Characterizing the Deployment of the STIR/SHAKEN PKI

Brad Reaves
Associate Professor
Department of Computer Science

Hamim Hamid
PhD Student Researcher
Department of Computer Science

Based on
Hamim Hamid, David Adei, and Bradley Reaves. 2026. Characterizing the Deployment of the STIR/SHAKEN Telephone Network PKI. In Proceedings of the 2026 ACM Internet Measurement Conference (IMC '26), October 12–16, 2026, Karlsruhe, Germany. ACM, New York, NY, USA, 16 pages. https://doi.org/10.1145/3777912.3839819

NC STATE

STIR/SHAKEN deployment timelines had no precedent.

NC STATE

PKIs are ridiculously hard

“Public Key Infrastructure” is a system to link cryptographic information to identity and authorization.

RPKI adoption is 56% after 15 years

HTTPS adoption is 71% after 30 years

Voice providers had 18 months to deploy a national, industry-wide federated PKI.

Any degree of success would be heroic.

... How well did it go?

CRYPTOGRAPHY

Ten Risks of PKI: What You’re not Being Told about Public Key Infrastructure

By Carl Ellison and Bruce Schneier

Computer security has been victim of the “year of the...” syndrome. First it was firewalls, then intrusion detection systems, then VPNs, and now certification authorities (CAs) and public-key infrastructure (PKI). “If you only buy X,” the sales pitch goes, “then you will be secure.” But reality is never that simple, and that is especially true with PKI.

Certificates provide an attractive business model. They cost almost nothing to make, and if you can convince someone to buy a certificate each year for $5, that times the population of the Internet is a big yearly income. If you can convince someone to purchase a private CA and pay you afee for every certificate he issues, you’re also in good shape. It’s no wonder so many companies are trying to cash in on this potential market.With that much money at stake, it is also no wonder that almost all the literature and lobbying on the subject is produced by PKI vendors. And this literature leaves some pretty basic questions unanswered: What good are certificates anyway? Are they secure? For what? In this essay, we hope to explore some of those questions.

Security is a chain; it’s only as strong as the weakest link. The security of any CA-based system is based on many links and they’re not all cryptographic. People are involved.

Does the system aid those people, confuse them or just ignore them? Does it rely inappropriately on the honesty or thoroughness of people? Computer systems are involved. Are those systems secure? These all work together in an overall process. Is the process designed to maximize security or just profit?

Each of these questions can indicate security risks that need to be addressed.

Before we start: “Do we even need a PKI for e-commerce?”

Open any article on PKI in the popular or technical press and you’re likely to find the statement that a PKI is desperately needed for e-commerce to flourish. This statement is patently false. E-commerce is already flourishing, and there is no such PKI. Web sites are happy to take your order, whether or not you have a certificate. Still, as with many other false statements, there is a related true statement: commercial PKI desperately needs e-commerce in order to flourish. In other words, PKI startups need the claim of being essential to e-commerce in order to get investors.

There are risks in believing this popular falsehood. The immediate risk is on the part of investors. The security risks are borne by anyone who decides to actually use the product of a commercial PKI.

Risk #1: “Who do we trust, and for what?”

There’s a risk from an imprecise use of the word “trust.” A CA is often defined as “trusted.”

In the cryptographic literature, this only means that it handles its own private keys well. This doesn’t mean you can necessarily trust a certificate from that CA for a particular purpose: making a micropayment or signing a million-dollar purchase order.

Who gave the CA the authority to grant such authorizations? Who made it trusted?

A CA can do a superb job of writing a detailed Certificate Practice Statement, or CPS — all the ones we’ve read disclaim all liability and any meaning to the certificate — and then do a great job following that CPS, but that doesn’t mean you can trust a certificate for your application. Many CAs sidestep the question of having no authority to delegate authorizations by

Computer Security Journal • Volume XVI, Number 1, 2000 1

NC STATE

In this talk

We'll take a deep dive into deployment rates and specification conformance

Our full paper is available at https://robocall.science

So is our implementation correctness checklist, our validation/verification code, and our certificate dataset.

Our analysis is exhaustive and detail-oriented

When it comes to security, small details matter!

We'll end with non-trivial lessons for future efforts

Characterizing the Deployment of the STIR/SHAKEN Telephone Network PKI

Hamim Hamid
NC State University
Raleigh, USA
hhamid@ncsu.edu

David Adei
NC State University
Raleigh, USA
dahmed@ncsu.edu

Bradley Reaves
NC State University
Raleigh, USA
bgreaves@ncsu.edu

Abstract

In response to an epidemic of unlawful unsolicited telephone calls, the United States mandated the use of a novel, previously unimplemented call attestation framework called STIR/SHAKEN (S/S) in 2019. The mandate required telephone network operators to deploy a new, federated, industry-wide PKI in timelines shorter than *2 years* for large providers. Under those circumstances, achieving any degree of successful deployment would be remarkable.

In this paper, we present a longitudinal study of S/S deployment, evaluating standards compliance, certificate authority practices, and provider call signatures and metadata. Our primary data source is signaling data from 7.75 million calls collected by multiple telephone honeypots over four years (November 2021–February 2026). Our results show rapid adoption of S/S, but with pervasive non-compliance with standards.

We also found repeated instances of problematic practices, including providers misreferencing the keys used to sign calls and originating calls with pre-signed attestations from unrelated calls. Despite these lapses, we find that most calls are correctly signed and that certificate authority and operator practices and standards compliance are improving at a modest pace. Our discussions highlight concrete directions to strengthen policy and deployment, enabling more effective mitigation of telephone network abuse.

CCS Concepts

• **Security and privacy → Security protocols**.

Keywords

STIR/SHAKEN, telephone networks, public key infrastructure, call authentication, network measurement

ACM Reference Format:

Hamim Hamid, David Adei, and Bradley Reaves. 2026. Characterizing the Deployment of the STIR/SHAKEN Telephone Network PKI. In *Proceedings of the 2026 ACM Internet Measurement Conference (IMC '26), October 12–16, 2026, Karlsruhe, Germany.* ACM, New York, NY, USA, 16 pages. https://doi.org/10.1145/3777912.3839819

1 Introduction

Telephone networks are a critical global infrastructure that connect 5.8B people worldwide and underpin modern society. However, this network is persistently abused by unsolicited calls that facilitate a wide range of harmful activities [19, 49, 59, 60]. Billions of dollars in annual losses from the US and worldwide are routinely estimated [22, 72].

The near-universal hatred of ubiquitous unsolicited calls in the US has made stopping them a goal of both major political parties and a cornerstone of every presidential communications agenda since the Obama administration. In the 2010s, it was widely believed that the reason it was difficult to stop or prosecute was widespread caller ID spoofing, so preventing such spoofing became the aim of research and commercial solutions [44, 53, 62, 63, 73]. This thinking led to the bipartisan passage of the TRACED Act in the US in 2019.

As directed by the TRACED Act, the Federal Communications Commission (FCC) mandated the implementation of STIR/SHAKEN (S/S) for all telecommunications voice operators by June 2021 [24]. S/S provides technical standards [11, 35] that enable originating service providers (OSPs) to assign an *attestation* reflecting their knowledge and confidence in the caller identity for each call [8]. S/S also defines mechanisms for OSPs to cryptographically sign this information, along with other signaling data, allowing terminating service providers (TSPs) to verify it. This process relies on an industry-wide public key infrastructure (PKI) for secure signature generation and verification.

Prior studies show that PKIs have historically been difficult to deploy at scale across Internet protocols, IoT systems, CDNs, and other environments [16, 17, 21, 41, 46, 47, 64, 69, 75, 77, 82]. On top of that, the U.S. telephone ecosystem was mandated to deploy S/S within an aggressive ~2-year timeline (2019–2021 for large providers), requiring rapid, industry-wide coordination and substantial resource investment. Initial FCC estimates [25] placed carrier implementation costs between $15,000 and $300,000, but subsequent industry reports and practitioner accounts indicate significantly higher deployment and maintenance costs. These constraints raise a central question: *how effectively does S/S function as a real-world PKI for telephony?*

To answer this question, we conducted a longitudinal measurement of S/S deployment, focusing on its PKI ecosystem. We demonstrate rapid adoption of S/S, but with pervasive formatting inconsistencies. We also found instances of concerning practices by certificate authorities and providers. Our independent S/S verification results differ significantly from those reported by providers, which we detail in this paper. We further characterized the behavior of key participants. Critically, our findings reveal policy gaps that can render S/S ineffective despite observed improvements in compliance over time. Overall, we make the following contributions:

(1) A strict, exhaustive validation library for S/S certificates and attestations that aims to cover every requirement from

IMC '26, Karlsruhe, Germany

ACM ISBN 979-8-4007-2327-8/2026/10
https://doi.org/10.1145/3777912.3839819

NC STATE

Details Matter

The Fundamental Theorem of Software Security*

"**All** exploitable software vulnerabilities originate in a failure to validate input"

Proof: Attackers only control inputs; successful attacks depend on an attacker's input. QED.

You cannot validate non-compliant data correctly.

To accept non-compliant data, you must either:

Proactively ignore fields you should be checking.

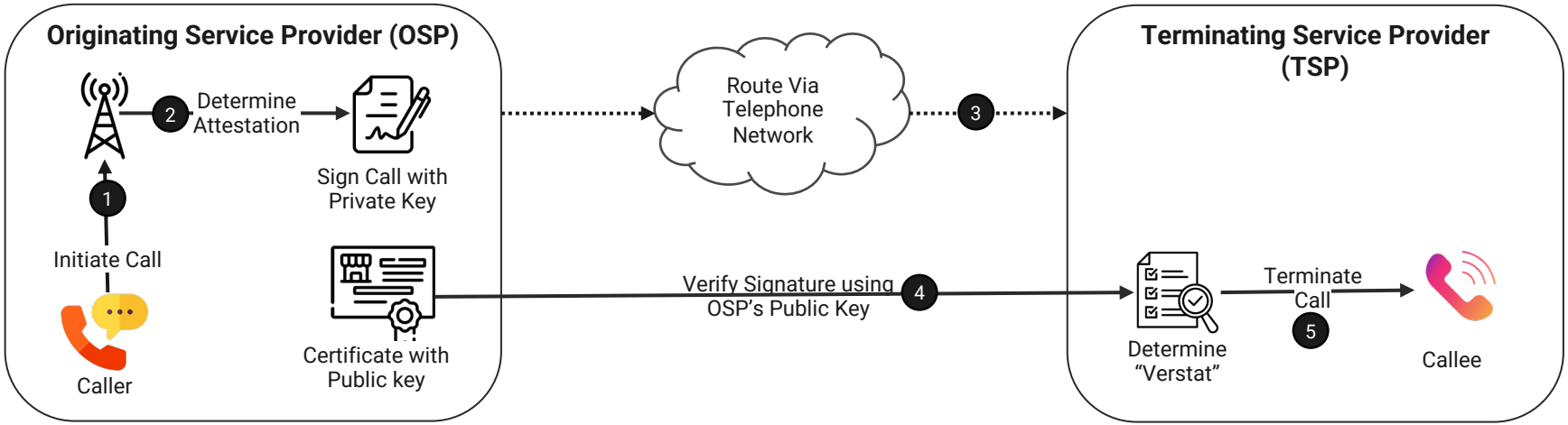
Reactively add exceptions to your implementation.

Unclear or unspecified details mean OSPs can't know how a TSP will assess a call

Every deviation from the spec creates work or problems for others.

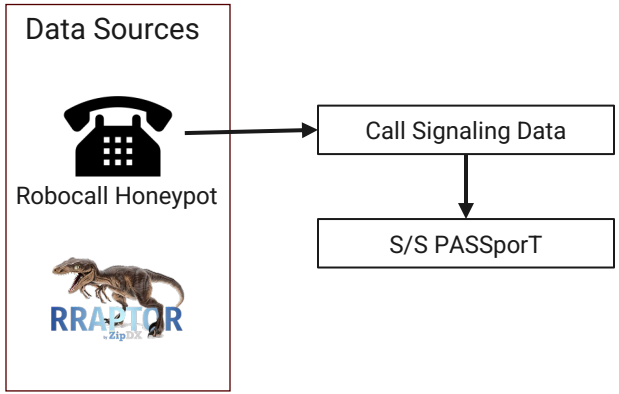
*The name is my terminology. Others developed the big idea.

STIR/SHAKEN Workflow



NC STATE

Our Method



7.75 M calls (Nov'21 – Feb'26)

```
[Feb 21 23:20:37] VERBOSE[61] <--- Received SIP request (1504 bytes
      ↪ ) from UDP:256.231.8.75:5060 --->
INVITE sip:+12025552317@honeypot.example:5060 SIP/2.0
Via: SIP/2.0/UDP 256.231.8.75:5060;branch=
      ↪ z9hG4bK0cB5b4924167846b76f
From: <sip:+12025558484@256.231.8.75>;tag=gK0c656b77
To: <sip:+12025552317@honeypot.example>
Call-ID: 19663844.127903956@256.231.8.75
PAID: <sip:+12025558484;verstat=No-TN-Validation@256.231.8.75:5060>
Attestation: C
Identity: eyJhbGciOiJFUzI1NiIsInBwdCI6InNoYWtlbiIsInR5c...J0In;<
      ↪ https://certificates.exampletel.com/shaken.crt>;alg=ES256;
      ↪ ppt=shaken
Content-Length: 280
Content-Disposition: session; handling=required
Content-Type: application/sdp
```

SIP INVITE EXAMPLE

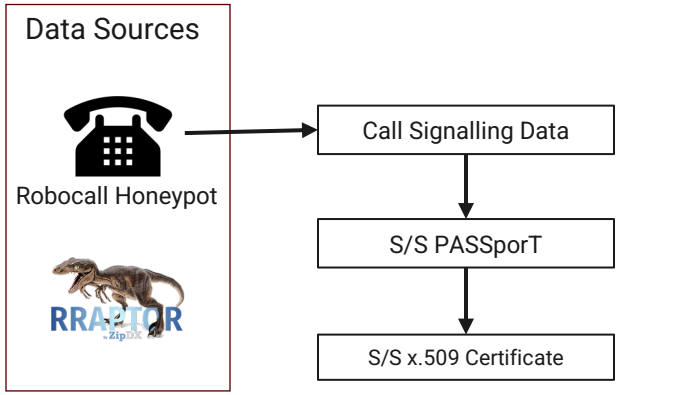
```
{ "header": {
        "alg": "ES256",
        "ppt": "shaken",
        "typ": "passport",
        "x5u": "https://certificates.exampletel.com/shaken.crt"
  "payload": {
        "attest": "C",
        "orig": { "tn": "12025558484" },
        "dest": {  "tn": ["12025552317"] },
        "iat": 1705934984,
        "origid": "7513ba85-cb60-43c3-ac06-22f47e3372bf"
  },
  "signature": "<ES256 digital signature (base64url-encoded)>"
```

S/S PASSporT Example

"S/S "and "STIR/SHAKEN" are used interchangeably from this slide

NC STATE

Our Method



7.75 M calls (Nov'21 – Feb'26)


```
{ "header": {
        "alg": "ES256",
        "ppt": "shaken",
        "typ": "passport",
        "x5u": "https://certificates.exampletel.com/shaken.crt"
  "payload": {
        "attest": "C",
```

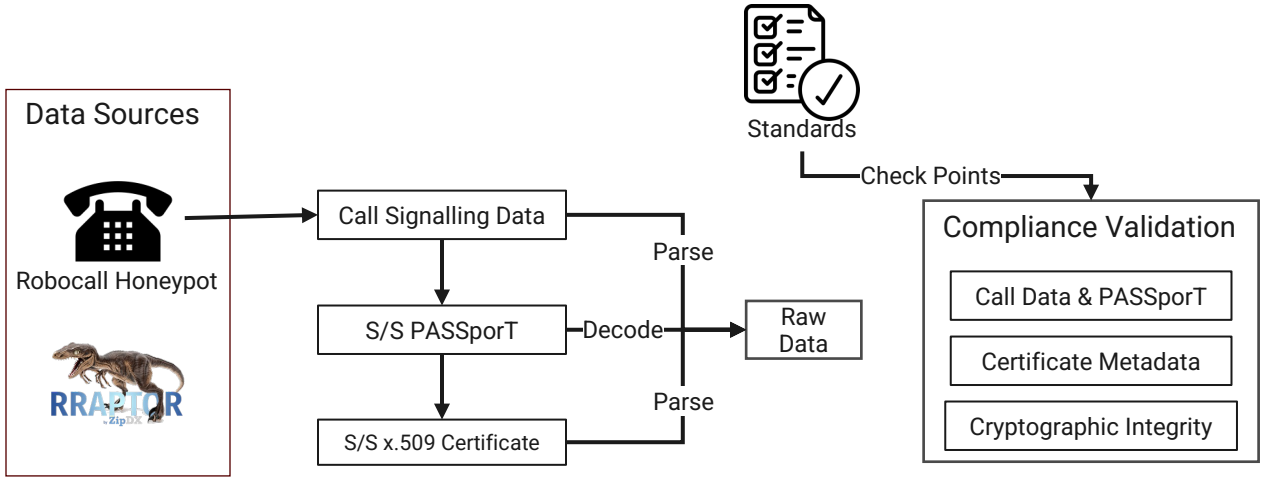


```
Certificate:
    Data:
        Version: 3 (0x2)
        Serial Number:
            7e:56:67:b3:27:fe:a0:11:f8:30:95:bc:98:df:a9:03:15:85:68:d3
        Signature Algorithm: ecdsa-with-SHA256
        Issuer: C = US, ST = WA, L = Seattle, O = "Martini Security, LLC", CN = Martini Security SHAKEN G3
        Validity
            Not Before: Feb 17 12:00:28 2025 GMT
            Not After : Mar 21 19:51:29 2025 GMT
        Subject: CN = SHAKEN 738J, serialNumber = 5F992B7D7EFE340BAB5356139BF0F7A2, C = US, O = "BCM One Cloud Communications, LLC"
        Subject Public Key Info:
            Public Key Algorithm: id-ecPublicKey
                Public-Key: (256 bit)
                pub:
                    04:2a:2e:7e:a6:6f:e0:6d:7c:29:8a:da:db:d1:4c:
                    23:80:42:ed:4f:5d:65:c4:aa:ca:d2:f5:4a:b1:ab:
                    c1:01:f0:dc:5f:58:16:ce:5b:73:d4:8d:57:78:26:
                    f7:44:5b:97:82:4f:75:5a:d3:9b:12:b1:d8:2c:ed:
                    21:fa:ae:ed:6c
                ASN1 OID: prime256v1
                NIST CURVE: P-256
        X509v3 extensions:
            X509v3 Key Usage: critical
                Digital Signature
            X509v3 Basic Constraints: critical
                CA:FALSE
            X509v3 Subject Key Identifier:
                5E:E3:EC:23:D1:C9:C2:3A:7B:A1:2A:81:A0:85:DB:06:73:FF:5C:3D
            X509v3 Authority Key Identifier:
                2E:5A:41:53:26:E2:70:AA:6C:01:C0:E6:76:F0:EE:22:F7:33:0F:1C
            X509v3 CRL Distribution Points:
                Full Name:
                  URI:https://authenticate-api.iconectiv.com/download/v1/crl                CRL Issuer:
                  DirName:L = Bridgewater, ST = NJ, CN = STI-PA CRL, C = US, O = STI-PA
            1.3.6.1.5.5.7.1.26:
                0.....738J
            X509v3 Certificate Policies:
                Policy: 2.16.840.1.114569.1.1.4
    Signature Algorithm: ecdsa-with-SHA256
    Signature Value:
        30:45:02:21:00:aa:8a:2c:c6:c3:2c:cb:79:14:d0:4e:24:24:
        aa:dd:c2:22:80:73:05:12:38:98:ac:1b:e5:0b:43:16:7d:97:
        a1:02:20:60:5a:cd:e8:a2:2b:59:ba:1c:b5:a1:94:b9:90:58:
        88:9e:a3:5a:71:df:e7:5f:0b:b6:86:6b:a3:e4:63:d2:0c
```


x.509 Certificate Example

NC STATE

Our Method



7.75 M calls (Nov'21 – Feb'26)

NC STATE

Our Verification Rules

CP	Category	Validation Check	Reference
1	PASSporT	The originating number in the JWT matches the SIP P-Asserted-Identity (PAID).	ATIS-100074
2	PASSporT	When PAID is absent, the JWT originating number matches the SIP From number.	ATIS-100074
3	PASSporT	The SIP PAID and SIP From numbers are consistent with each other.	ATIS-100074
4	PASSporT	The called number in SIP follows valid E.164 formatting.	ATIS-100074
5	PASSporT	The destination number in the JWT matches the SIP called number.	ATIS-100074
6	PASSporT	The certificate URL (`x5u`) in the SIP header matches the URL in the JWT header.	ATIS-100074
7	PASSporT	The `x5u` URL uses HTTPS and a secure port (e.g., 443 or 8443).	ATIS-100074
8	PASSporT	The `x5u` URL does not contain insecure components, such as query strings or fragments.	ATIS-100074
9	PASSporT	The `x5u` URL does not rely on HTTP redirection.	ATIS-100074
10	PASSporT	The JWT signing algorithm is consistent with the certificate's signature algorithm.	RFC 8224
11	PASSporT	The JWT `ppt` field is set to `shaken`.	ATIS-100074
12	PASSporT	The JWT `typ` field is set to `passport`.	RFC 8224
13	PASSporT	The attestation level in SIP matches the attestation value in the JWT.	ATIS-100074
14	PASSporT	The destination type in the JWT is specified as a telephone number (`tn`).	ATIS-100074
15	PASSporT	The JWT issuance time is within an acceptable window (e.g., within five minutes of the call).	ATIS-100074

Table 1: PASSporT and call-data compliance checks implemented in Module 1.

CP	Category	Validation Check	Reference
35	Cryptographic	The public key lies on the expected elliptic curve and satisfies the curve equation.	RFC 7518
36	Cryptographic	The digital signature is correctly decoded from DER format into (r, s) components.	RFC 7518
37	Cryptographic	The signature values (r, s) fall within the valid cryptographic range.	RFC 7518
38	Cryptographic	The signature satisfies low-s normalization requirements.	RFC 7518
39	Cryptographic	Reuse of signature randomness (e.g., identical r-values) is detected.	RFC 7518
40	Cryptographic	Signature randomness exhibits the expected statistical properties, with no detected bias or clustering.	RFC 7518
41	Cryptographic	The final verification outcome is consistent with the attestation level and validation results.	ATIS-100074
42	Cryptographic	The certificate chain is successfully validated against trusted authorities.	ATIS-100074
43	Cryptographic	The PASSporT signature is successfully verified using the public key.	ATIS-100074

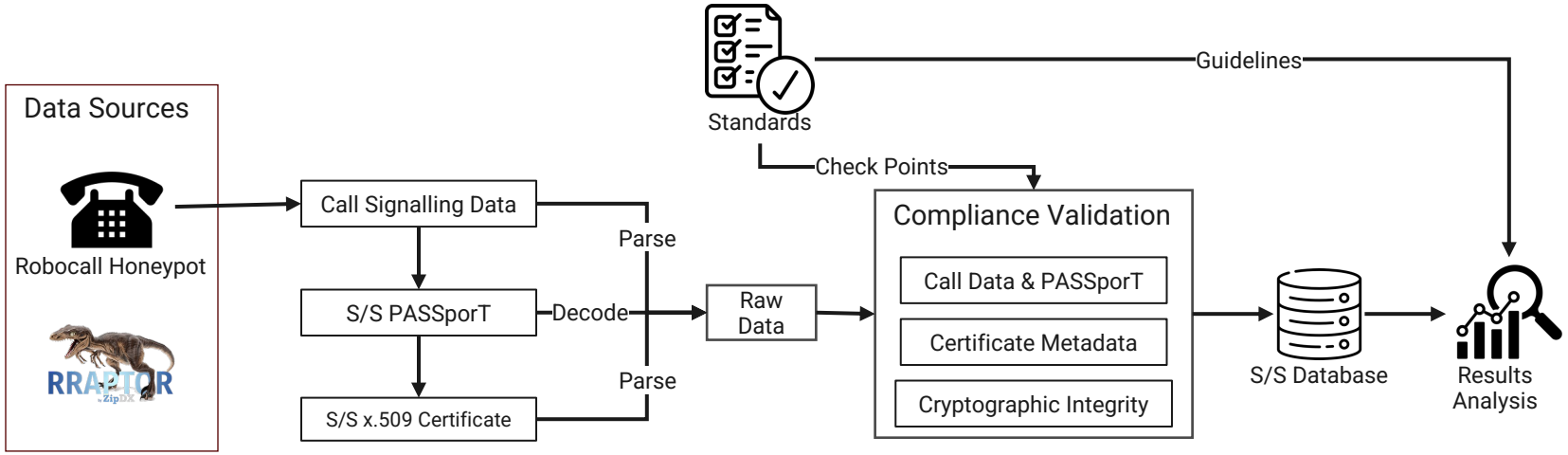
Table 3: Cryptographic integrity checks implemented in Module 3.

CP	Category	Validation Check	Reference
16	Certificate	The certificate version is X.509 v3.	ATIS-100080
17	Certificate	The certificate serial number is unique within the issuing authority.	ATIS-100080
18	Certificate	The signature algorithm uses an approved ECDSA variant (e.g., SHA-256 or SHA-384).	ATIS-100080
19	Certificate	The subject common name follows the format `SHAKEN <SPC>`.	ATIS-100080
20	Certificate	The Service Provider Code (SPC) in the subject common name matches the value in the TNAuthList extension.	ATIS-100080
21	Certificate	The certificate is valid at the time of the call (i.e., the call occurs after `notBefore`).	ATIS-100080
22	Certificate	The certificate is not expired at the time of the call (i.e., the call occurs before `notAfter`).	ATIS-100080
23	Certificate	The public-key algorithm is Elliptic Curve (EC).	ATIS-100080
24	Certificate	The public-key size corresponds to an approved curve (e.g., 256 or 384 bits).	ATIS-100080
25	Certificate	The public-key structure is valid and correctly encoded.	ATIS-100080
26	Certificate	The certificate uses a valid NIST elliptic curve (P-256 or P-384).	ATIS-100080
27	Certificate	The Subject Key Identifier (SKI) is derived from the public-key hash.	RFC 5280; ATIS-100080
28	Certificate	The Authority Key Identifier (AKI) matches the issuer's key identifier.	ATIS-100080
29	Certificate	The Key Usage extension is marked as critical.	ATIS-100080
30	Certificate	The Key Usage value is appropriate: `digitalSignature` for an end-entity certificate or `keyCertSign` for a CA certificate.	ATIS-100080
31	Certificate	The Basic Constraints extension is present and marked as critical.	ATIS-100080
32	Certificate	The Basic Constraints extension correctly specifies the CA status (`TRUE` for a CA certificate and `FALSE` for an end-entity certificate).	ATIS-100080
33	Certificate	The CRL Distribution Point is correctly specified for revocation checking.	ATIS-100080
34	Certificate	The TNAuthList extension contains one valid SPC and no telephone numbers.	ATIS-100080

Table 2: Certificate structural compliance checks implemented in Module 2.

NC STATE

Our Method



7.75 M calls (Nov'21 – Feb'26)

Verstat	Attestation	Call Data & PASSporT	Certificate Metadata	Cryptographic Integrity
TN-Validation-Passed	A	✓	✓	✓
No-TN-Validation	B or C	✓	✓	✓
No-TN-Validation	Any	✗	✓	✓
TN-Validation-Failed	Any	N/A	At least 1 ✗	

NC STATE

Caveat

Our findings reflect unsolicited calls reaching our honeypot vantage points and may not generalize to the broader telephone ecosystem.

NC STATE

STIR/SHAKEN Deployment

As observed through our robocall honeypots

NC STATE

Big Picture

The Good

88% of calls arrive with a passport

Passport arrival is increasing over time

Cryptographic errors are rare

Malicious S/S call attempts are rare

Overall errors are decreasing over time

The Bad

~60% of calls have at least one standard compliance issue

~48% of certificates have at least one standard compliance issue

NC STATE

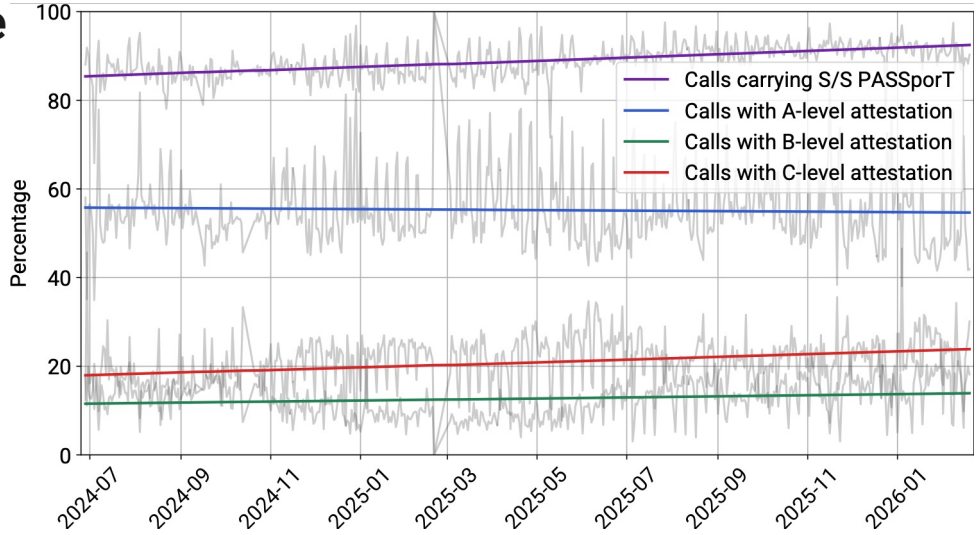
STIR/SHAKEN Presence Is Steadily Increasing

Incoming Calls with S/S Signature

86% → **91%**

Originating Providers with S/S signature Calls

220 → **613**



NC STATE

STIR/SHAKEN Presence Is Steadily Increasing

11.9%

Incoming Calls Without PASSporT

➡

89.5K

Unique Calling Numbers without PASSporT

➡

29.5K

Unique Calling Numbers reappeared with PASSporT

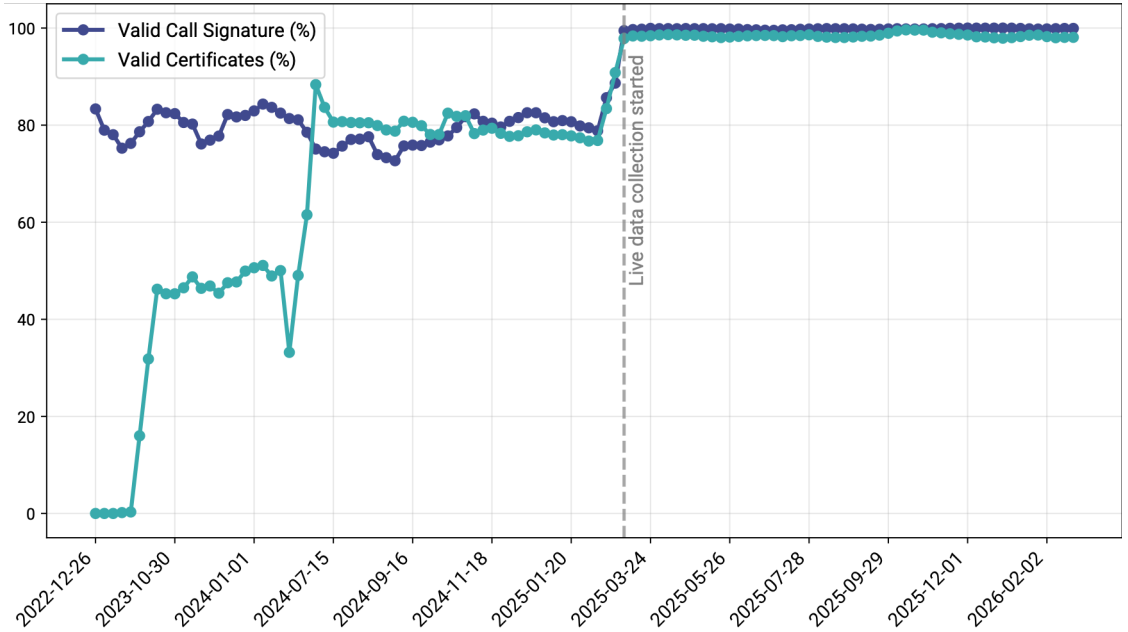
May reflect legacy incompatibility, unsupported call paths, provider variance, or unintentional stripping during call routing

NC STATE

Validation Is Time-sensitive

Certificate download failure
0.1% calls at call-time
13% calls retrospectively

Cryptographic Certificate Verification Failures
~0% calls in call-time
28% calls retrospectively

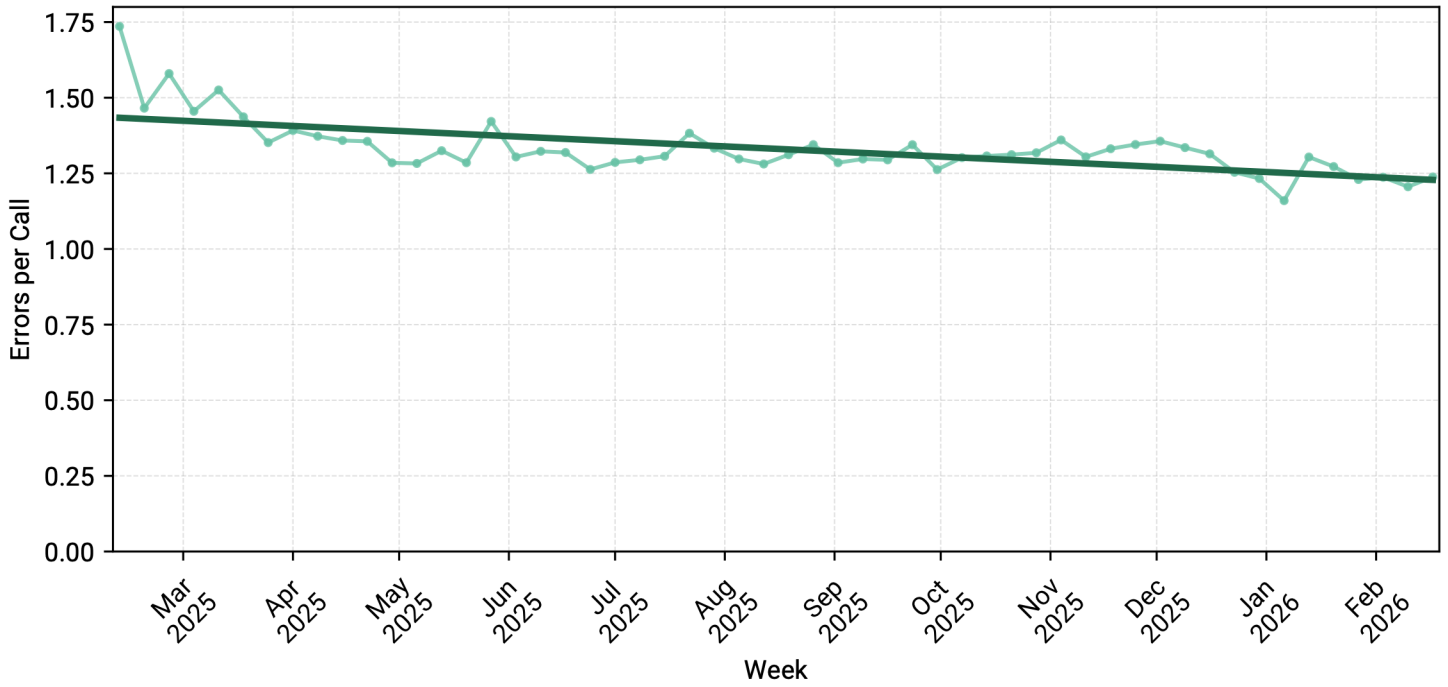


No certificate archival: rotated or withdrawn certs make old calls unverifiable.

Fix: A CT-style log or PA archive

NC STATE

Measurable Improvement Throughout Ecosystem



Errors per call fell from 1.6 → 1.2 over the last year

NC STATE

Originating Provider Practices

Signing is highly concentrated

15 (1%) of providers signed 50.6% calls, 72 (5%) of providers signed 79.5% calls.

Certificate Authority Practices

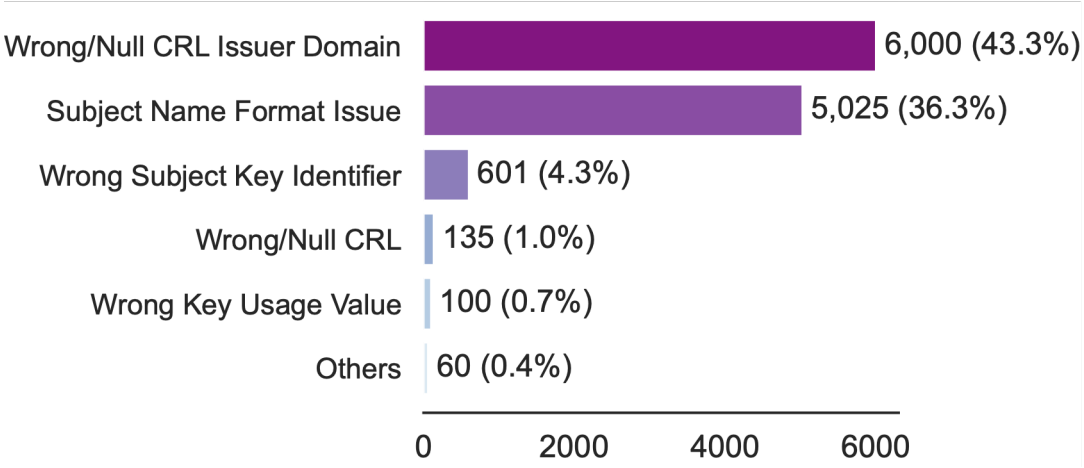
13,861 total certificates

48% violate ≥1 guideline

90% fail format conformance

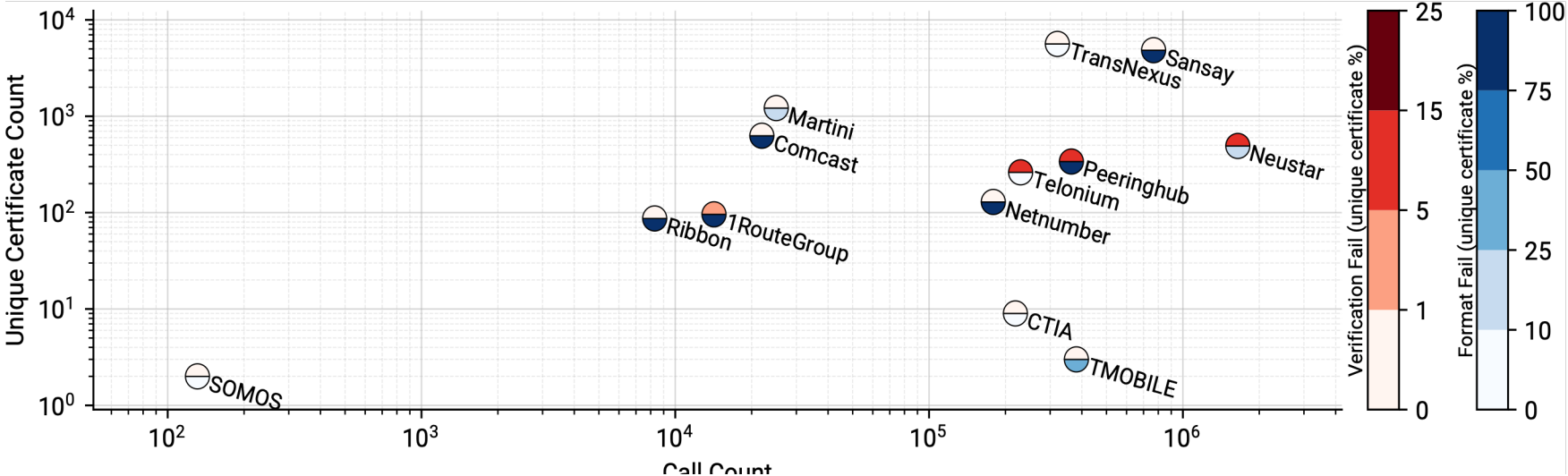
3% fail cryptographic validation

6.4% fail cryptographic AND format validation



NC STATE

Certificate Authority Practices



Business models vary wildly in business models and priorities

Full compliance is achievable

Unregistered CAs appeared in the wild

NC STATE

Responsible Disclosures

Provider/CA feedback helped us identify alternative explanations, conduct follow-up experiments, and refine several findings:

Telonium: 3,747 calls used valid leaf certificates, but their certificate URIs incorrectly pointed to the Telonium root certificate.

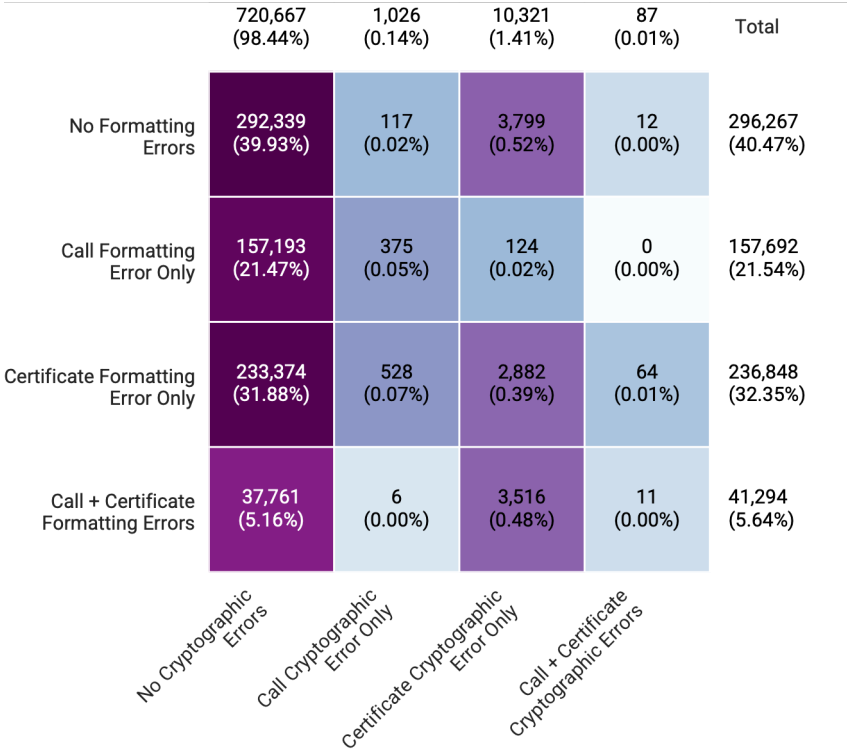
Can Independent Implementers agree?

~60% of calls violate ≥ 1 specification in our validation implementation

72% of calls have different verstats from us and a provider

Current validation guidelines permit multiple interpretations

- Validation guidelines are non-exhaustive
- Specific cases scattered across documents
- Standard explicitly defers critical validation decisions to providers on several points.



NC STATE

But Wait, there's More!

High-level STIR/SHAKEN primer for non-telco folks

Detailed Attestation Level Analyses

International STIR/SHAKEN Calls

CA business model variance

Certificate cryptography and validity times

…

NC STATE

Lessons from Hindsight

Some CA's issue lots of certificates with few or no compliance issues

Compliance is possible!

GAs could monitor and ensure CAs issue compliant certificates

Either at initial onboarding or as a condition for CA renewal

Certificate transparency would create a useful archive for retrospective validation

We like the ALIII certificate transparency proposal!

Current protocols say what senders SHALL/MUST do.
Future protocols should also say what receivers SHALL/MUST reject.

Future protocols should consider a channel for validation feedback

NC STATE

Brad Reaves
https://bradreaves.net

Hamim Hamid
hhamid@ncsu.edu

Questions?

Thanks to:

SIPNOC for the invitation
Bandwidth, Comcast, PeeringHub, Telonium, & T-Mobile for prompt responses to our queries
Bandwidth and RRaptor for in-kind support
National Science Foundation

Paper, code, and data at https://robocalls.science

NC STATE