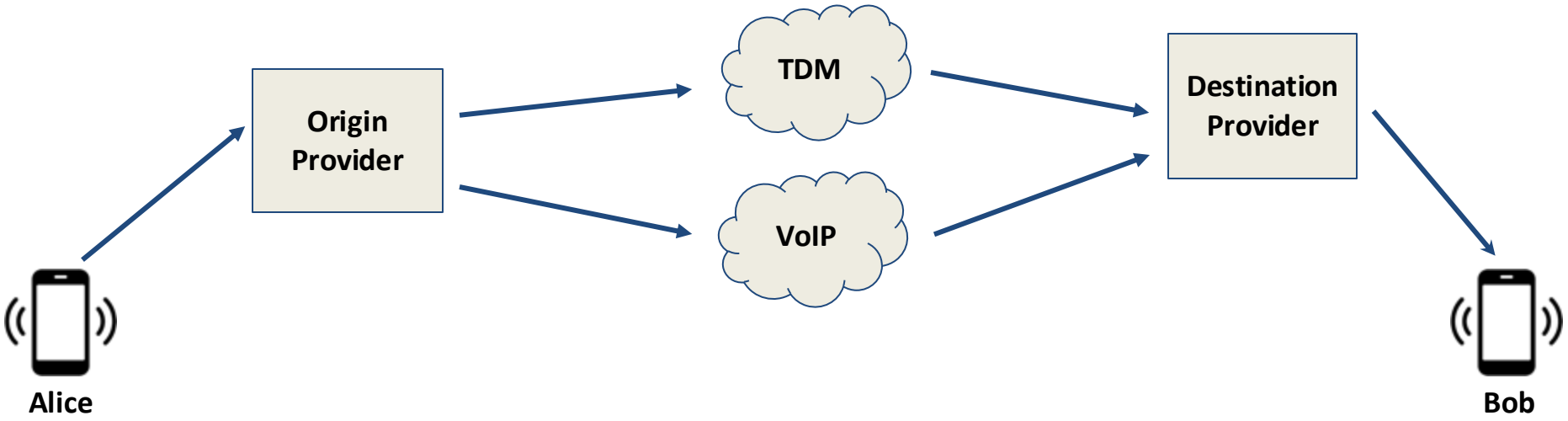
The law implements new consumer protections, gives more teeth to law enforcement efforts and takes other steps to combat unwanted robocalls.

Results Overview

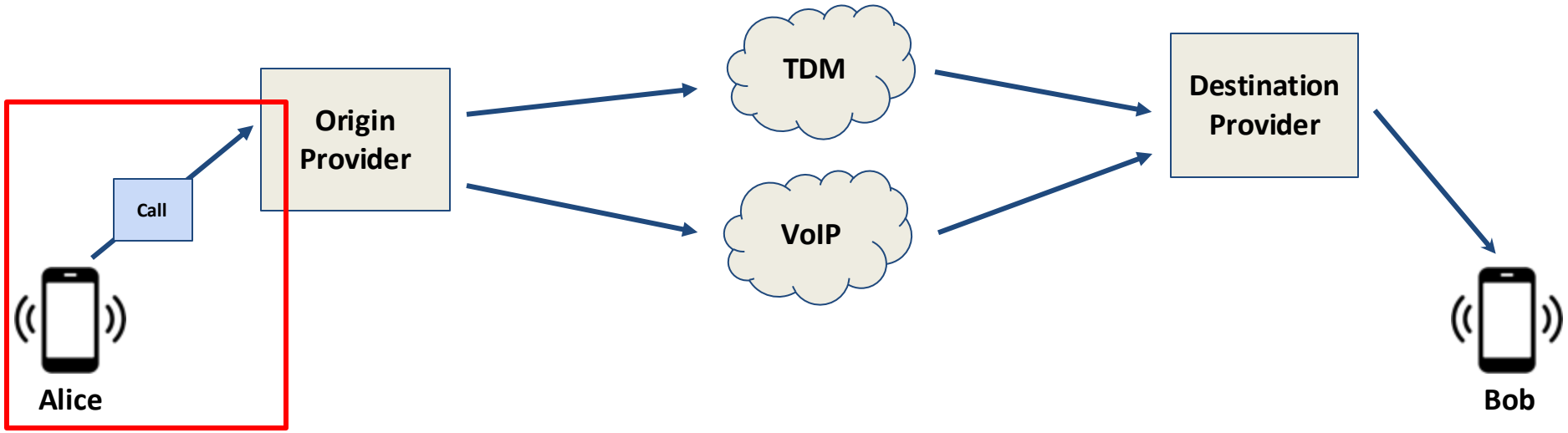
- Flaws
  - Non-repudiable metadata
  - New metadata leakage
  - Numerous PKI issues
- Survey (n=29)
  - Conducted using FCC's Robocall Mitigation Database
- Solutions
  - Blind signing (and verifying)
  - Deniable signatures
  - Improved protocol for non-internet calls

Background

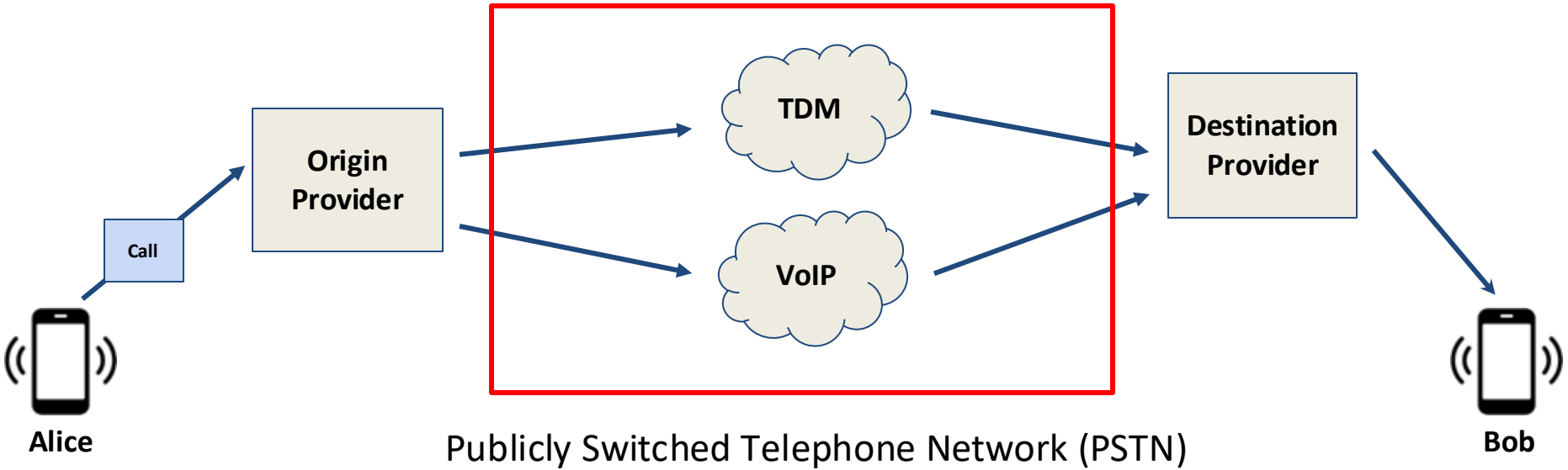
Telecom Ecosystem: How to make a phone call?



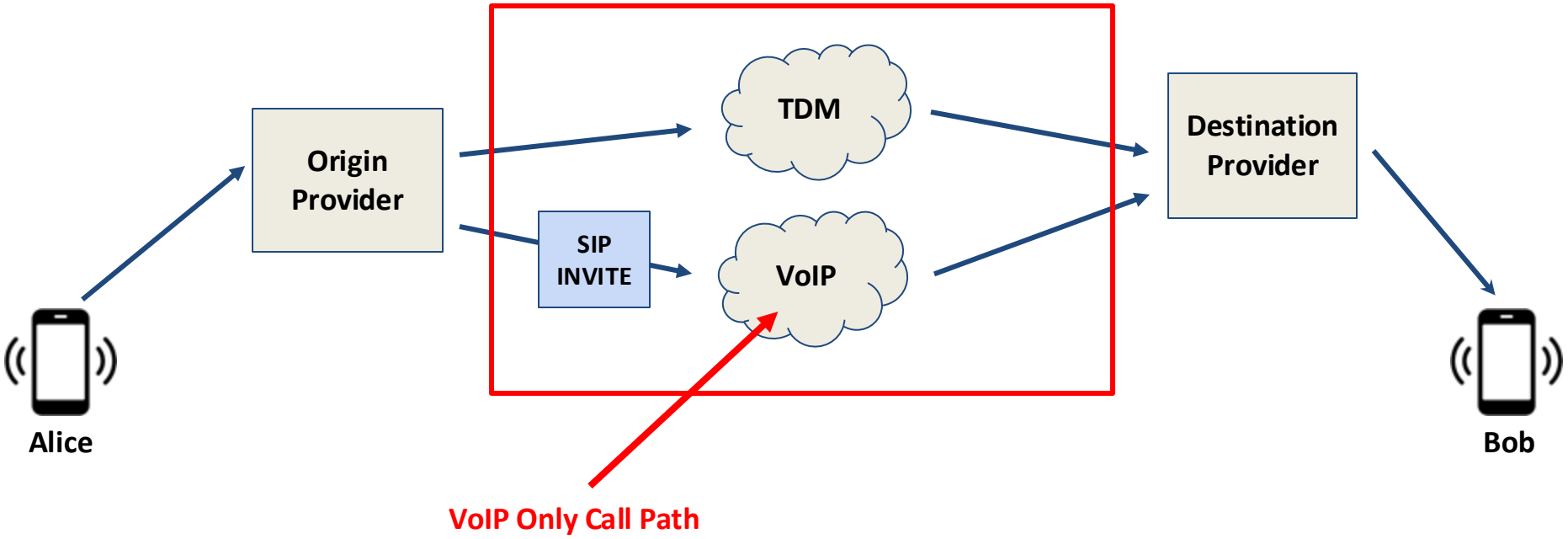
Telecom Ecosystem: How to make a phone call?



Telecom Ecosystem: How to make a phone call?



Telecom Ecosystem: How to make a phone call?



Traditional SIP INVITE Example

```
INVITE sip:+14155552222@example.att.com SIP/2.0
Via: SIP/2.0/UDP 1.2.3.4:5060;branch=z9hG4bK776asdhds
Max-Forwards: 70
To: "Bob" <sip:+14155552222@example.att.com>
From: "Alice" <sip:+14155551111@example.pstn.verizon.com>;tag=1
Call-ID: a84b4c76e66710
CSeq: 1 INVITE
Contact: "Alice" <sip:+14155551111@1.2.3.4:5060>
Content-Length:
```

Traditional SIP INVITE Example

```
INVITE sip:+14155552222@example.att.com SIP/2.0
Via: SIP/2.0/UDP 1.2.3.4:5060;branch=z9hG4bK776asdhds
Max-Forwards: 70
To: "Bob" <sip:+14155552222@example.att.com>
From: "Alice" <sip:+14155551111@example.pstn.verizon.com>;tag=1
Call-ID: a84b4c76e66710
CSeq: 1 INVITE
Contact: "Alice" <sip:+14155551111@1.2.3.4:5060>
Content-Length:
```

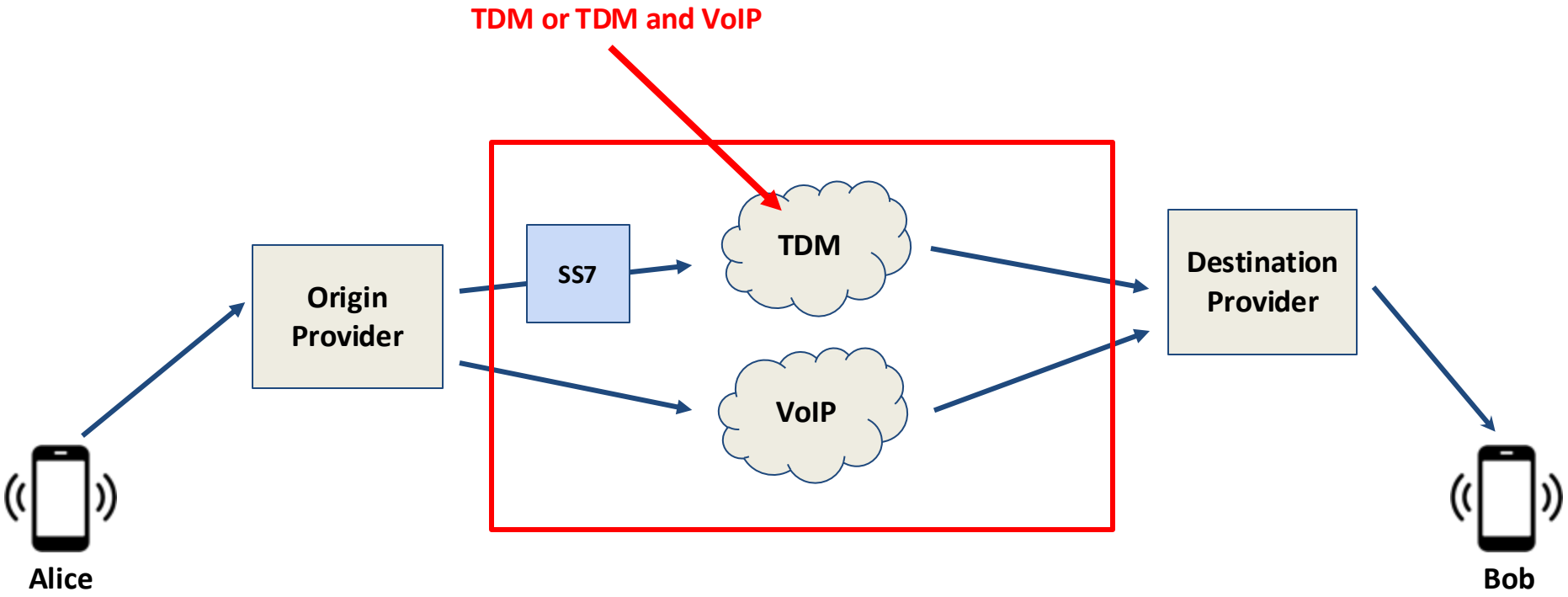
Traditional SIP INVITE Example

```
INVITE sip:+14155552222@example.att.com SIP/2.0
Via: SIP/2.0/UDP 1.2.3.4:5060;branch=z9hG4bK776asdhds
Max-Forwards: 70
To: "Bob" <sip:+14155552222@example.att.com>
From: "Alice" <sip:+14155551111@example.pstn.verizon.com>;tag=1
Call-ID: a84b4c76e66710
CSeq: 1 INVITE
Contact: "Alice" <sip:+14155551111@1.2.3.4:5060>
Content-Length:
```

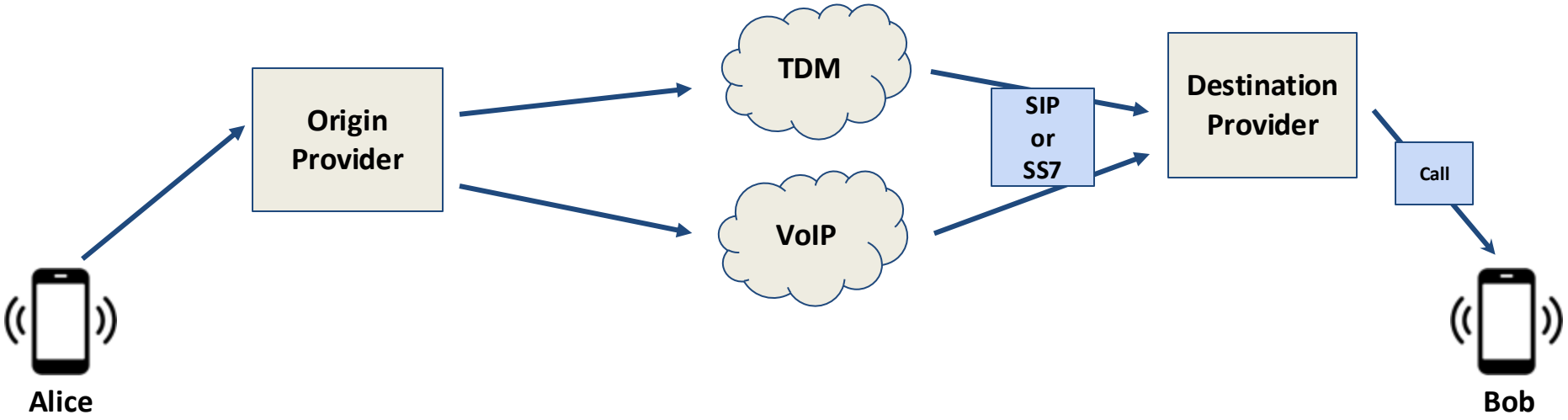
Trivial to spoof.

Leads to spam calls

Telecom Ecosystem: How to make a phone call?



Telecom Ecosystem: How to make a phone call?

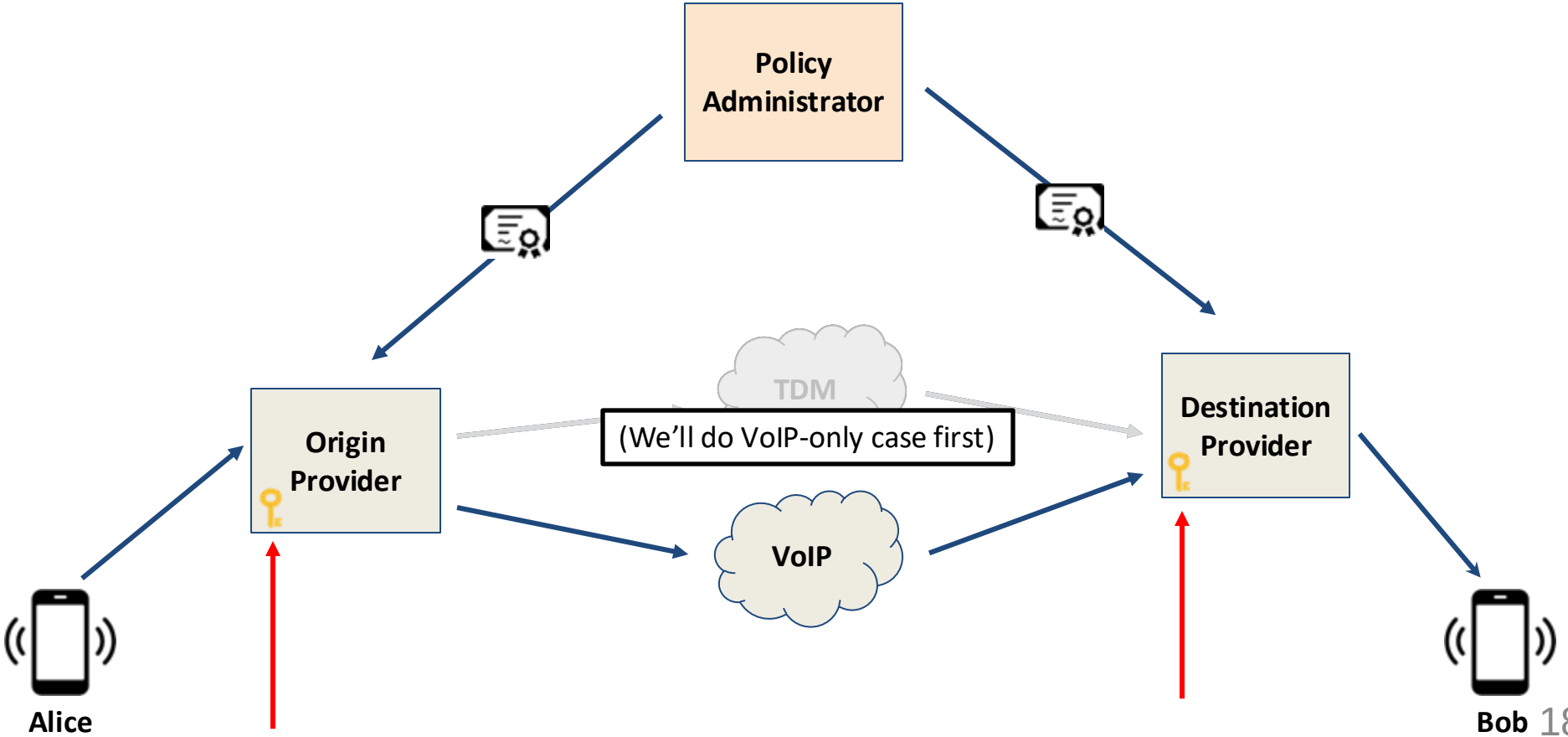


STIR/SHAKEN

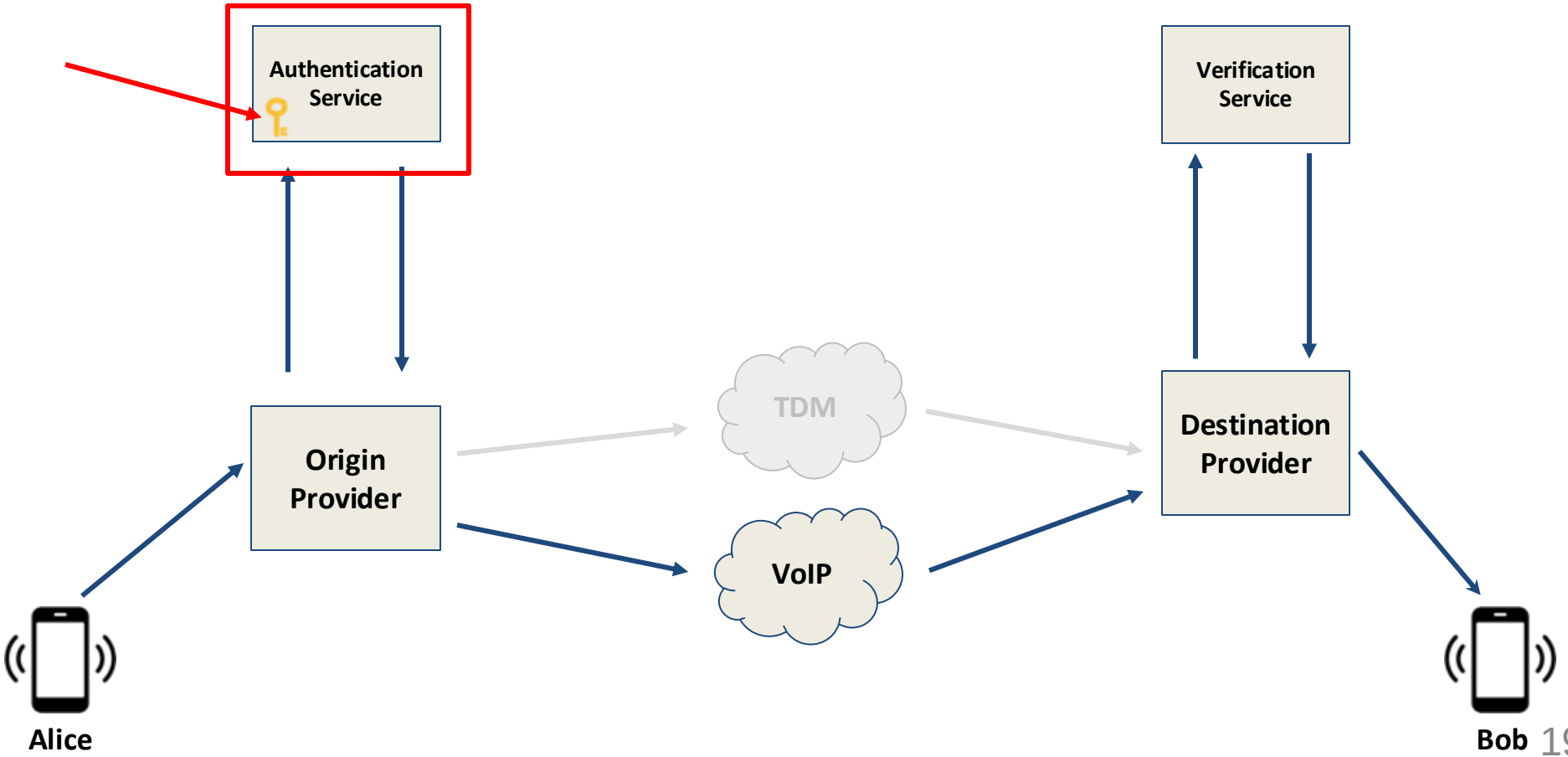
- Telecoms sign call metadata = “attestation” about caller
- Creates a new PKI for providers
- **NOT** identity system for callers
- Reporting mechanisms help punish negligent telecoms
- ~900 telcos participating, 37% of all calls signed (Feb. ‘24)

Source: https://transnexus.com/blog/2024/shaken-statistics-february/

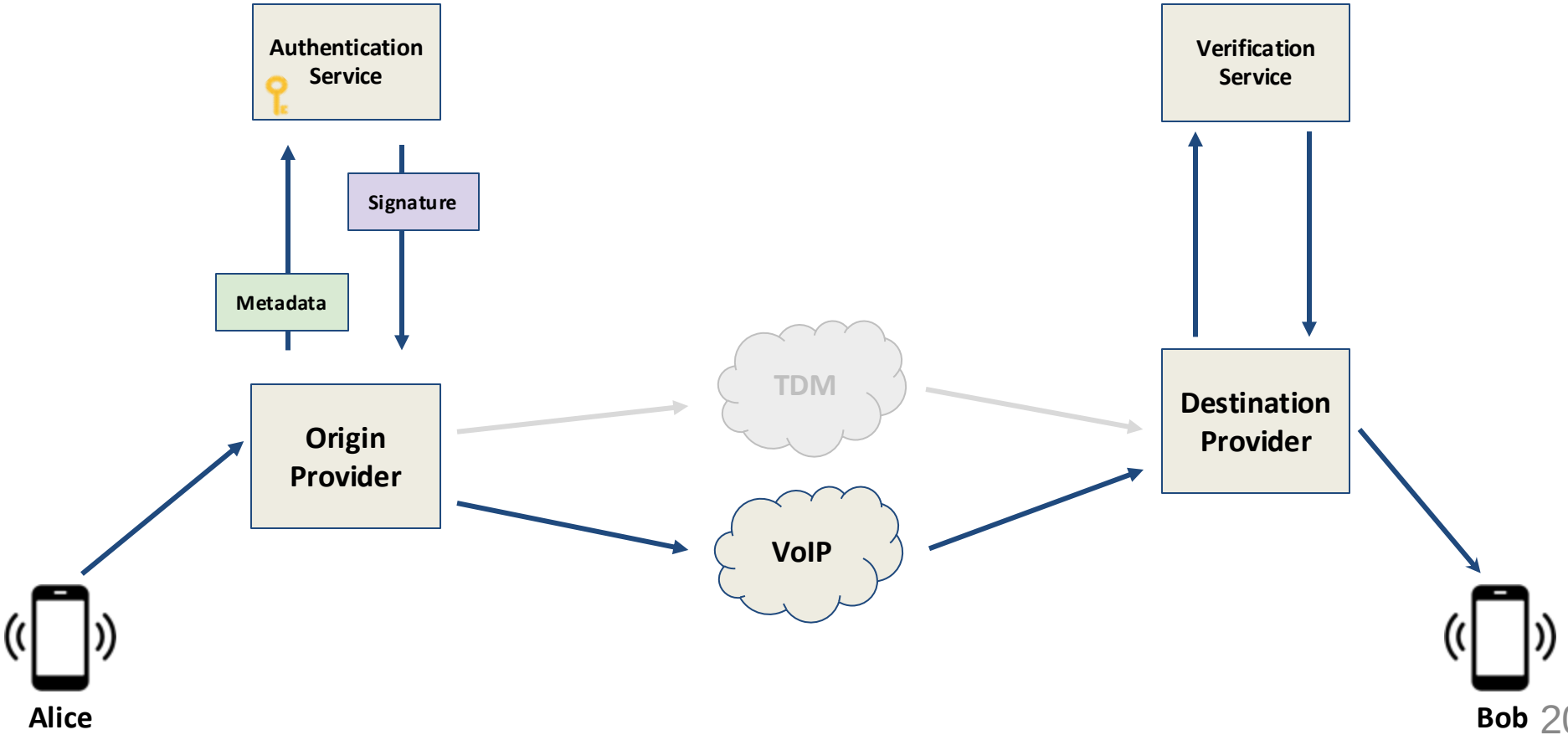
STIR/SHAKEN: Architecture



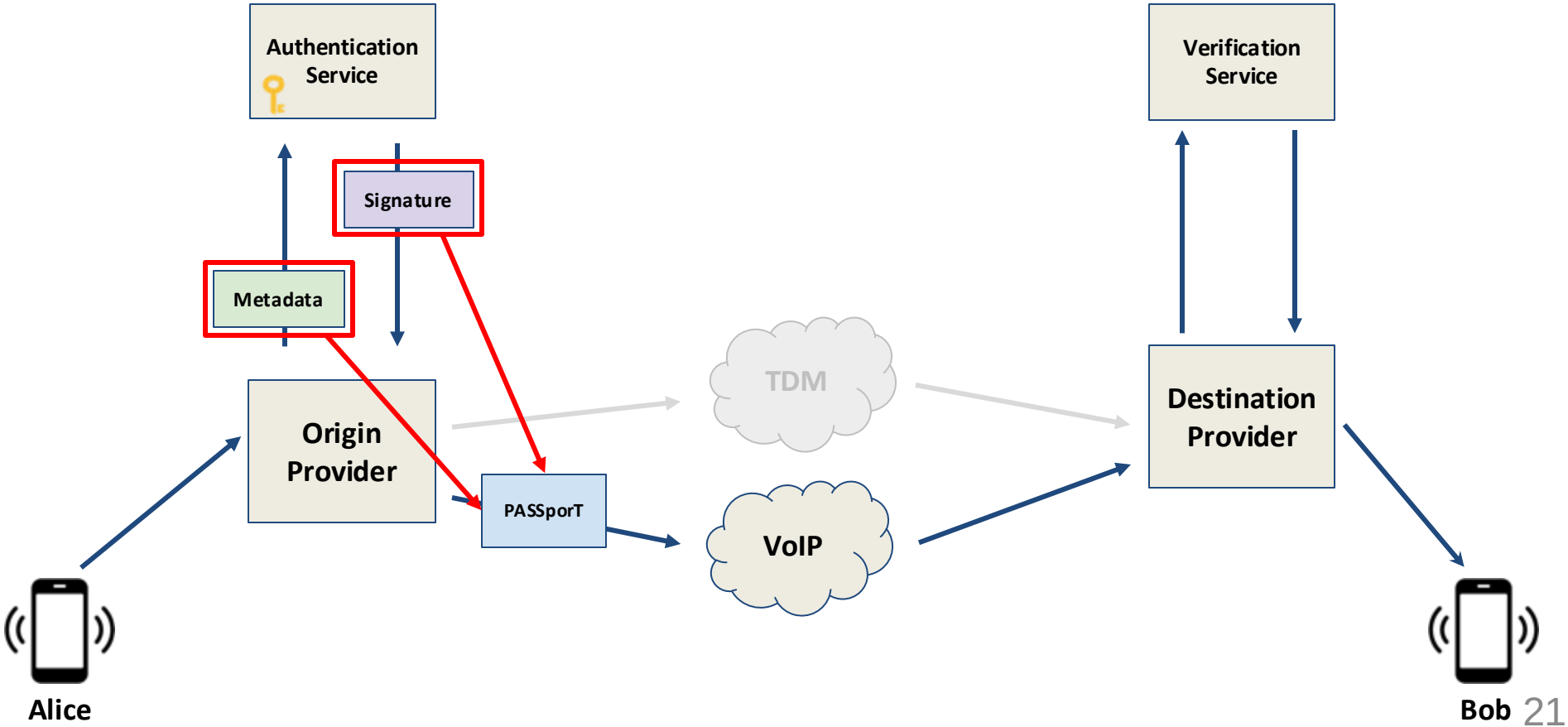
STIR/SHAKEN: Architecture



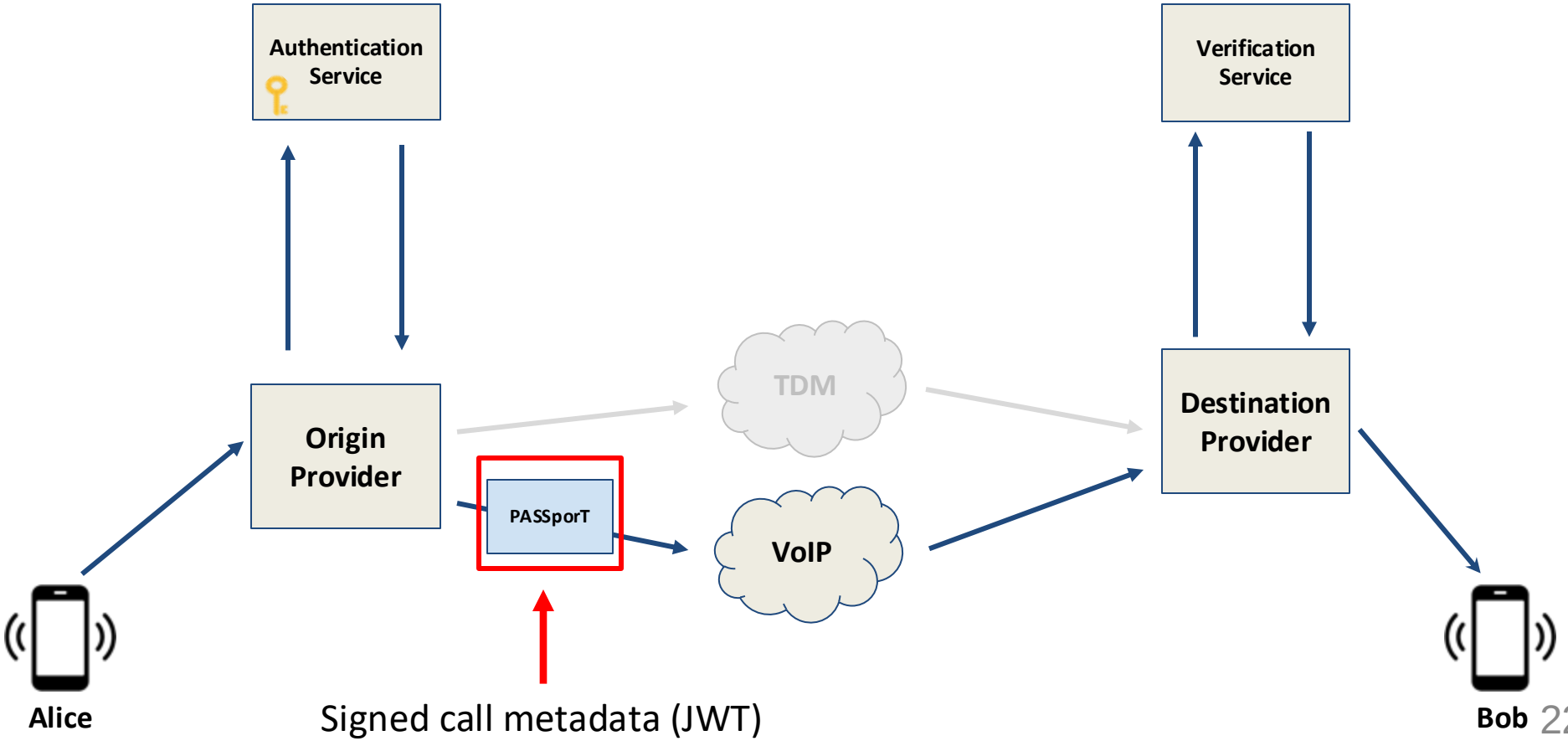
STIR/SHAKEN: Architecture



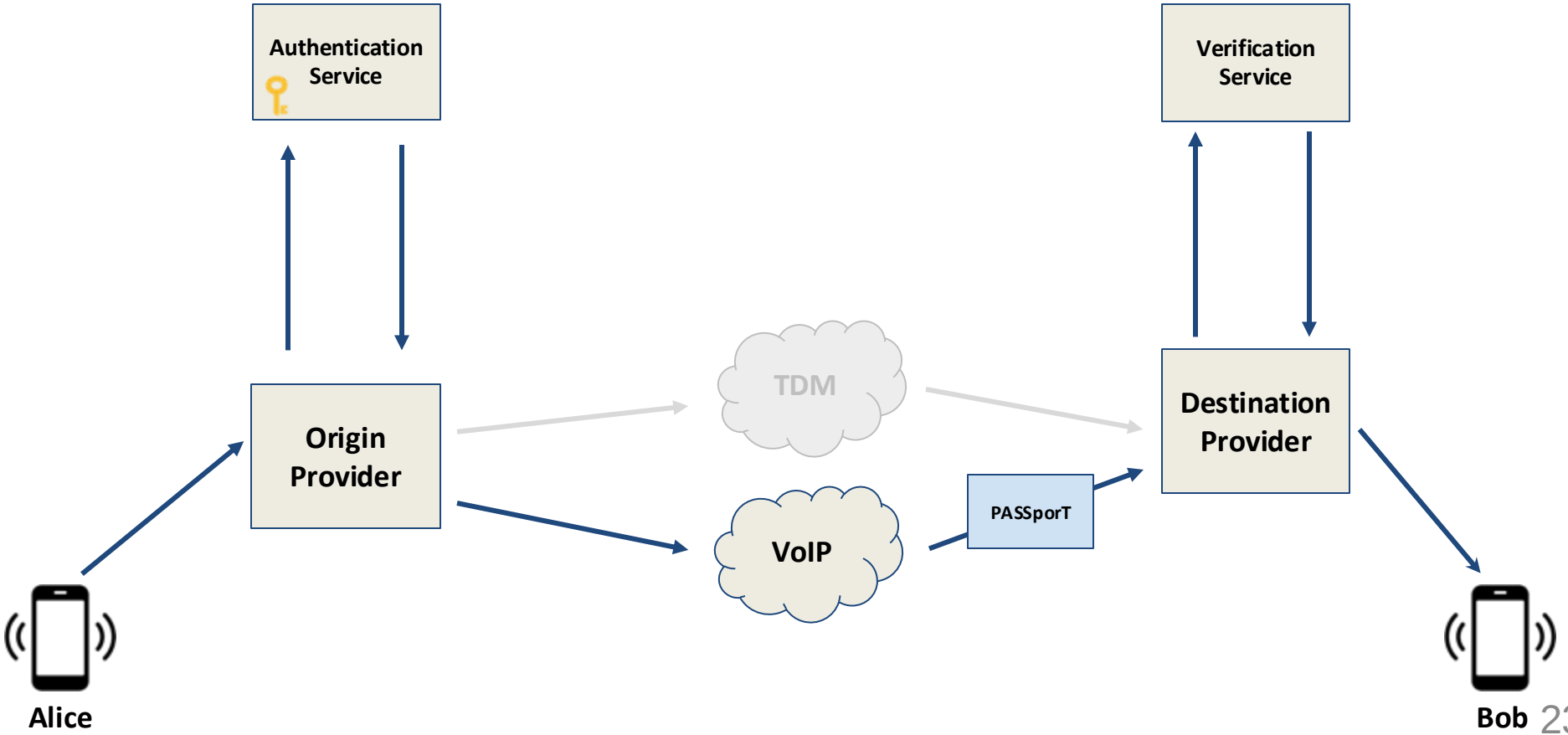
STIR/SHAKEN: Architecture



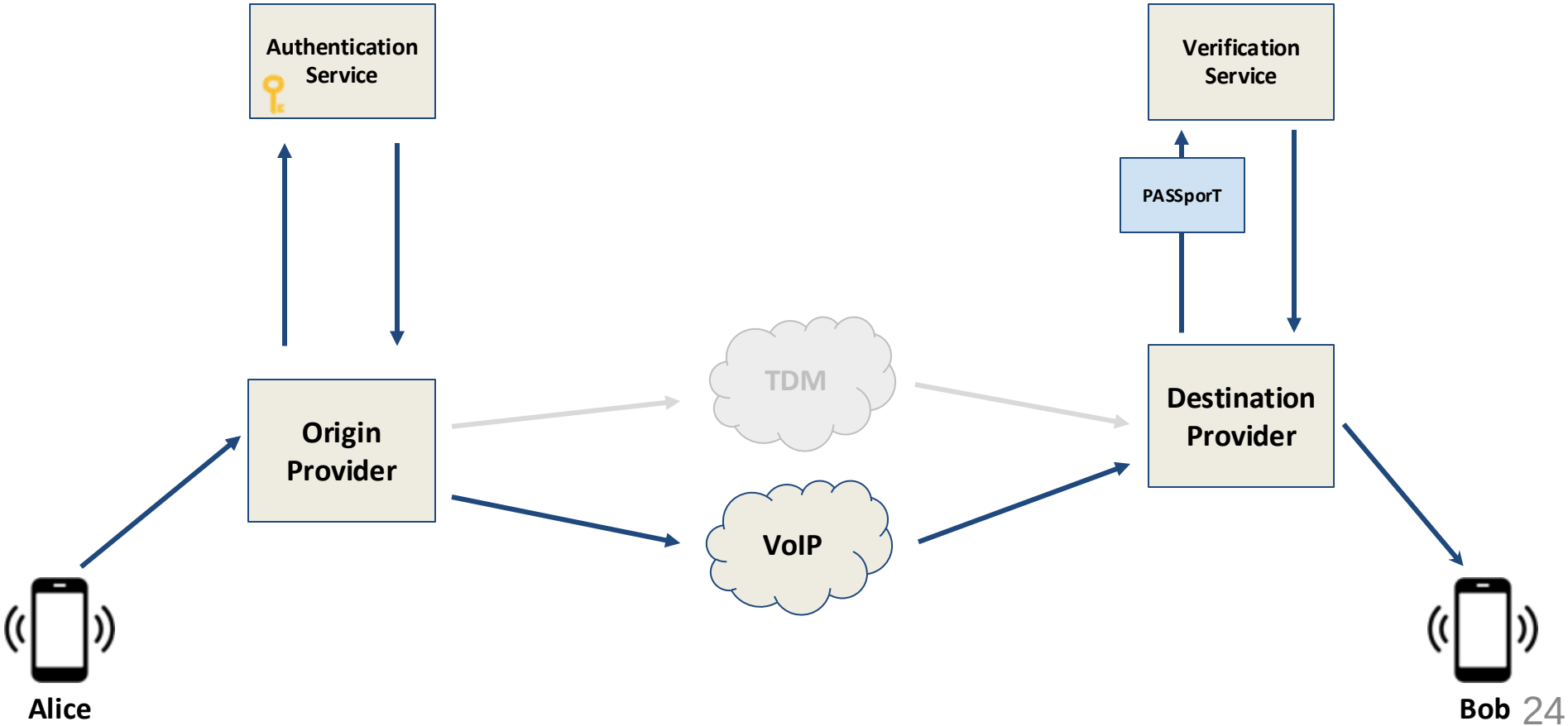
STIR/SHAKEN: Architecture



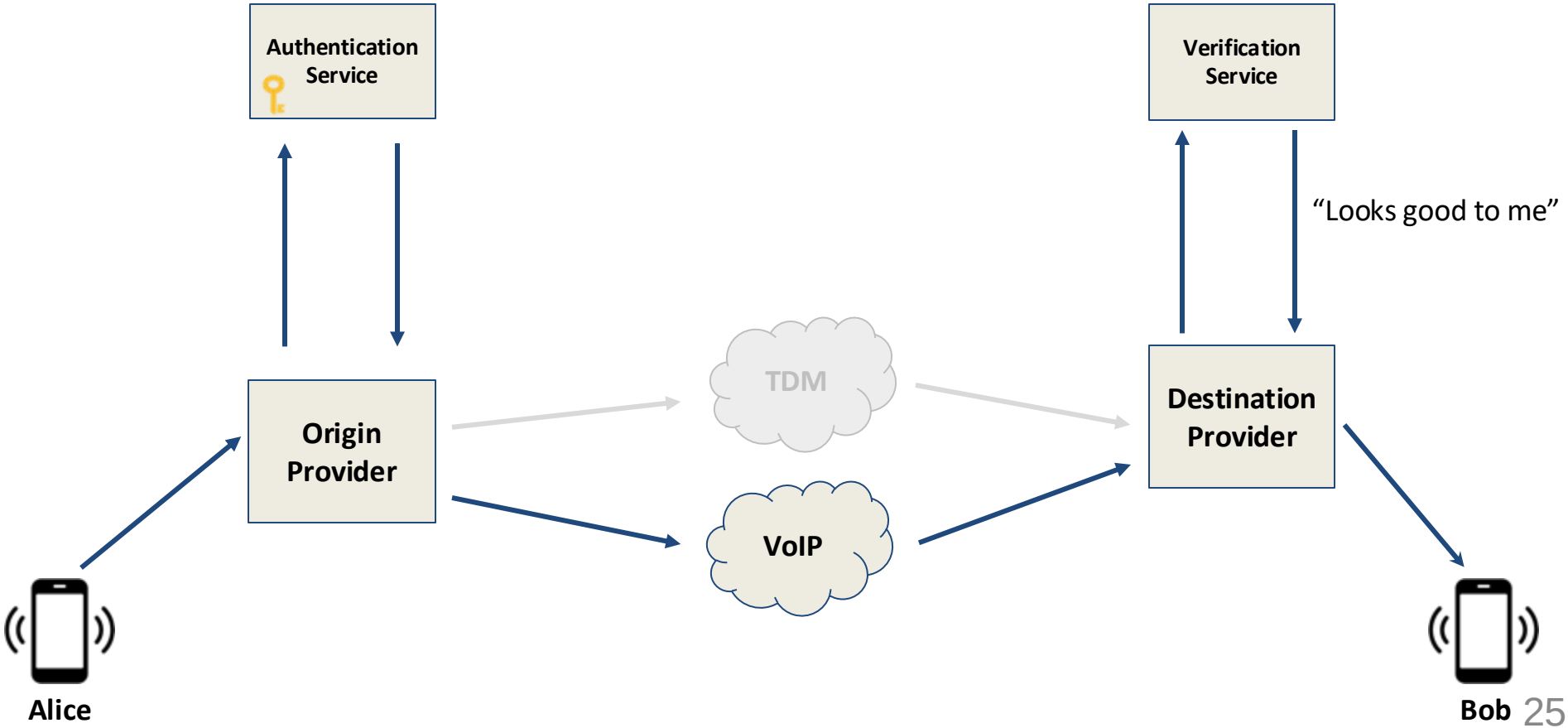
STIR/SHAKEN: Architecture



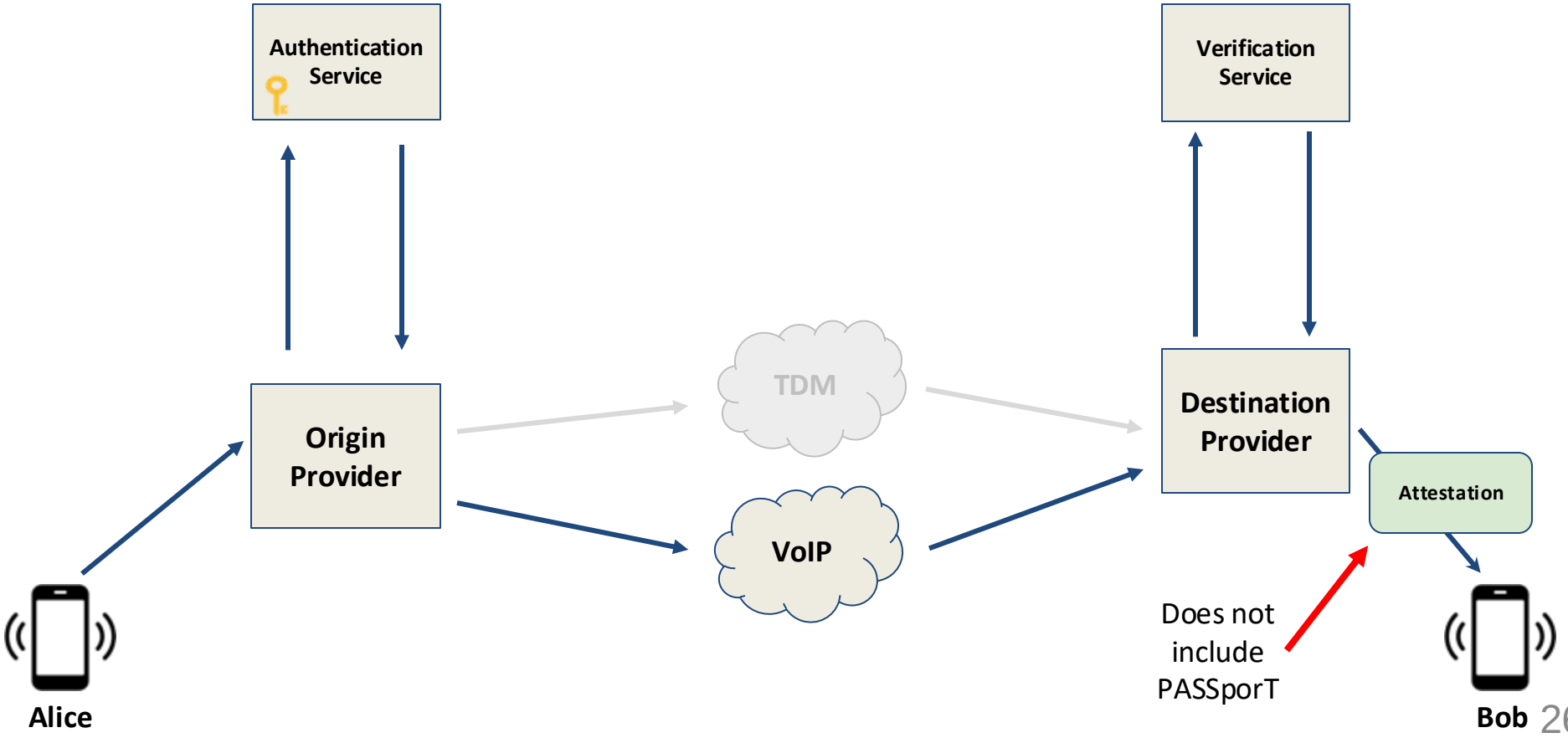
STIR/SHAKEN: Architecture



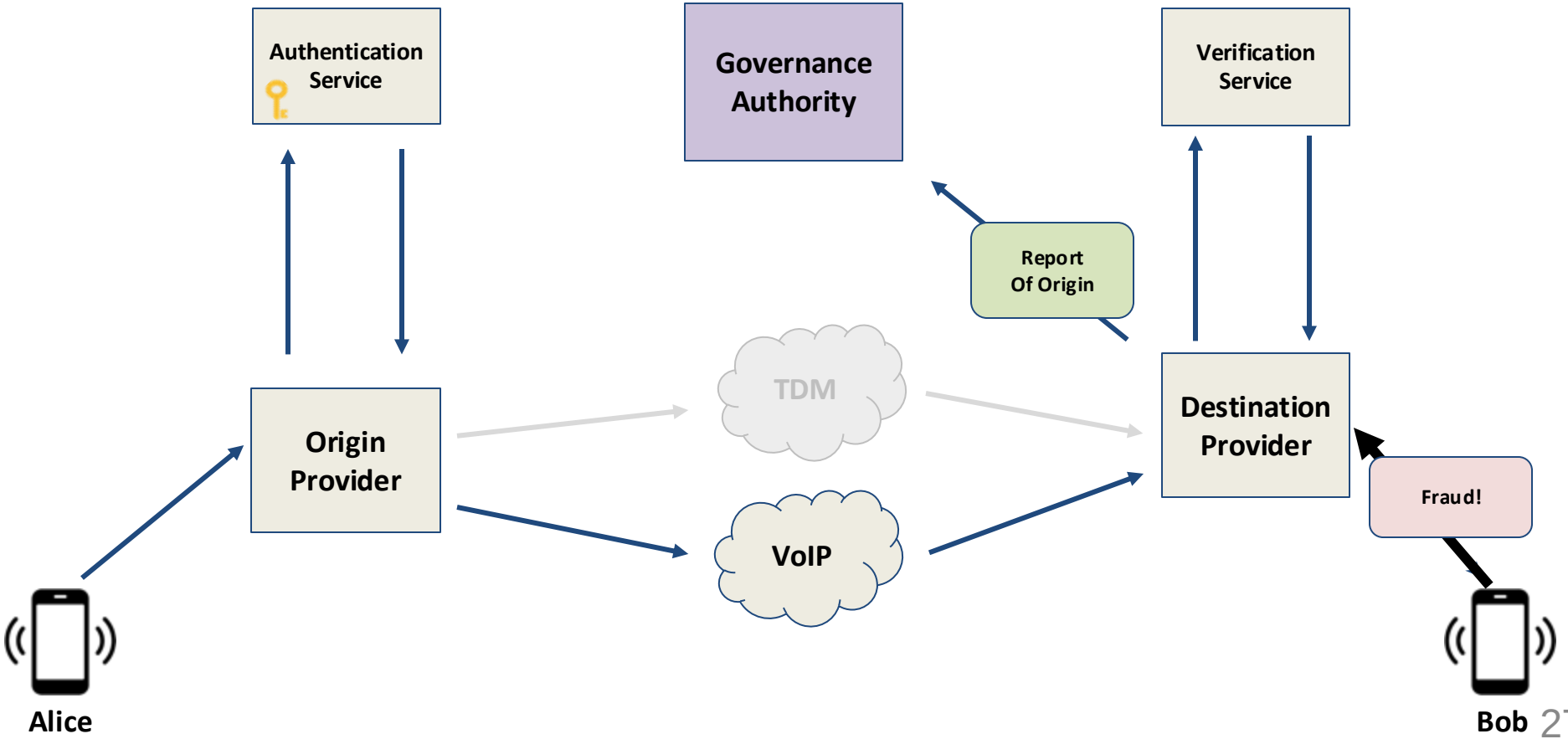
STIR/SHAKEN: Architecture



STIR/SHAKEN: Architecture



STIR/SHAKEN: Architecture



SIP INVITE With STIR/SHAKEN

```
INVITE sip:+14155552222@example.att.com SIP/2.0
Via: SIP/2.0/UDP 1.2.3.4:5060;branch=z9hG4bK776asdhds
Max-Forwards: 70
To: "Bob" <sip:+14155552222@example.att.com>
From: "Alice" <sip:+14155551111@example.pstn.verizon.com>;tag=1
Call-ID: a84b4c76e66710
CSeq: 1 INVITE
Contact: "Alice" <sip:+14155551111@1.2.3.4:5060>
Content-Length:
Identity:
eyJhbGciOiJFUzI1NiIsInBwdCI6InNoYWtlbiIsInR5cCI6InBhc3Nwb3J0IiwieDV1IjoiaHR0cH
M6Ly9jZXJ0LmV4YW1wbGUub3JnL3Bhc3Nwb3J0LnBlbSJ9.eyJhdHRlc3QiOiJBIiwiZGVzdCI6eyJ
0biI6WyIxMjEyNTU1MTIxMyJdfSwiaWF0IjoxNDcxMzc1NDE4LCJvcmlnIjp7InRuIjoiMTIxNTU1N
TEyMTIifSwib3JpZ2lkIjoiMTIzZTQ1NjctZTg5Yi0xMmQzLWE0NTYtNDI2NjU1NDQwMDAwIn0._V4
1ThRJ74MktxeLGaZQGAir8pcIvmB6OQEMgS4Ym7FPwGxm3tDUTRTpQ5X0relYset-
EScb9otFNDxOCTjerg;info=<https://cert.example.org/passport.pem>;ppt="shaken"
```

SIP INVITE With STIR/SHAKEN

```
INVITE sip:+14155552222@example.att.com SIP/2.0
Via: SIP/2.0/UDP 1.2.3.4:5060;branch=z9hG4bK776asdhds
Max-Forward
To: "Bob" <
From: "Alic
Call-ID: a8
CSeq: 1 INV
Contact: "A
Content-Len
Identity:
eyJhbGciOiJFUzI1NiIsInBwdCI6InNoYWtlbiIsInR5cCI6InBhc3Nwb3J0IiwieDV1IjoiaHR0cH
M6Ly9jZXJ0LmV4YW1wbGUub3JnL3Bhc3Nwb3J0LnBlbSJ9.eyJhdHRlc3QiOiJBIiwiZGVzdCI6eyJ
0biI6WyIxMjEyNTU1MTIxMyJdfSwiaWF0IjoxNDcxMzc1NDE4LCJvcmlnIjp7InRuIjoiMTIxNTU1N
TEyMTIifSwib3JpZ2lkIjoiMTIzZTQ1NjctZTg5Yi0xMmQzLWE0NTYtNDI2NjU1NDQwMDAwIn0._V4
1ThRJ74MktxeLGaZQGAir8pcIvmB6OQEMgS4Ym7FPwGxm3tDUTRTpQ5X0relYset-
EScb9otFNDxOCTjerg;info=<https://cert.example.org/passport.pem>;ppt="shaken"
```

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

(ECDSA using P-256 and SHA-256)

SIP INVI

```
{
  "attest": "A",
  "dest": {
        "tn": [
        "14155552222"
        ]
  },
  "iat": 1471375418,
  "orig": {
        "tn": "14155551111"
  },
  "origid": "123e4567-e89b-12d3-a456-426655440000"
}
```

```
INVITE sip:+1
Via: SIP/2.0/
Max-Forwards:
To: "Bob" <si
From: "Alice"
Call-ID: a84b
CSeq: 1 INVIT
Contact: "Ali
Content-Lengt
Identity:
eyJhbGciOiJFUzI1NiIsInBwdCI6InNoYWtlbiIsInR5cCI6InBhc3Nwb3J0IiwieDV1IjoiaHR0cH
M6Ly9jZXJ0LmV4YW1wbGUub3JnL3Bhc3Nwb3J0LnBlbSJ9.eyJhdHRlc3QiOiJBIiwiZGVzdCI6eyJ
0bi I6WyIxMjEyNTU1MTIxMyJdfSwiaWF0IjoxNDcxMzc1NDE4LCJvcmlnIjp7InRuIjoiMTIxNTU1N
TEyMTIifSwib3JpZ2lkIjoiMTIzZTQ1NjctZTg5Yi0xMmQzLWE0NTYtNDI2NjU1NDQwMDAwIn0._V4
1ThRJ74MktxeLGaZQGAir8pcIvmB6OQEMgS4Ym7FPwGxm3tDUTRTpQ5X0relYset-
EScb9otFNDxOCTjerg;info=<https://cert.example.org/passport.pem>;ppt="shaken"
```

SIP INVI

```
{
  "attest": "A",
  "dest": {
        "tn": [
        "14155552222"
        ]
  },
  "iat": 1471375418,
  "orig": {
        "tn": "14155551111"
  },
  "origid": "123e4567-e89b-12d3-a456-426655440000"
}
```

A, B, C refer to **different signer confidence** levels of various metadata

```
INVITE sip:+1
Via: SIP/2.0/
Max-Forwards:
To: "Bob" <si
From: "Alice"
Call-ID: a84b
CSeq: 1 INVIT
Contact: "Ali
Content-Lengt
Identity:
eyJhbGciOiJFUzI1NiIsInBwdCI6InNoYWtlbiIsInR5cCI6InBhc3Nwb3J0IiwieDV1IjoiaHR0cH
M6Ly9jZXJ0LmV4YW1wbGUub3JnL3Bhc3Nwb3J0LnBlbSJ9.eyJhdHRlc3QiOiJBIiwiZGVzdCI6eyJ
0bi I6WyIxMjEyNTU1MTIxMyJdfSwiaWF0IjoxNDcxMzc1NDE4LCJvcmlnIjp7InRuIjoiMTIxNTU1N
TEyMTIifSwib3JpZ2lkIjoiMTIzZTQ1NjctZTg5Yi0xMmQzLWE0NTYtNDI2NjU1NDQwMDAwIn0._V4
1ThRJ74MktxeLGaZQGAir8pcIvmB6OQEMgS4Ym7FPwGxm3tDUTRTpQ5X0relYset-
EScb9otFNDxOCTjerg;info=<https://cert.example.org/passport.pem>;ppt="shaken"
```

SIP INVI

```
{
  "attest": "A",
  "dest": {
        "tn": [
        "14155552222"
        ]
  },
  "iat": 1471375418,
  "orig": {
        "tn": "14155551111"
  },
  "origid": "123e4567-e89b-12d3-a456-426655440000"
}
```

```
INVITE sip:+1
Via: SIP/2.0/
Max-Forwards:
To: "Bob" <si
From: "Alice"
Call-ID: a84b
CSeq: 1 INVIT
Contact: "Ali
Content-Lengt
Identity:
eyJhbGciOiJFUzI1NiIsInBwdCI6InNoYWtlbiIsInR5cCI6InBhc3Nwb3J0IiwieDV1IjoiaHR0cH
M6Ly9jZXJ0LmV4YW1wbGUub3JnL3Bhc3Nwb3J0LnBlbSJ9.eyJhdHRlc3QiOiJBIiwiZGVzdCI6eyJ
0bi I6WyIxMjEyNTU1MTIxMyJdfSwiaWF0IjoxNDcxMzc1NDE4LCJvcmlnIjp7InRuIjoiMTIxNTU1N
TEyMTIifSwib3JpZ2lkIjoiMTIzZTQ1NjctZTg5Yi0xMmQzLWE0NTYtNDI2NjU1NDQwMDAwIn0._V4
1ThRJ74MktxeLGaZQGAir8pcIvmB6OQEMgS4Ym7FPwGxm3tDUTRTpQ5X0relYset-
EScb9otFNDxOCTjerg;info=<https://cert.example.org/passport.pem>;ppt="shaken"
```

SIP INVI

```
{
  "attest": "A",
  "dest": {
          "tn": [
          "14155552222"
          ]
  },
  "iat": 1471375418,
  "orig": {
          "tn": "14155551111"
  },
  "origid": "123e4567-e89b-12d3-a456-426655440000"
}
```

```
INVITE sip:+1
Via: SIP/2.0/
Max-Forwards:
To: "Bob" <si
From: "Alice"
Call-ID: a84b
CSeq: 1 INVIT
Contact: "Ali
Content-Lengt
Identity:
eyJhbGciOiJFUzI1NiIsInBwdCI6InNoYWtlbiIsInR5cCI6InBhc3Nwb3J0IiwieDV1IjoiaHR0cH
M6Ly9jZXJ0LmV4YW1wbGUub3JnL3Bhc3Nwb3J0LnBlbSJ9.eyJhdHRlc3QiOiJBIiwiZGVzdCI6eyJ
0bi I6WyIxMjEyNTU1MTIxMyJdfSwiaWF0IjoxNDcxMzc1NDE4LCJvcmlnIjp7InRuIjoiMTIxNTU1N
TEyMTIifSwib3JpZ2lkIjoiMTIzZTQ1NjctZTg5Yi0xMmQzLWE0NTYtNDI2NjU1NDQwMDAwIn0._V4
1ThRJ74MktxeLGaZQGAir8pcIvmB6OQEMgS4Ym7FPwGxm3tDUTRTpQ5X0relYset-
EScb9otFNDxOCTjerg;info=<https://cert.example.org/passport.pem>;ppt="shaken"
```

SIP INVI

```
{
  "attest": "A",
  "dest": {
        "tn": [
        "14155552222"
        ]
  },
  "iat": 1471375418,
  "orig": {
        "tn": "14155551111"
  },
  "origid": "123e4567-e89b-12d3-a456-426655440000"
}
```

```
INVITE sip:+1
Via: SIP/2.0/
Max-Forwards:
To: "Bob" <si
From: "Alice"
Call-ID: a84b
CSeq: 1 INVIT
Contact: "Ali
Content-Lengt
Identity:
eyJhbGciOiJFUzI1NiIsInBwdCI6InNoYWtlbiIsInR5cCI6InBhc3Nwb3J0IiwieDV1IjoiaHR0cH
M6Ly9jZXJ0LmV4YW1wbGUub3JnL3Bhc3Nwb3J0LnBlbSJ9.eyJhdHRlc3QiOiJBIiwiZGVzdCI6eyJ
0bnI6WyIxMjEyNTU1MTIxMyJdfSwiaWF0IjoxNDcxMzc1NDE4LCJvcmlnIjp7InRuIjoiMTIxNTU1N
TEyMTIifSwib3JpZ2lkIjoiMTIzZTQ1NjctZTg5Yi0xMmQzLWE0NTYtNDI2NjU1NDQwMDAwIn0._V4
1ThRJ74MktxeLGaZQGAir8pcIvmB6OQEMgS4Ym7FPwGxm3tDUTRTpQ5X0relYset-
EScb9otFNDxOCTjerg;info=<https://cert.example.org/passport.pem>;ppt="shaken"
```

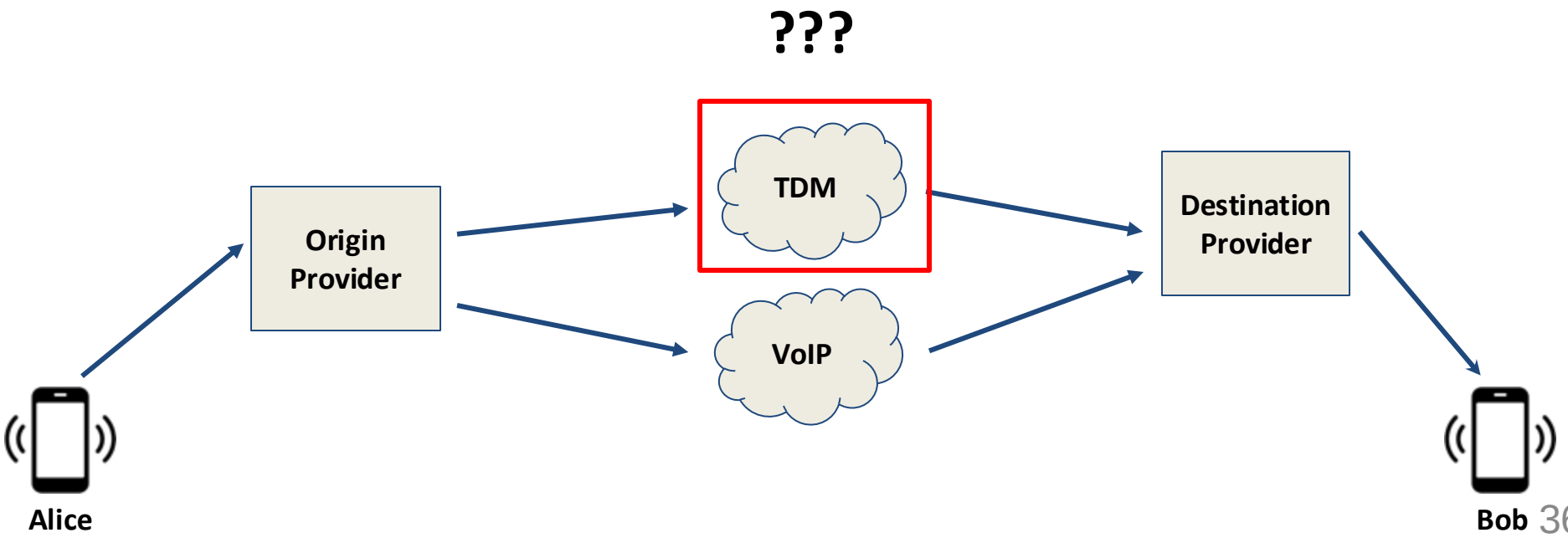
SIP INVITE With STIR/SHAKEN

```
INVITE sip:+14155552222@example.att.com SIP/2.0
Via: SIP/2.0/UDP 1.2.3.4:5060;branch=z9hG4bK776asdhds
Max-Forwards: 70
To: "Bob" <sip:+14155552222@example.att.com>
From: "Alice" <sip:+14155551111@example.pstn.verizon.com>;tag=1
Call-ID: a84b4c76e66710
CSeq: 1 INVITE
Contact: <sip:+14155551111@1.2.3.4:5060>
Content-Length: 0
Identity:
eyJhbGciOiJFUzI1NiIsInBwdCI6InNoYWtlbiIsInR5cCI6InBhc3Nwb3J0IiwieDV1IjoiaHR0cH
M6Ly9jZXJ0LmV4YW1wbGUub3JnL3Bhc3Nwb3J0LnBlbSJ9.eyJhdHRlc3QiOiJBIiwiZGVzdCI6eyJ
0biI6WyIxMjEyNTU1MTIxMyJdfSwiaWF0IjoxNDcxMzc1NDE4LCJvcmlnIjp7InRuIjoiMTIxNTU1N
TEyMTIifSwib3JpZ2lkIjoiMTIzZTQ1NjctZTg5Yi0xMmQzLWE0NTYtNDI2NjU1NDQwMDAwIn0.
_V4
1ThRJ74MktxeLGaZQGAir8pcIvmB6OQEMgS4Ym7FPwGxm3tDUTRTpQ5X0relYset-
EScb9otFNDxOCTjerg;info=<https://cert.example.org/passport.pem>;ppt="shaken"
```

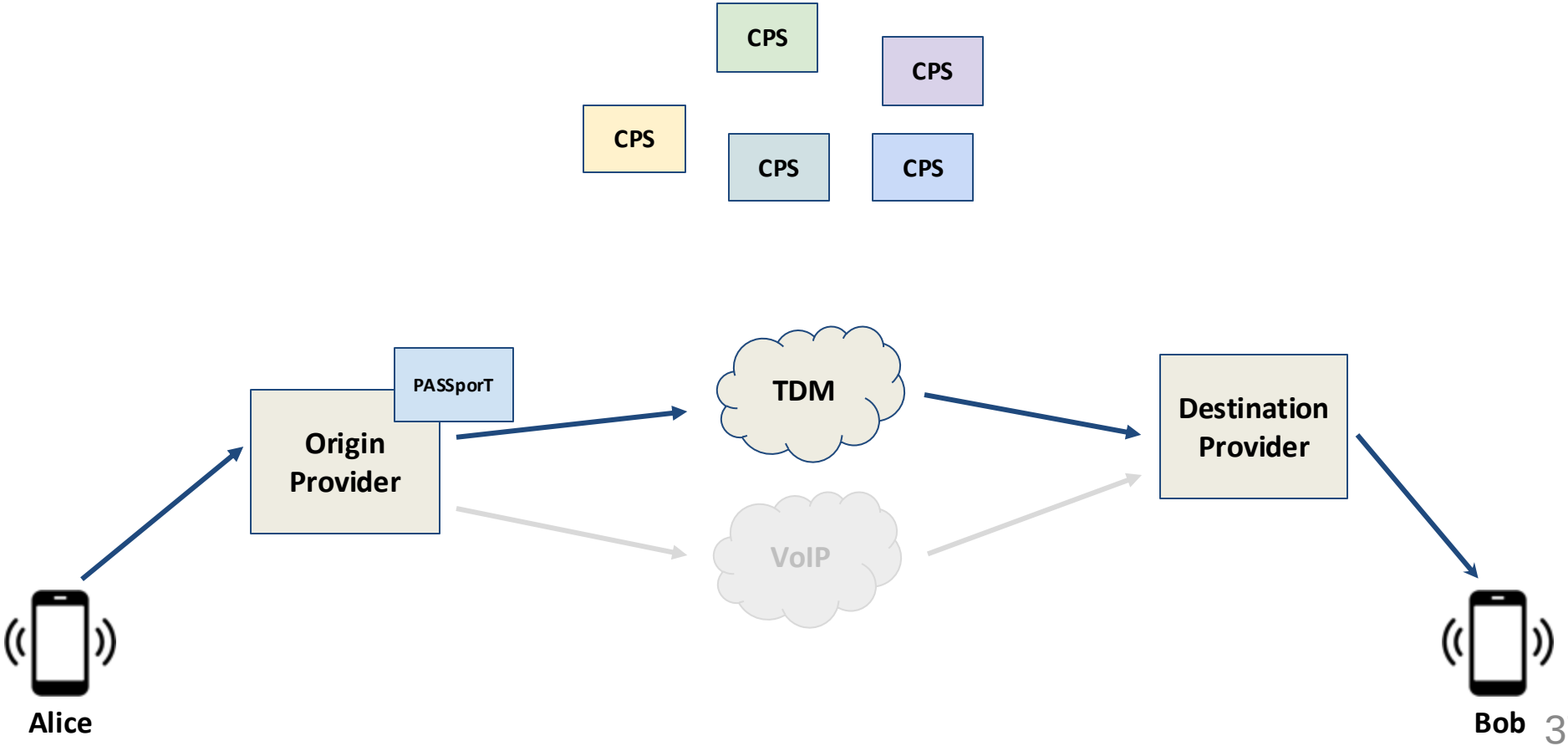
ECDSASHA256(base64(header) + "." + base64(payload), SK)

Note: This signature is for illustrative purposes and doesn't actually verify properly

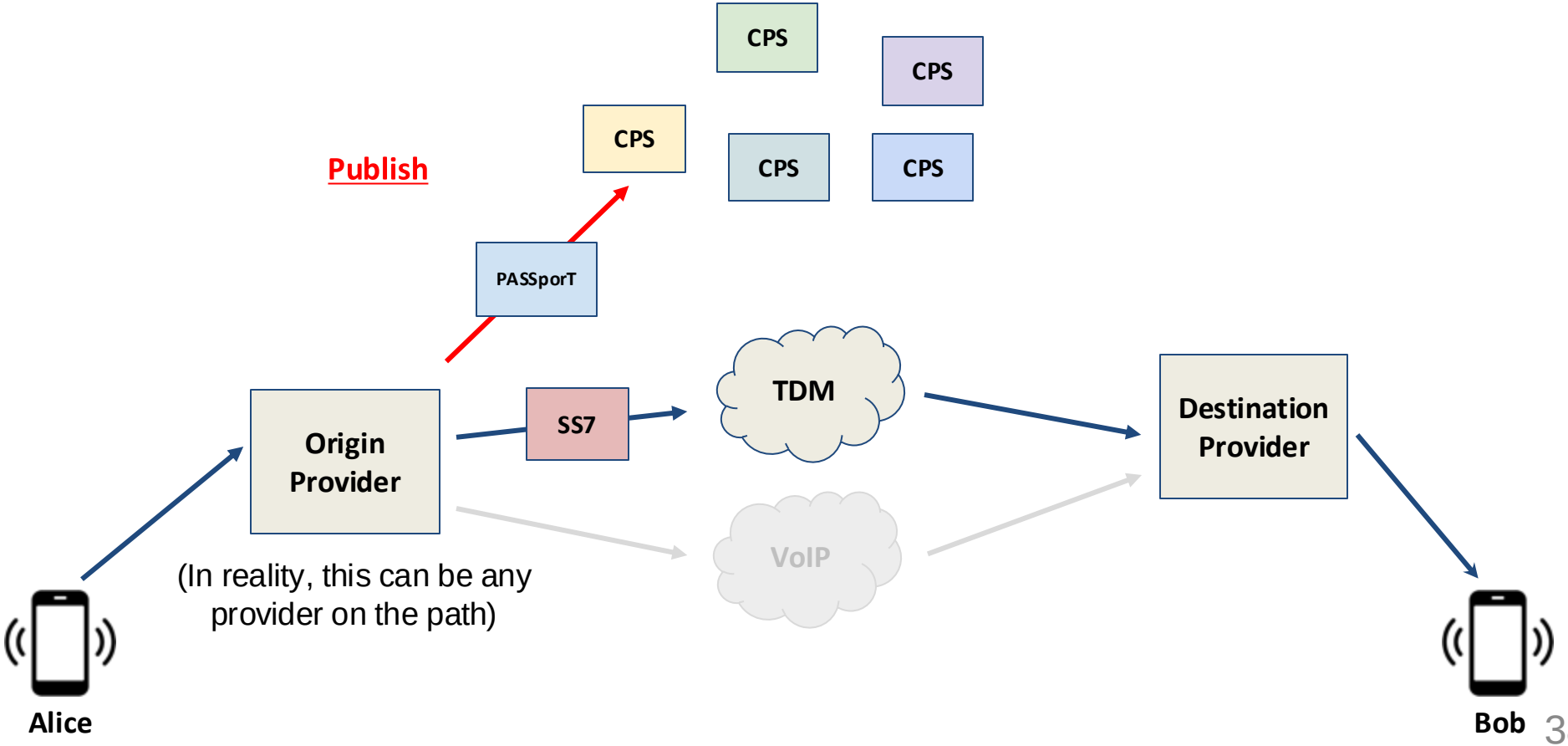
STIR/SHAKEN for TDM (?)



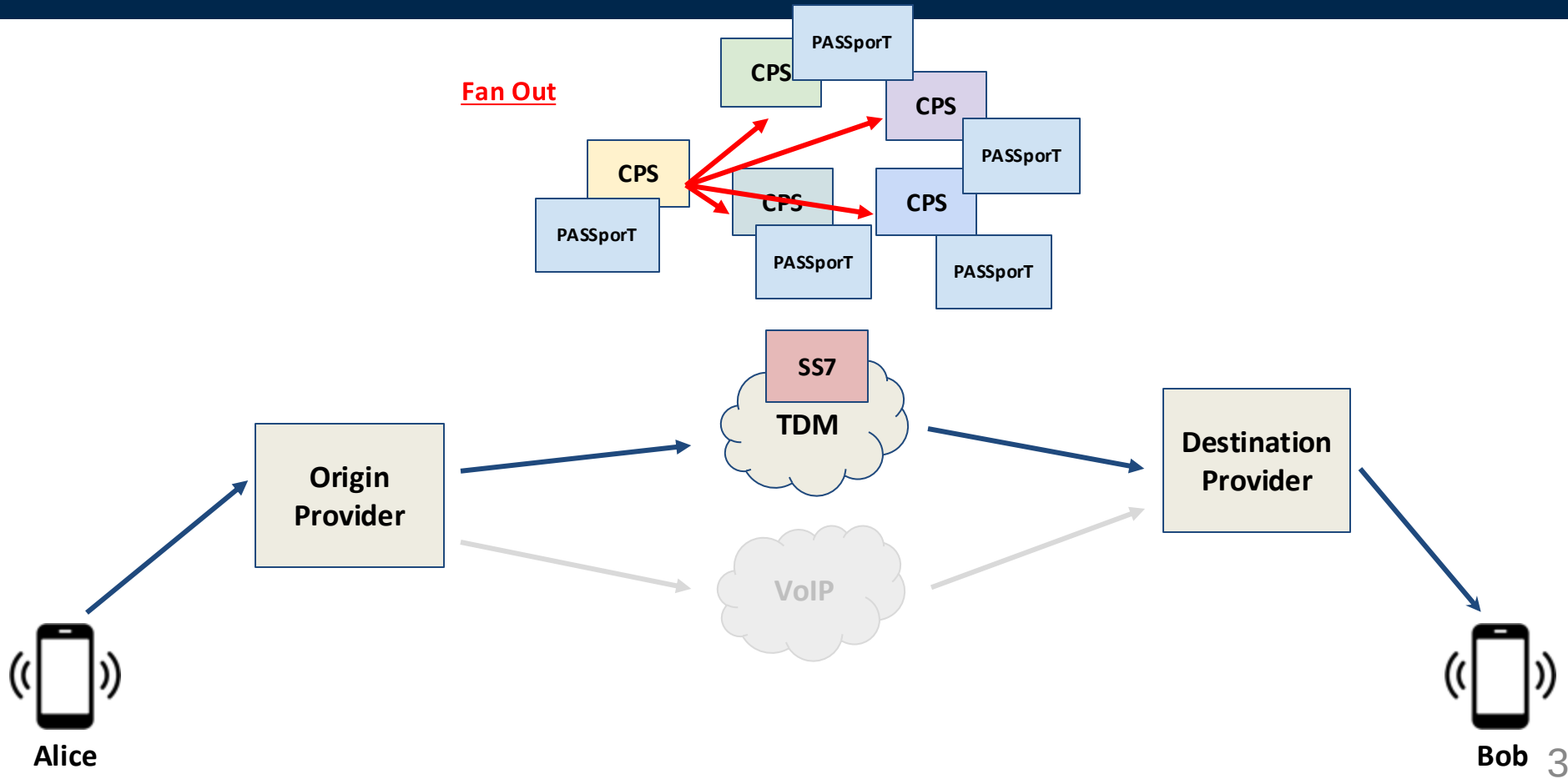
Out-Of-Band STIR/SHAKEN: Architecture



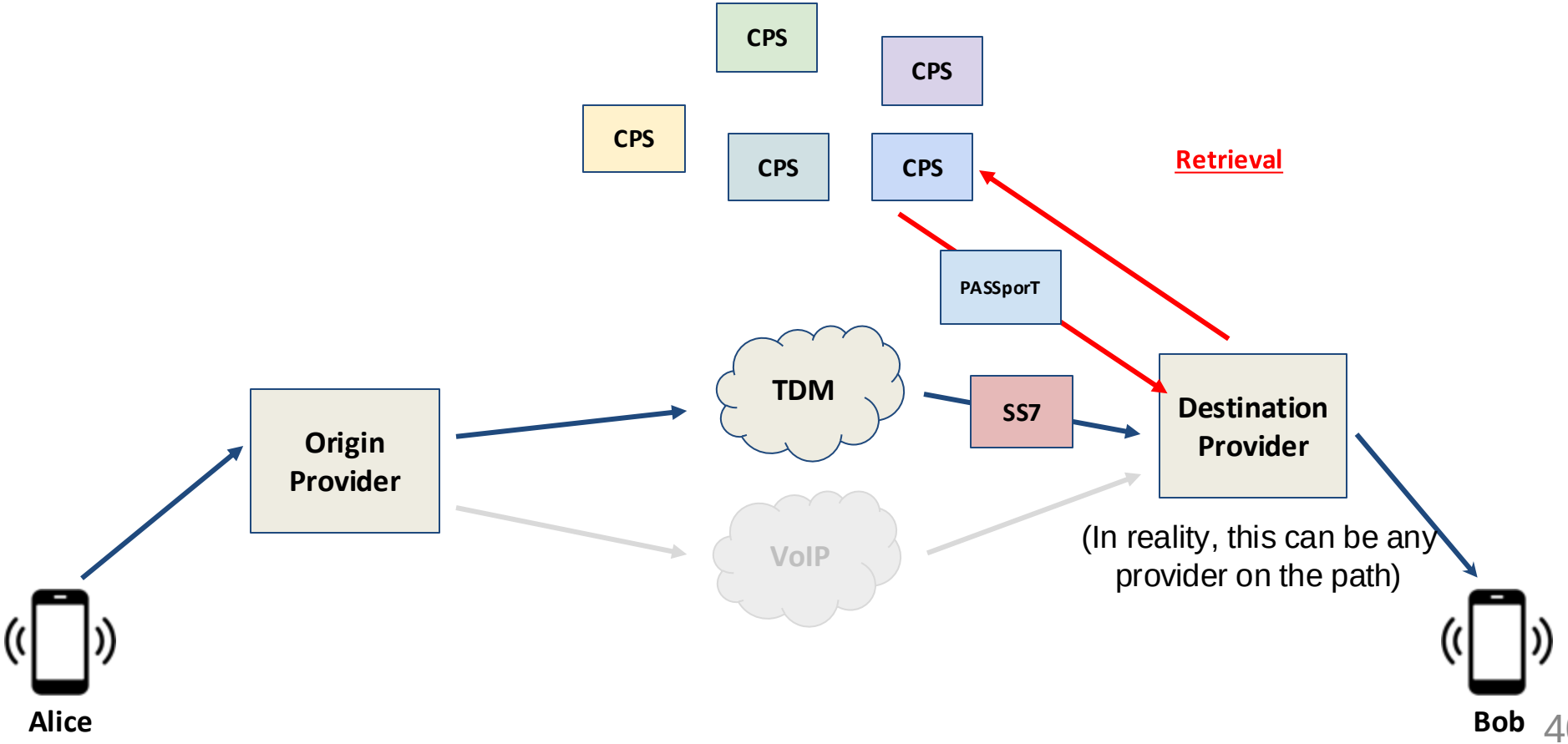
Out-Of-Band STIR/SHAKEN: Architecture



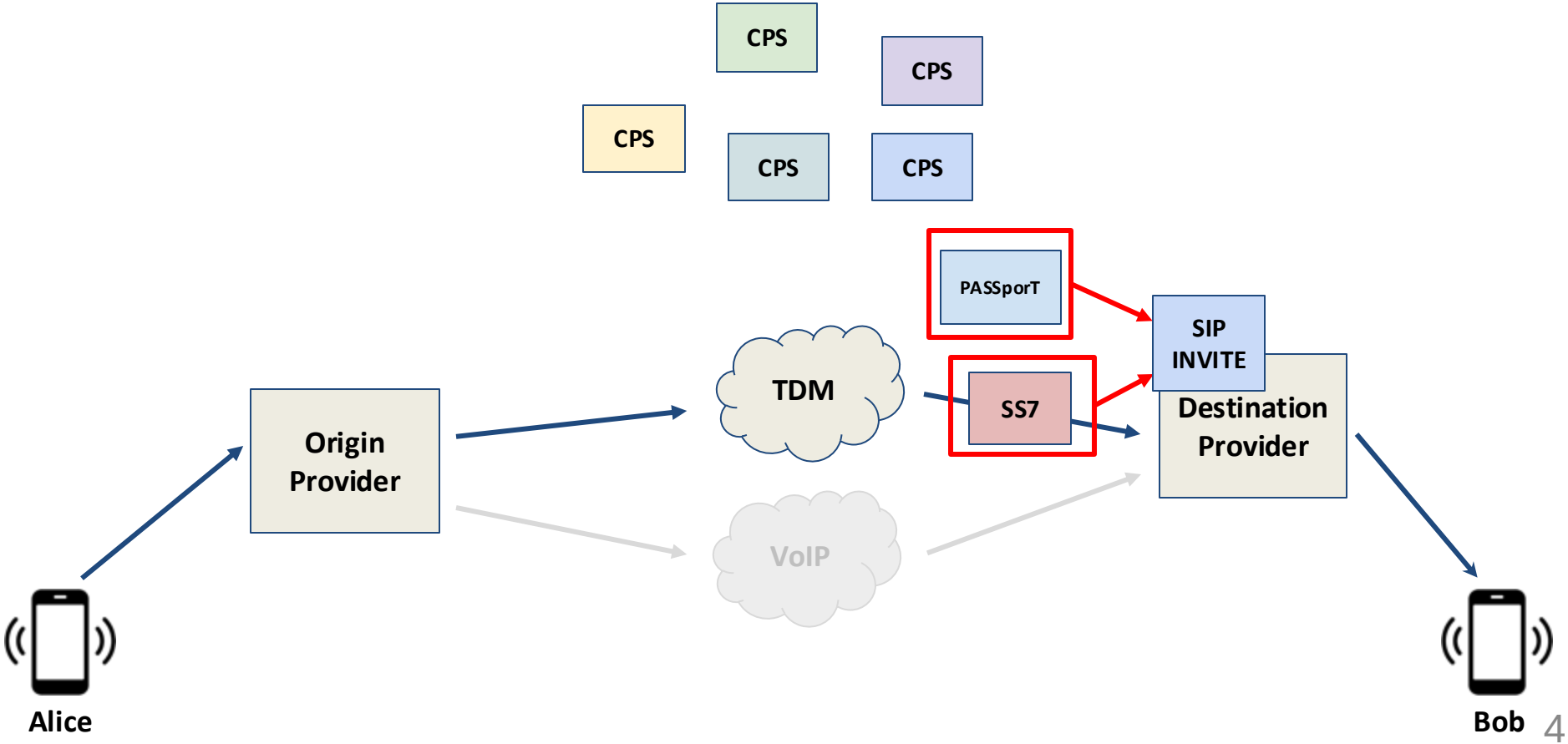
Out-Of-Band STIR/SHAKEN: Architecture



Out-Of-Band STIR/SHAKEN: Architecture



Out-Of-Band STIR/SHAKEN: Architecture



Summary of Background

- PSTN: either just VoIP or VoIP + TDM
- SIP: setup/teardown protocol for VoIP calls. Has “INVITE” msg
- STIR/SHAKEN lets telcos make assertions about caller identity
- PASSporTs: Signed metadata (to/from numbers) in SIP INVITE
- For TDM calls, PASSporTs held by “drop box” (CPS)

Flaws

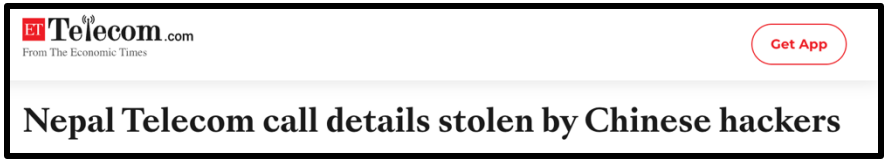
Deniability of Call Metadata

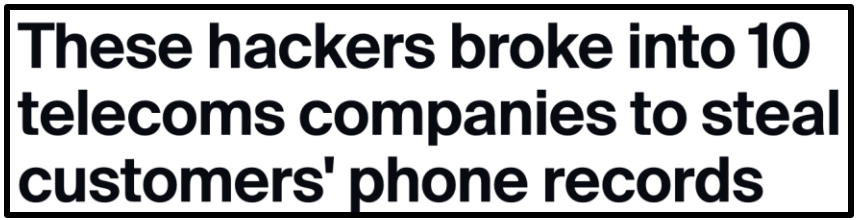
This PASSporT is cryptographic proof that Alice called Bob!

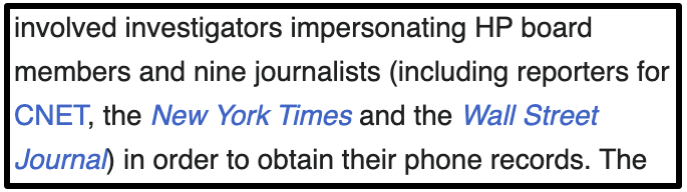
```
INVITE sip:+14155552222@example.att.com SIP/2.0
Via: SIP/2.0/UDP 1.2.3.4:5060;branch=z9hG4bK776asdhds
Max-Forwards: 70
To: "Bob" <sip:+14155552222@example.att.com>
From: "Alice" <sip:+14155551111@example.pstn.verizon.com>;tag=1
Call-ID: a84b4c76e66710
CSeq: 1 INVITE
Contact: "Alice" <sip:+14155551111@1.2.3.4:5060>
Content-Length:
Identity:
eyJhbGciOiJFUzI1NiIsInBwdCI6InNoYWtlbiIsInR5cCI6InBhc3Nwb3J0IiwieDV1IjoiaHR0cH
M6Ly9jZXJ0LmV4YW1wbGUub3JnL3Bhc3Nwb3J0LnBlbSJ9.eyJhdHRlc3QiOiJBIiwiZGVzdCI6eyJ
0biI6WyIxMjEyNTU1MTIxMyJdfSwiaWF0IjoxNDcxMzc1NDE4LCJvcmlnIjp7InRuIjoiMTIxNTU1N
TEyMTIifSwib3JpZ2lkIjoiMTIzZTQ1NjctZTg5Yi0xMmQzLWE0NTYtNDI2NjU1NDQwMDAwIn0._V4
1ThRJ74MktxeLGaZQGAir8pcIvmB6OQEMgS4Ym7FPwGxm3tDUTRTpQ5X0relYset-
EScb9otFNDxOCTjerg;info=<https://cert.example.org/passport.pem>;ppt="shaken"
```

Why is deniability important for call metadata?

- Makes stolen call logs easier to verify => incentivizes theft.
- Reduces “ephemerality” of calls.







Why is deniability important for call metadata?

AT&T says hackers stole records of nearly all cellular customers' calls and texts

The data contains records of calls and texts between approximately May 1 and Oct. 31, 2022, and on Jan. 2, 2023.

one report suggests AT&T paid a ransom for the hackers to delete the stolen data) and the data itself does not contain the contents of calls or text messages, the "metadata" still reveals who called who and when, and in some cases the

In July, AT&T said cybercriminals had stolen a cache of data that contained phone numbers and call records of "nearly all" of its customers, or around 110 million people, over a six-month

That was AT&T's second data breach this year. Earlier in March, a data breach broker dumped online a full cache of 73 million customer records to a known cybercrime forum for anyone to see, some three years after a much smaller sample was teased online.

Comparison to DKIM for Email

- DKIM, STIR/SHAKEN goals similar
- DKIM signatures are used to authenticate leaks
- DKIM signs email body, STIR/SHAKEN only metadata
- However, PASSporTs more available to intermediaries…

Authenticating Email Using DKIM and ARC, or How We Analyzed the Kasowitz Emails

The AP worked to authenticate the 200-odd documents, in some cases by verifying the digital signatures carried in email headers.

DKIM Deniability

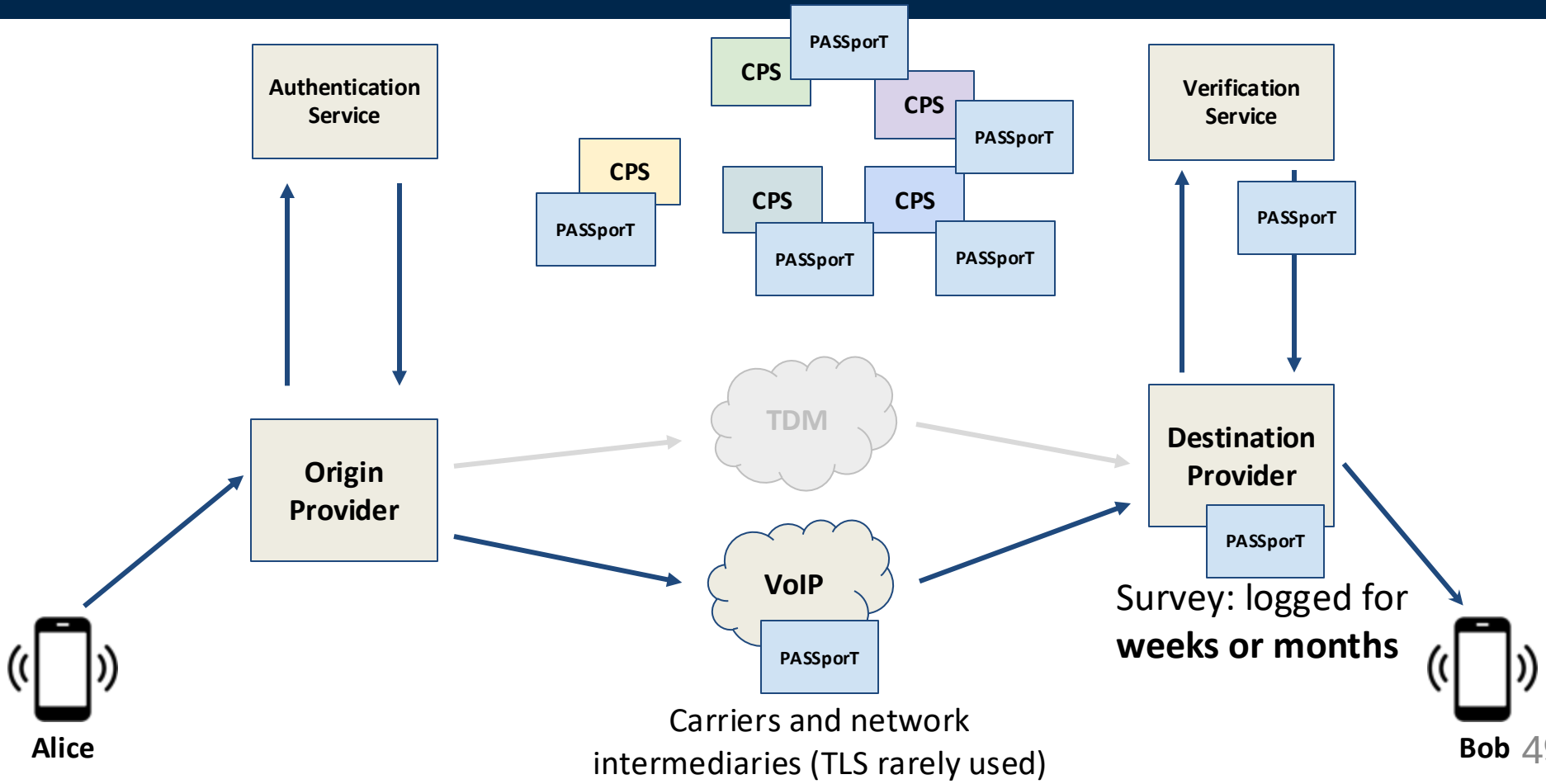
WikiLeaks released a trove of emails apparently hacked from Hillary Clinton's campaign chairman email account, unleashing thousands of messages that reveal for the first time excerpts of Clinton's paid speeches — including those delivered before Wall Street — that were flagged as problematic or potentially damaging.

WikiLeaks

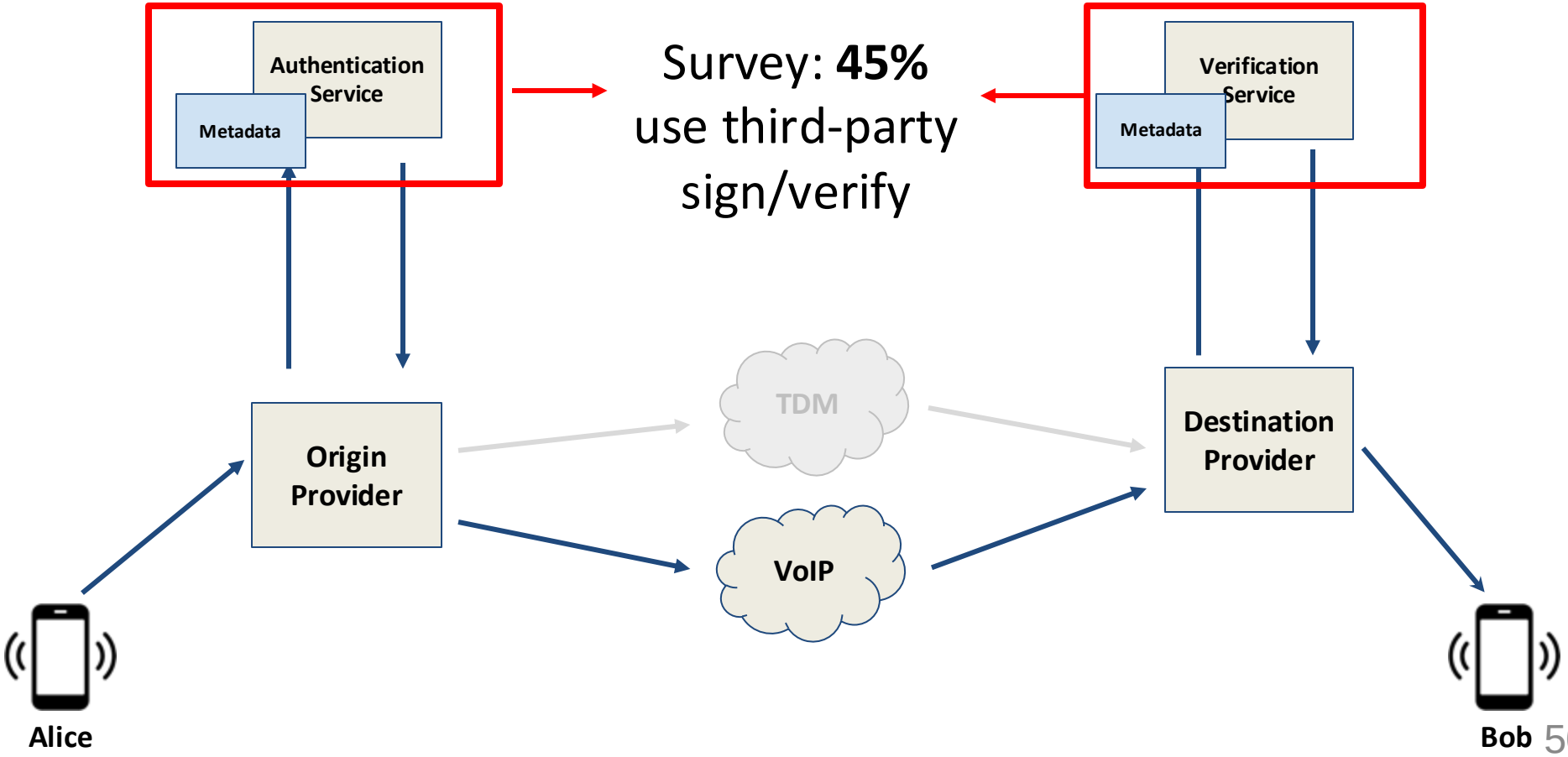
For example, an email that DNC Chair Donna Brazile falsely claimed to be "doctored by Russian sources" is in fact validated. Similarly validated is the email referencing a future appointment of Tim

In the Podesta email archive, many of the politically significant emails use DKIM authentication, including several contentious emails which some politicians have attempted to repudiate. These mails are, in fact, signed by HillaryClinton.com's email provider, Google. This authentication is on top of the journalistic

PASSporTs are everywhere…



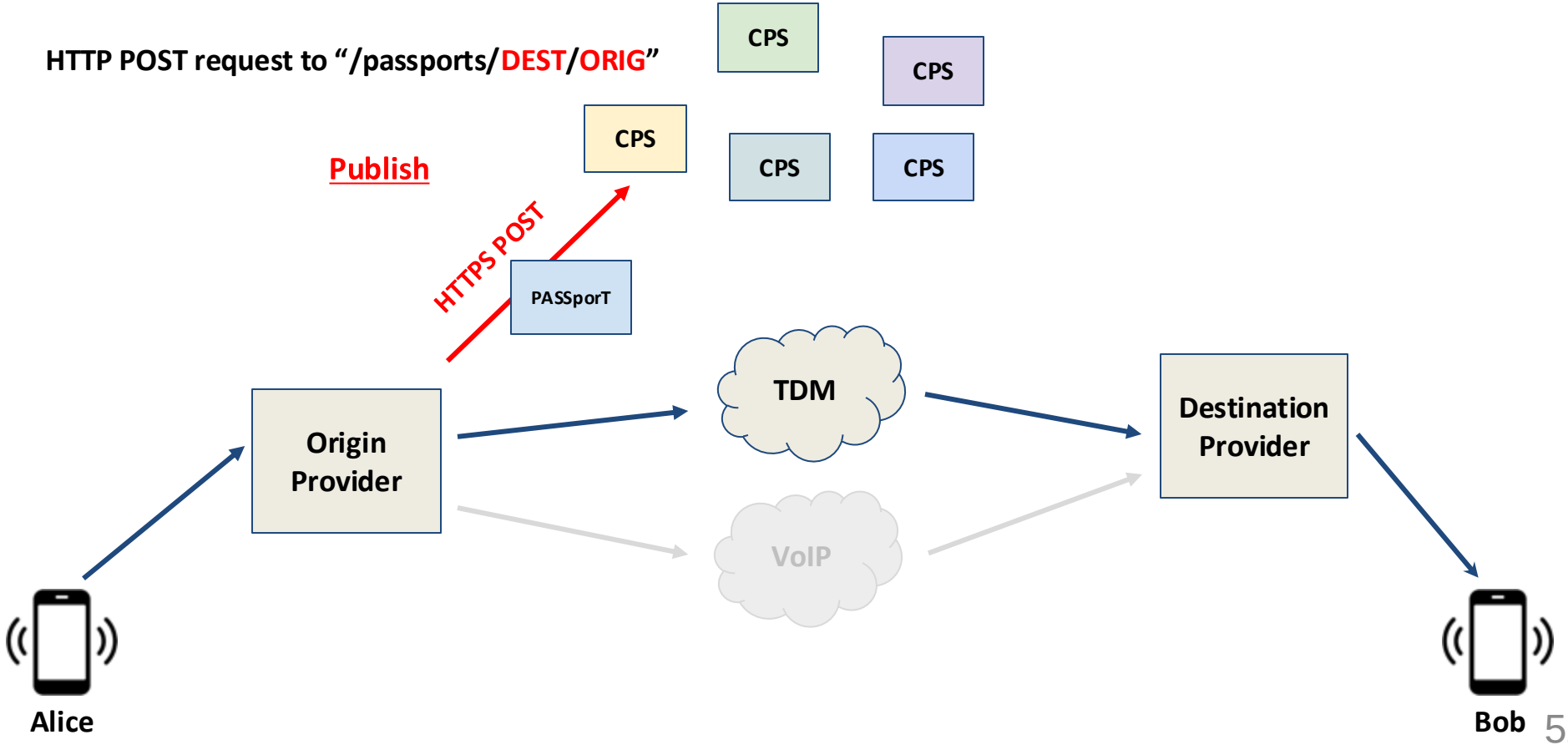
Metadata Leakage



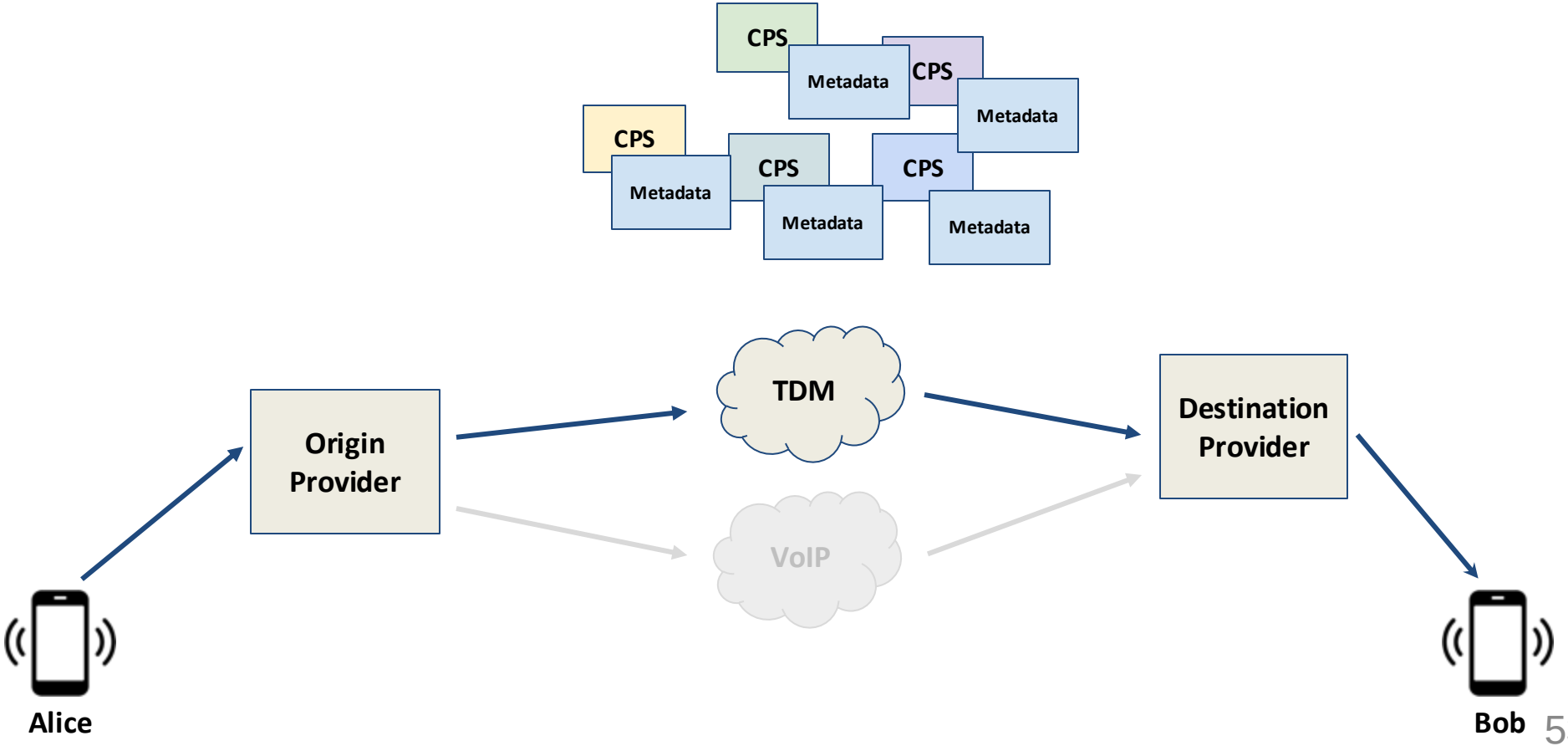
Why is call metadata sensitive?

Abortion clinic, political party, suicide hotline, religious organization, journalist, rehab…

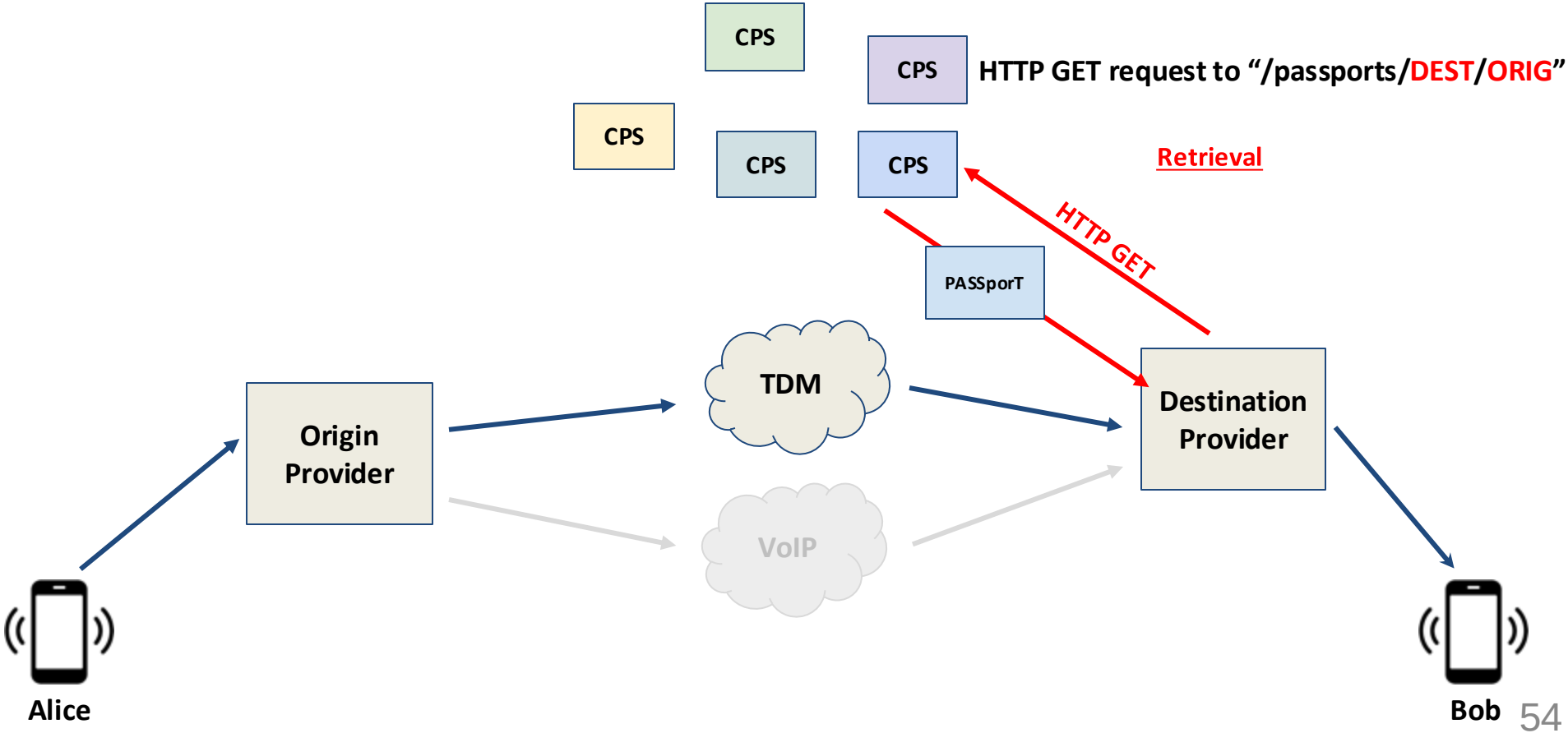
Out-Of-Band *requires* metadata leakage



Out-Of-Band *requires* metadata leakage



Out-Of-Band *requires* metadata leakage



PKI Issues

- No certificate transparency
- Certificate misissuance
- Revocation issues
- Policy administrator is single point of failure for entire PKI

Solutions

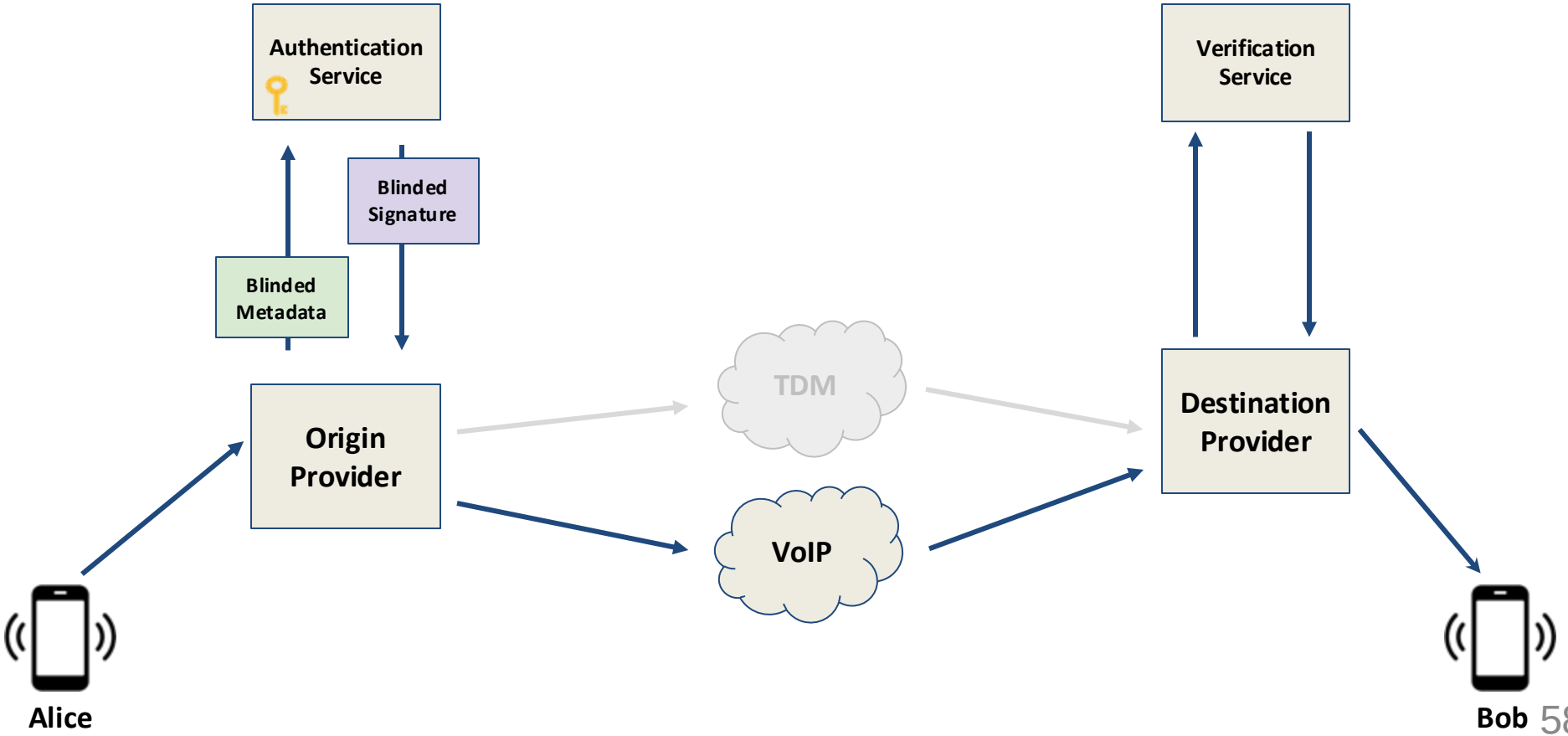
Security + Privacy Goals

- **Metadata Hiding:** Authentication and verification service can't see PASSporT metadata
- **Unlinkability:** Authentication and verification service cannot correlate phone number or provider pairs
- **Deniability:** Origin callers can deny placing a call
- **Reportability:** Ability to report to governance authority
- **Confidentiality:** On-path parties can't see PASSporT contents

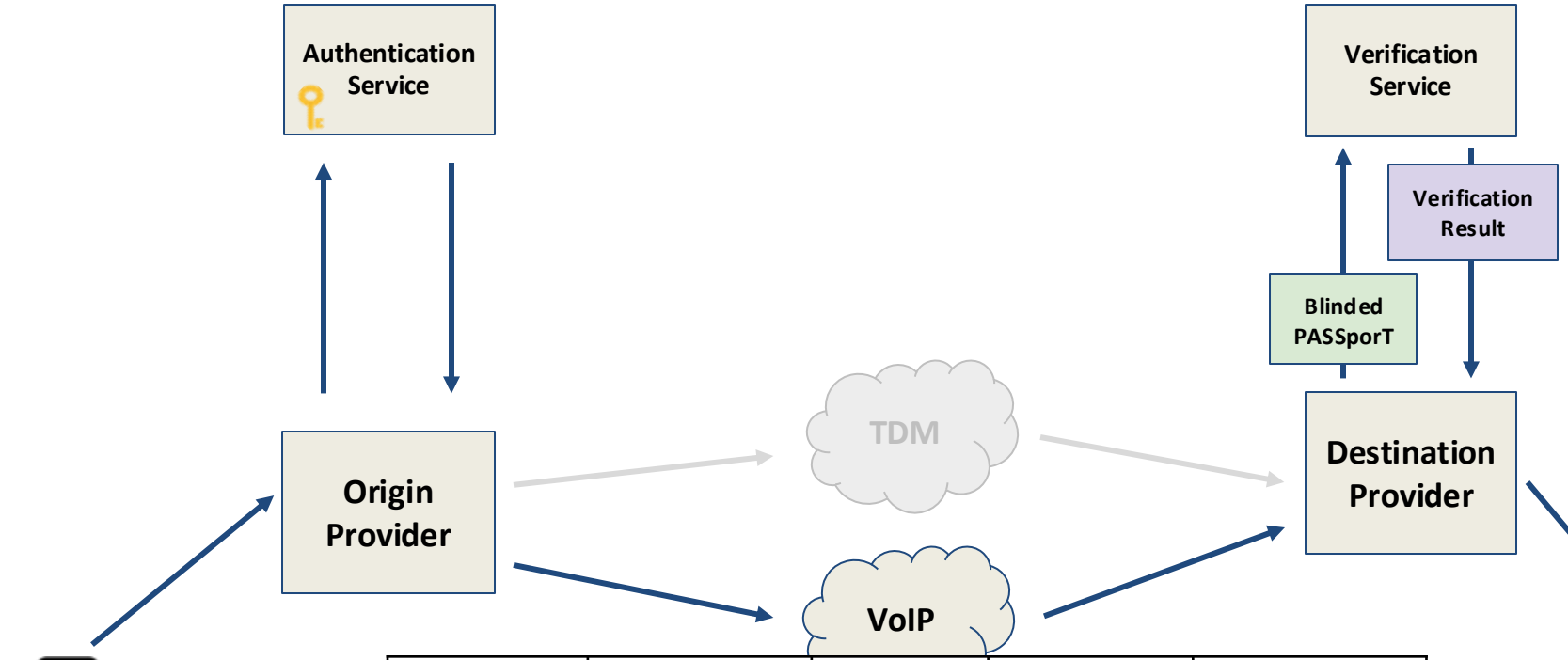
Sign(Hash(metadata || random**)**

Third parties can correlate sign + verify, learn partial information about (to, from) pair

Blind Signing (e.g., RFC 9474)

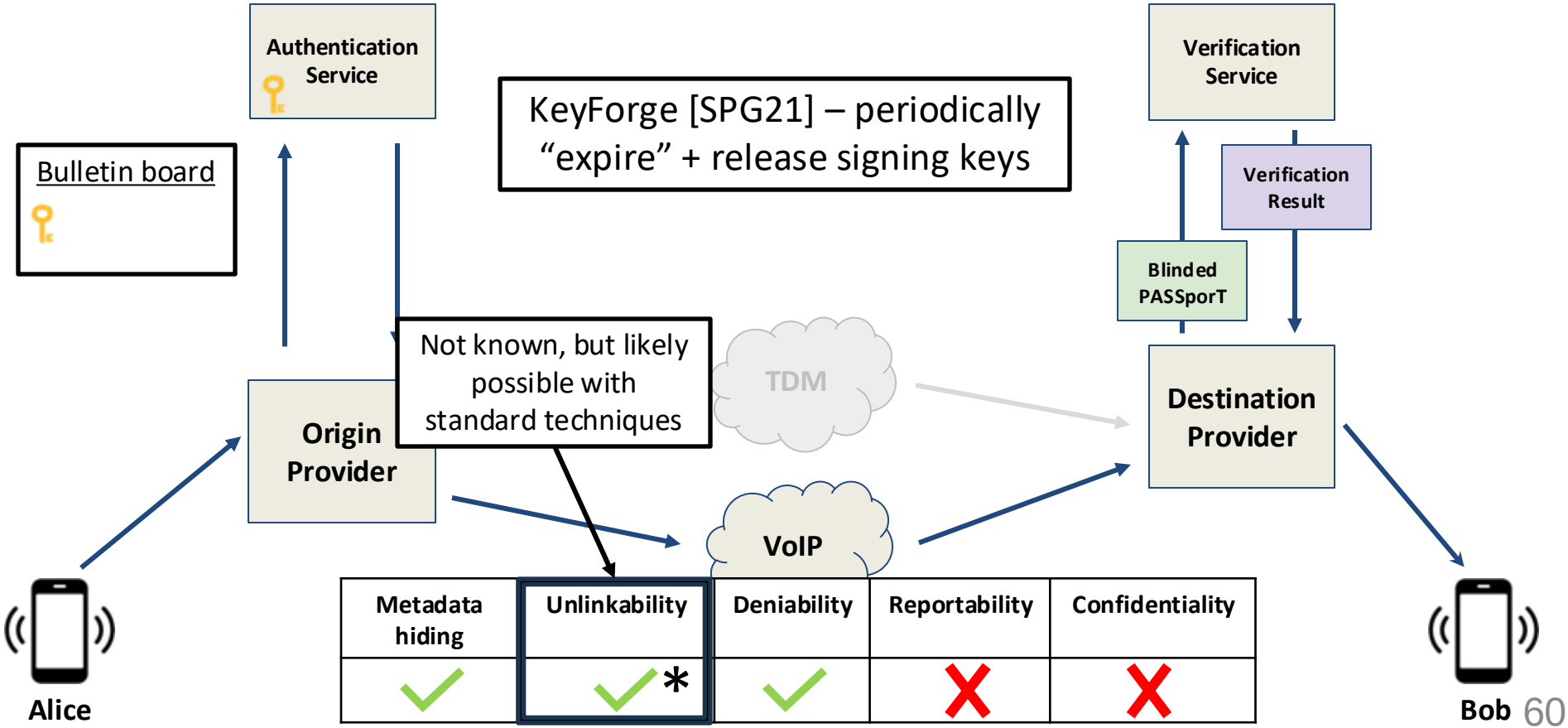


Blind (or in-house) Verification



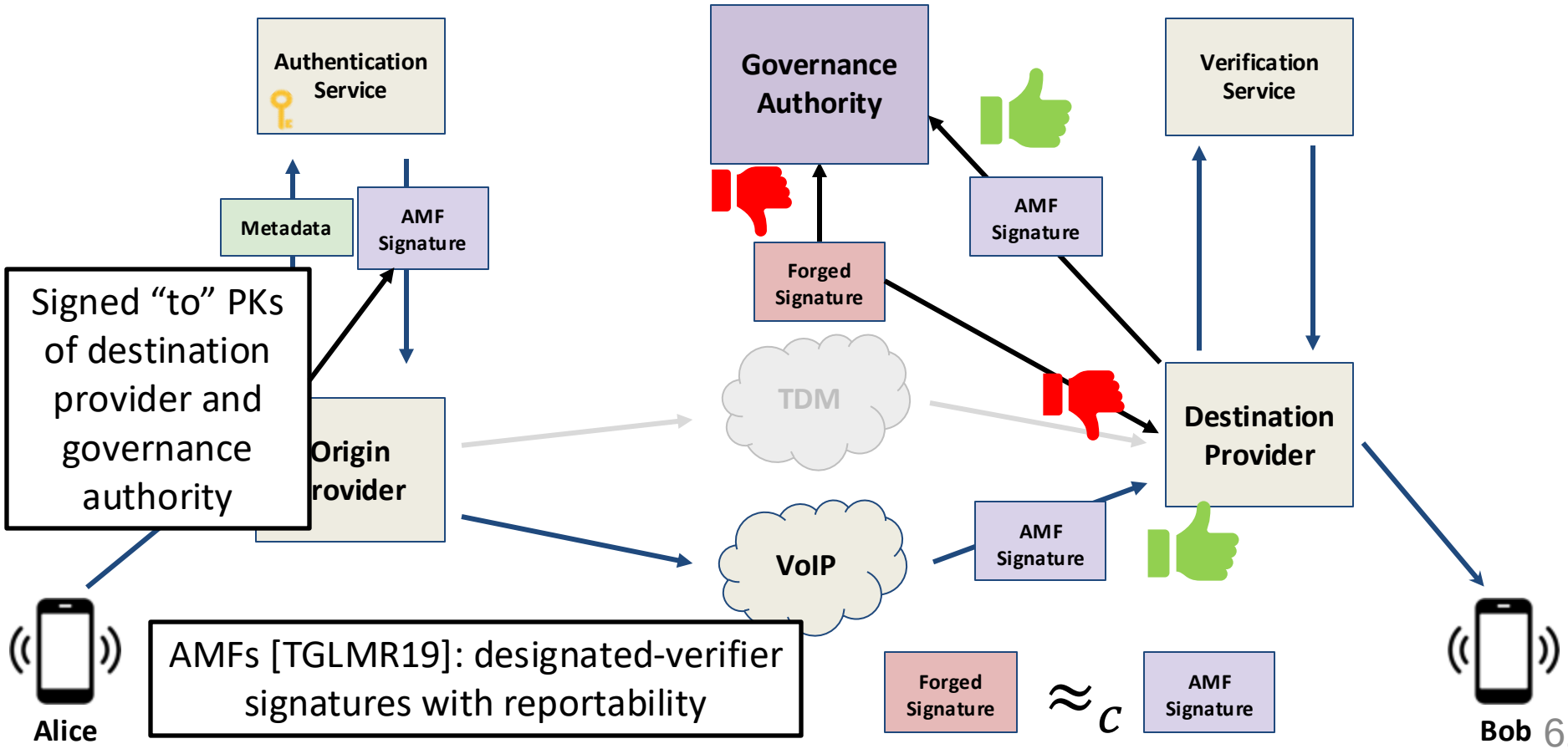
Metadata hiding	Unlinkability	Deniability	Reportability	Confidentiality
✓	✓	✗	✓	✗

Achieving deniability?

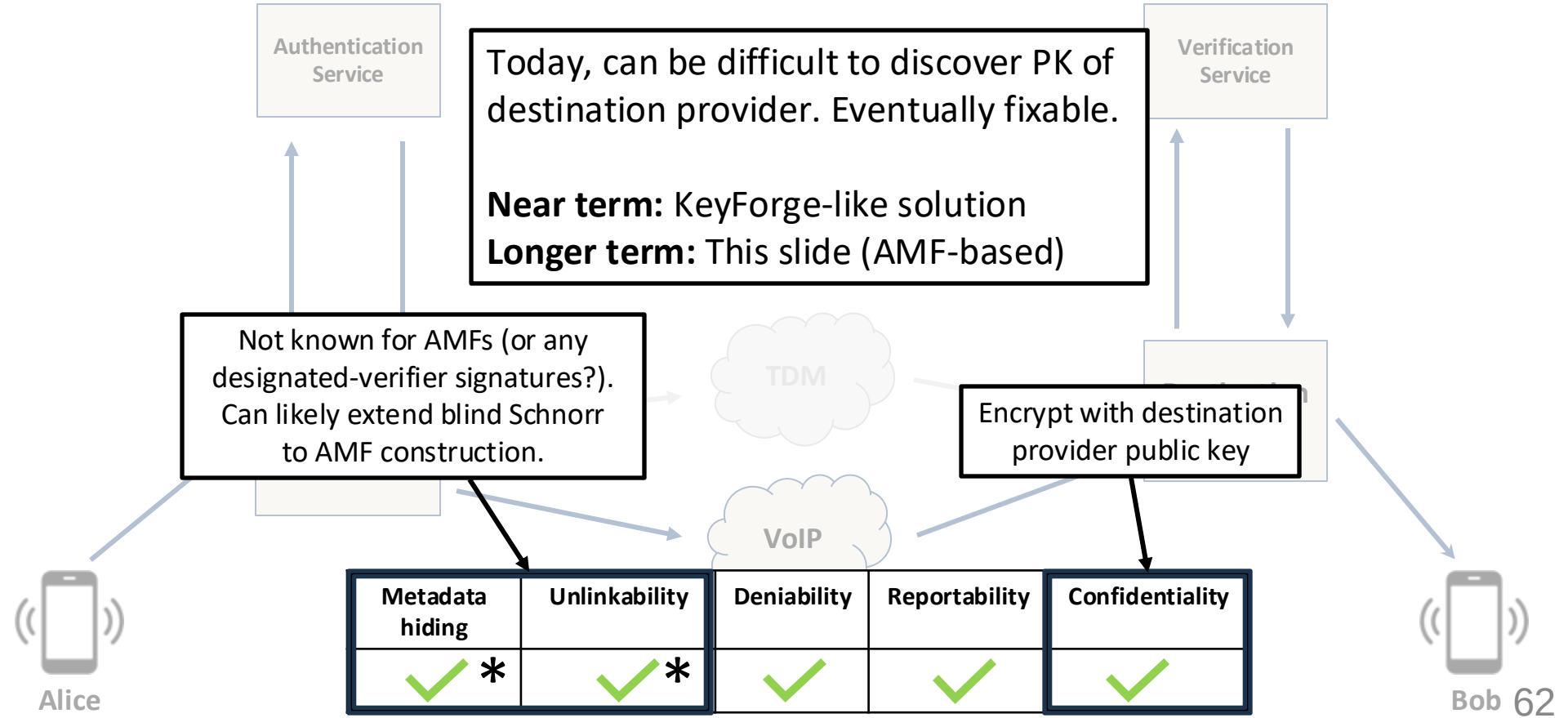


Metadata hiding	Unlinkability	Deniability	Reportability	Confidentiality
✓	✓*	✓	✗	✗

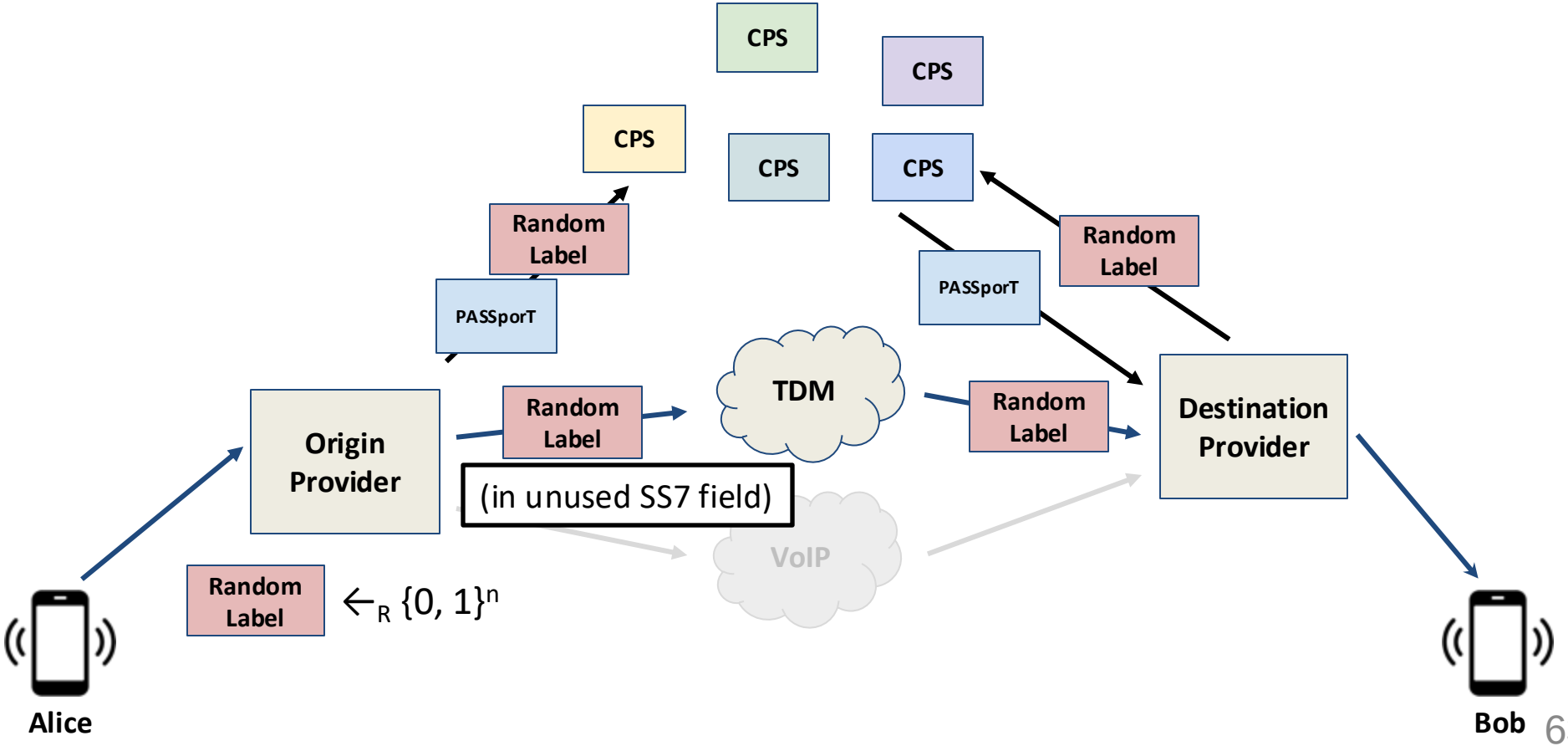
Asymmetric Message Franking (AMFs)



AMFs, blind signing, and encrypted PASSporTs



Improving the Out-of-Band Protocol



Survey Results

Survey Results

"I *hate* STIR/SHAKEN"

- An American Telecom Operator

- 18% of telecoms built their own STIR/SHAKEN implementation
- Over 60% of telecoms say STIR/SHAKEN has been a burden
- Less than 40% believe STIR/SHAKEN has been effective
- ~20% of telecoms have received inquires to route fraudulent traffic
- >80% store metadata after a call has concluded (~20% indefinitely)

N=29, Feb-March 2024

Conclusion

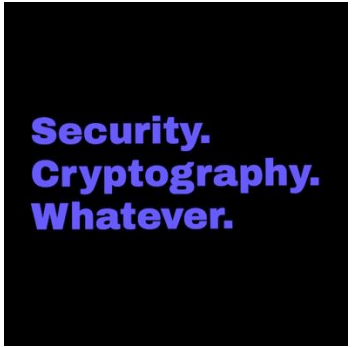
- STIR/SHAKEN is a new protocol in use by ~all telecoms operating in the U.S.
- The STIR/SHAKEN ecosystem has a variety of privacy and security flaws
  - Non-repudiable metadata
  - New metadata leakage
  - Numerous PKI issues
- We are in the process of designing solutions to these issues
  - Blind signing verification
  - Deniable signatures
  - Improved out-of-band protocol

Conclusion

Thanks to:
Matt Hardeman & Ryan Hurst – Martini Security
Yoon-Sung Ji – University of Michigan

Contact:
Josh Brown - jbis@umich.edu
Paul Grubbs - paulgrub@umich.edu

Podcast link



Thanks for listening! Any questions?

Questions