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 noncompliance 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

the standards. We will release this to the community before publication.
(2) Longitudinal analysis of S/S development based on a dataset of over 7.7M calls between November 2021 to February 2026. We show that over 91% of calls are now signed and observe a positive trend in key health measurements: call attestation prevalence, provider adoption, and error rates.
(3) We thoroughly detail certificate, call data, and call verification standards compliance. We find 53.7% of calls violate at least one specification requirement.
(4) We characterize the nascent certificate authority ecosystem, showing a massive variety of business models and operating practices, as well as non-trivial deviations from best practices.
(5) We examine provider practices, finding that cryptographic errors and bogus attestations do occur, but rarely. On the other hand, the S/S ecosystem features to identify abusive callers and the responsible service providers are unreliable.

This paper measures the deployment of an industry-wide cryptographic system. The reader is probably asking if that system was effective. There is wide belief among industry, academics, regulators, and ourselves that STIR/SHAKEN has likely dramatically reduced or eliminated caller ID spoofing, attaining its stated goal, though pure ground truth on this question is elusive. What is certain, though, is that S/S has made virtually no impact on unsolicited call volumes. Prasad et al., working from a dataset ending in 2024 [61], reported modest declines in robocall volume, but more recent industry reports showed a near-total reversal in that trend almost immediately after Prasad et al. stopped data collection.

This result does not mean that S/S is effectively worthless. In fact, it now serves as the foundation for several initiatives that provide positive authentication for caller ID while motivating a renewed push to decommission legacy non-IP infrastructure. Learning key lessons from its rollout and improving its availability and reliability are key to future improvements in telephone networks and other PKI systems.

2 Background and Related Work

The Public Switched Telephone Network (PSTN) is a global internetwork of autonomous networks capable of supporting synchronous voice communication between any two or more devices assigned a telephone number (TN). Many provider networks and the PSTN as a whole are amalgamations of incompatible technologies linked by translation gateways. These technologies include the original analog telephone infrastructure, legacy digital telephony (T/E-carrier/ISDN/SS7) referred to by the industry as "TDM," cellular networks from 1G to 5G, and VoIP primarily via SIP/RTP. In the United States, the vast majority of PSTN traffic is carried by providers who use VoIP technologies over private links or encrypted tunnels. It is worth mentioning that many other services also use VoIP technologies, including video conferencing and social media, but these so-called "over-the-top" services are generally not fully interoperable with the PSTN.

2.1 Network Abuse & Mitigation Efforts

Telephone numbers are the primary identifiers in the telephone network. When a call is placed, the network uses the dialed number to route the call to the recipient, while conveying the caller's number as the source address, commonly presented as the *Caller ID*. The network also allows callers to specify the value presented in the Caller ID field. This flexibility is useful for legitimate cases, such as businesses presenting a single customer-facing number for outbound calls. However, it can also be misused to conceal the caller's actual number by setting the source field to an arbitrary value, a practice commonly referred to as *Caller ID spoofing*.

Caller ID spoofing is a key enabler of telephone abuse [55]. Abuse takes several forms, including large-volume robocalls, unsolicited spam calls, and scams that impersonate trusted organizations to extract money or sensitive information. These calls impose social and economic costs on consumers and operators. By spoofing Caller ID to present a familiar or trusted number, scammers can increase the likelihood that recipients will answer. Because many call-blocking applications also rely on Caller ID, spoofing helps scammers evade these defenses. Effective Caller ID authentication can, therefore, make the source of a call easier to verify.

Academic and industry efforts proposed countermeasures, including call authentication [62, 63], device or call channel fingerprinting [50, 68], mining blacklists [44, 45, 74], NLP/ML based defense [44, 53], traceback [1, 36], addressing human factors [53, 54], etc. Early regulatory mechanisms include the Do-Not-Call (DNC) Registry [23] and Do-Not-Originate (DNO) lists [26], both of which maintain number registries intended to constrain unwanted or unauthorized calling.

2.2 S/S Standardization and Mandate

Before S/S, IETF RFC 3325 introduced *P-Asserted-Identity* (PAID) [57] to enable OSPs to convey the asserted caller identity. PAID, however, lacks integrity protection and provides no way to express provider confidence. The IETF later established STIR (Secure Telephone Identity Revisited) [37] Working Group to develop stronger assurance protocols, while the Alliance for Telecommunications Industry Solutions (ATIS) [11], a telecommunications standards body for the U.S., defined SHAKEN [8] to standardize STIR deployment across service providers.

In late 2019, the U.S. Congress passed the TRACED Act [76], directing the FCC to require more proactive mitigation. Among other measures, the Act required service providers to deploy S/S in IP networks, and required providers with non-IP networks to implement interoperable call-authentication measures [2]. S/S is the first regulator-mandated PKI-based effort to address Caller ID spoofing, but its effectiveness depends on how closely real-world deployment and operation align with the standards and mandates.

Beyond domestic deployment, ATIS has developed guidance for extending S/S across national boundaries. They define [7] an initial cross-border framework in which jurisdictions with similar legal and regulatory environments establish bilateral trust and exchange lists of trusted STI-CAs. They also generalize this approach for broader international deployment by proposing an international registry through which countries can discover other jurisdictions' trusted STI-CAs while retaining control over which jurisdictions

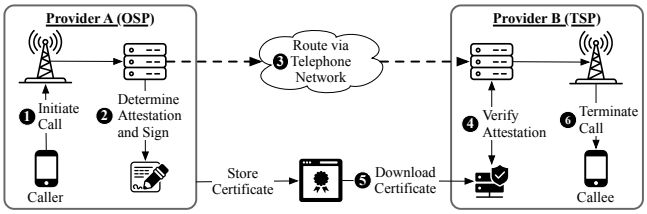

Figure 1: In a S/S call, the caller initiates a call; the OSP authenticates the caller, assigns attestation (*A*/*B*/*C*), signs the call, and forwards the signature. The TSP verifies the signature before call completion.

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

Listing 1: Example of a S/S PASSporT with header, call information payload, and signature. The *x5u* URL points to the X.509 certificate used for signing.

they trust [6]. These frameworks allow calls authenticated in one country to be verified in another without requiring a single global governance authority.

Beyond its original purpose, S/S has become a foundation for broader call trust in the telephone network. Weaknesses in its PKI can therefore affect not only call authentication, but also the mechanisms that build on it. By allowing providers and third parties to bind metadata to calls, S/S supports branded calling and Rich Call Data, including caller names, logos, and call reasons. Recent efforts such as VESPER [52] and Open Verifiable Calling [32] extend this model toward stronger assurances about business identity, number right-to-use, and authorization to present branded information.

2.3 Related Work

Prior work on PKIs documents recurring deployment problems, including missing verification and transparency records, weak keys, information leakage, and inadequate validation, often shaped by human and operational factors [13, 16, 17, 21, 41, 46, 47, 64, 65, 69, 75, 77, 82]. Root trust management can further affect certificate reliability [3, 15, 33, 47], while studies of Certification Authorities (CAs) have identified non-compliance [30, 38], weak accountability [42], and concentrations of invalid certificates among a small subset of CAs [33, 41]. Continued use of revoked certificates, incomplete CRLs, and CRL distribution failures are highlighted through studies of Certificate Revocation Lists (CRLs) [3, 30, 33, 42, 43, 46, 48, 82].

A concurrent study (to appear) identified potential security issues in S/S under a provider-informed threat model, using interviews, partial certificate measurements, and call data from manually initiated calls through a partner provider [12]. The authors also proposed policy and cryptographic measures. However, their measurement scope was limited: they analyzed 6,900 bulk-downloaded certificates outside real-time call processing and via `x5u` URLs from unspecified sources. They did not analyze large-scale call signaling, PASSporT adoption, provider behavior, or real-time certificate collection needed for longitudinal deployment measurement. Thus, a rigorous, end-to-end study of the S/S ecosystem at scale is needed to characterize deployment trends, certificate-authority behavior, provider-level practices, and the policy gaps underlying observed failures.

3 STIR/SHAKEN (S/S)

This section provides an overview of S/S operational framework, including call flow, registration process and interactions among its PKI entities.

3.1 STIR/SHAKEN Call Flow

A typical telephone call may traverse one or more provider networks, each running a different technology stack. Fig. 1 illustrates how calls are routed through the network.

Call Origination. When a caller, Alice, places a call to a callee, Bob, her phone sends a call setup request to her provider, termed the originating service provider (OSP). This request (denoted by ❶) includes the Caller ID that Alice wants presented to Bob as the callback. Upon receiving the request (as denoted in ❷), the OSP determines whether Alice is a known customer and whether she is authorized to use the Caller ID she presents. Under the standards, the OSP can choose from three attestation levels to encode their relationship with Alice and the calling number. They are:

- **Full Attestation (*A*):** The OSP knows the caller, and the caller has the right to use the presented number.
- **Partial Attestation (*B*):** The OSP knows the caller but cannot verify their right to use the presented number.
- **Gateway Attestation (*C*):** The OSP has no information about the caller or their right to use the presented number.

Using this attestation level, the OSP creates and signs a PASSporT [79], a specific-purpose JSON Web Token (JWT) [40]. The OSP then inserts the encoded PASSporT into the `Identity` header of the call request message, shown in Listing 2, and transmitted through the network to Bob (denoted in step ❸). The decoded PASSporT, shown in Listing 1, contains: (1) **a payload** with the signed call information, including the attestation level, originating number, destination number, issuance time (`iat`), and origination identifier (`origid`); (2) **a header** with S/S metadata used to construct and verify the PASSporT; and (3) **a signature** computed over the header and payload. The PASSporT header must also include the `x5u` field, a URI that points to the X.509 certificate [18] used to verify the PASSporT.

Call Termination. Upon receiving the message, Bob's service provider, termed the terminating service provider (TSP), executes the PASSporT verification procedure. The TSP retrieves the certificate URI from the PASSporT's `x5u` field, downloads and validates the certificate (step ❺), and then verifies the PASSporT signature and claims (step ❹). Based on the verification result, the TSP may take additional action before completing the call to Bob (step ❻). If Bob answers, the network establishes the media path, and voice

```
[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
```

Listing 2: Example SIP INVITE from the OSP with the Identity header carrying the encoded PASSporT (Listing 1). We collect signaling data and S/S-specific fields for system-wide measurement (Section 4.1).

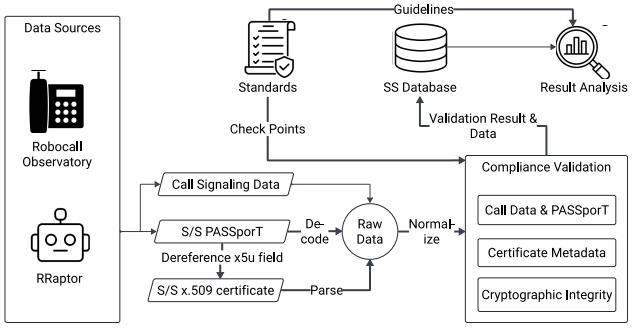

Figure 2: We collect data from Robocall Observatory (RO) and RRaptor, both supporting call-time certificate retrieval via dereferencing the x5u field in S/S PASSporT. We decode, parse, and normalize the data, and validate it using a standards-derived pipeline. We then analyze validation outcomes and underlying data for extended, standards-guided insights.

packets or circuit-switched audio begin to flow between the endpoints.

3.2 STIR/SHAKEN Entities

S/S introduces two governance entities beyond service providers and Certificate Authorities (CAs) [9]. First, the *Governance Authority (GA)* defines the ecosystem policy under FCC oversight [11]. S/S assumes one GA per region to establish the trust and governance model for that deployment.

Second, the *Policy Administrator (PA)* implements the policies defined by the GA [34]. The PA authorizes service providers and CAs before they can participate in the S/S ecosystem, maintains the list of approved CAs, and publishes certificate revocation lists (CRLs). In this role, the PA serves as the operational trust anchor for the S/S PKI. In the U.S., the FCC can also rely on this structure to monitor compliance and take action against non-compliant providers [27].

When a provider registers with the PA, it receives a unique Service Provider Code (SPC), which it can use to obtain certificates from authorized CAs [28]. We note that the bidding, registration, and PKI setup processes for the GA, PA, and CAs are closed and outside the scope of our measurement.

4 Methods

In this section, we present our data collection, processing, validation, and the ethical considerations of this work.

4.1 Data Collection

Our dataset comprises 7,749,934 calls collected from two telephone honeypots over a four-year period, from November 2021 to February 2026. A telephone honeypot operates a set of phone numbers reserved for receiving unsolicited calls, allowing researchers to study robocalling behavior and campaigns. We sourced this data from two such deployments, the Robocall Observatory [60] and the RRaptor honeypot [66].

4.1.1 Robocall Observatory (RO). The RO honeypot contributed 4,315,365 calls to our dataset (55.7% of the total). It consists of an Asterisk Private Branch Exchange (PBX) that controls 66,606 phone numbers. We extended its functionality with a custom module to capture S/S metadata and request certificate URLs in real time. This is crucial as certificate URLs often resolve to different content over time.

We began live collection under this extended RO in March 2025, capturing S/S metadata from 817,337 calls. We also processed earlier calls from the same honeypot through the same pipeline, dereferencing their certificate URLs offline rather than at call time. The two approaches should yield equivalent results in principle; we discuss observed differences in the Results section.

4.1.2 RRaptor. The RRaptor honeypot engages unsolicited callers with context-aware replies and draws additional data from service providers and analytics platforms, giving it broad coverage of robocall activity over many years. The dataset captures most of the same metadata as the RO, and adds call-type labels (inferred intent from call transcripts), but does not include terminating service provider (TSP) verification outcomes like `verstat` or PASSporT data. For analyses requiring those fields, we rely exclusively on RO data; for all other analyses, we combine both datasets. RRaptor contributed 3,434,569 calls collected between January 2024 and February 2026 (44.3% of the total).

4.1.3 Data Processing. We extract all observed fields from the PASSporT and X.509 certificates, including non-standard fields that may reflect deployment deviations. We remove malformed or incomplete records, normalize phone number fields, and standardize timestamps. We parse the `Identity` header into its semicolon-delimited components, separating the PASSporT from its parameters (`alg`, `info`, `ppt`) and then decoding the PASSporT header and payload into flattened columns. For certificates, we extract standard X.509 fields and S/S-specific extensions.

4.2 Validation Pipeline

Our goal is to determine whether the observed metadata conforms to the ATIS and IETF specifications approved by the GA. Rather than stopping at the first failure, we evaluate each check independently. Our pipeline analyzes PASSporT/SIP consistency, certificate

compliance, and cryptographic integrity, covering over 50 validation points per call. This allows us to systematically identify inconsistencies and weaknesses in real-world deployments.

PASSporT and Call Data Compliance. This layer validates the structure of the PASSporT and its cross-field consistency with SIP signaling, following the relevant standards [8, 57, 58, 78, 79]. This primarily captures provider-side implementation correctness and signaling consistency.

Certificate Structural Compliance. This layer evaluates X.509 certificate structure and S/S-specific extensions against the relevant requirements [9, 18, 80]. These checks capture correctness and compliance at the certificate-issuer level.

Cryptographic Integrity. This layer performs cryptographic validation according to the relevant standards [8, 39]. It verifies the call signature and certificate trust, and includes cryptographic sanity checks that may indicate flawed implementations or security vulnerabilities, such as whether two signatures used the same randomness.

A list of checkpoints used by the three layers mentioned above is documented in Appendix B.

Verification Status. We derive *verification status* or `verstat` aligned with TSP semantics: (1) *TN-Validation-Passed or* PASS: all checks pass and attestation is *A*. (2) *No-TN-Validation or* NOVER: all checks pass with attestation *B* or *C*, or only PASSporT/SIP compliance fails while all other checks pass, regardless of attestation. (3) *TN-Validation-Failed or* FAIL: otherwise.

Independent Validation and Code Review. We subjected our validation pipeline to a two-stage independent review. First, each reviewer examined the relevant IETF and ATIS standards and independently assessed whether our derived validation checkpoints accurately captured their requirements. A second-year Ph.D. student with two years of experience working with S/S reviewed the PASSporT and call-data compliance checkpoints. A fifth-year Ph.D. student with more than seven years of experience in telecommunications and network security reviewed the certificate structure and cryptographic integrity checkpoints.

Second, each reviewer examined the corresponding implementation to verify that the code correctly enforced the documented checkpoints, including its handling of malformed inputs and edge cases. The reviews identified minor issues involving input normalization and edge-case handling, which we corrected before conducting the final analysis. We then re-evaluated the affected checks to confirm that the revised implementation remained consistent with the standards-derived validation criteria.

5 Results

We now characterize S/S deployment, present validation results, highlight key findings, and profile ecosystem entities as observed from our vantage points.

5.1 Characterizing Observed S/S Deployment

We observed S/S adoption increases from multiple perspectives. We use 5-month averages to mitigate the impacts of transient fluctuations in the reported values in this section.

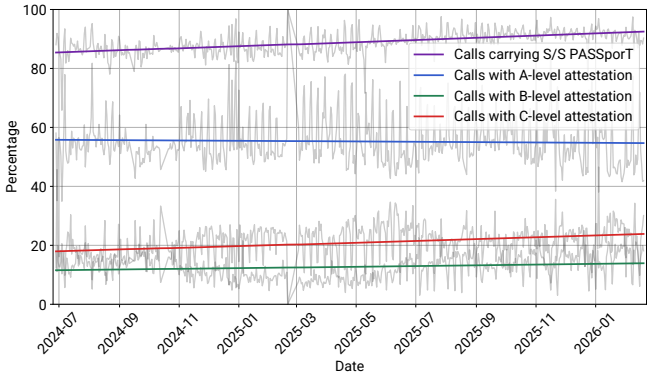

Figure 3: Over the most recent 20 months, PASSporT presence and *C* attestation exhibit steady upward trends; *A* attestation exhibits a slight downward trend, while *B* attestation remains stable

Finding 1: **S/S PASSporT presence is steadily increasing**.
We observed an increase in PASSporT presence from approximately 86.3% in June 2024 to 91.1% in February 2026, corresponding to an increase of 0.31 percentage points per month ($p < 0.0001$, $R^2 = 0.635$). We used data collected from the Robocall Observatory, as RRaptor data did not carry PASSporT. This trend suggests increasing adoption of S/S among providers represented in our dataset.

Since calls may traverse non-IP segments that strip PASSporTs, we anticipated a lower presence of S/S. The high and increasing presence may indicate broader IP-based routing, adoption of out-of-band S/S [56], or other provider practices that preserve S/S PASSporTs across the call path.

Finding 2: **S/S adoption is increasing among providers**.

We also observed an increase in the number of unique providers each month, from 220 in June 2024 to 613 in February 2026, corresponding to an estimated increase of approximately 17 providers per month ($p < 0.0001$, $R^2 = 0.849$) throughout our whole dataset. In total, we observed 1,434 uniquely named providers in our dataset, although not all were active in every month. Together, these results indicate a steady expansion of the observed provider ecosystem.

Finding 3: **5,722 (65.9%) of U.S.-based providers have fully or partially implemented S/S**.
We summarize this information using the Robocall Mitigation Database (RMD) [29] (as of April 12, 2026), maintained by the FCC, which enables providers to report their S/S implementation status and compliance plans. Currently, 10,798 providers are registered, including 2,109 foreign providers from 157 countries. We find that 35.7% of foreign providers exhibit full or partial S/S compliance. These providers represent international providers with a defined relationship with U.S.-based providers, rather than a conclusive list of all international providers that might generate a call to the U.S.

Finding 4: **S/S achieved around 65.9% provider level deployment coverage in 5 years, compared to roughly 56% RPKI coverage over 15 years**.

The Resource Public Key Infrastructure (RPKI), which enables verification of an Autonomous System's (AS) authority to originate an IP prefix in BGP, provides a useful point of comparison with S/S. RPKI development began in 2008, with deployment starting around 2011 [14]. Like S/S, RPKI deployment operates at the ISP level without involving end users. 55.71% of *unique IP-prefix-to-AS mapping pairs* of regions under American Registry for Internet Numbers (ARIN) are now covered by RPKI [51]. Another point of comparison is HTTPS deployment. In 2025, around 71% of popular websites support secure implementation of HTTPS [81], nearly 30 years after the start of widespread operational deployment of SSL/TLS on the Internet.

We acknowledge the substantial differences in scale, governance, and architectural design between the public Internet and the telecommunications ecosystem. Nevertheless, these two comparisons highlight that regulatory intervention can accelerate the deployment of complex security mechanisms across large-scale networks.

Finding 5: **Around 11.88% of calls within our dataset did not have PASSporTs**.
We found 162,413 calls from 89,517 unique calling numbers with no PASSporT. We used the same data as Finding 1. Among these numbers, 29,559 (33%) reappeared in our dataset with PASSporTs, suggesting that S/S PASSporTs are not consistently preserved for the same calling number. This may reflect legacy incompatibility, unsupported call paths, or unintentional stripping during call routing [2]. Thus, despite the gradual increase in S/S adoption over time (Fig. 3), missing PASSporTs remain non-negligible.

Finding 6: **Error-per-call has modestly improved over time**.
We define error-per-call as the total number of validation errors across all categories (allowing multiple errors per call), normalized by the total number of calls. We calculate this metric using Robocall Honeypot data collected during the live-collection period as described in Section 4.1.1. We chose the subset in which validation errors are not influenced by time-sensitive factors, as described in Finding 12.

We found that, this metric decreases from 1.59 to 1.23 between March 2025 and February 2026 (slope = −0.0039 per week, $p < .001$, $R^2 = 0.43$). While non-compliance remains non-negligible, these results indicate measurable progress toward ecosystem maturity.

We additionally measured the fraction of calls that contained at least one validation error, normalized by the total number of calls received. The metric remained at approximately 80% between March 2025 and February 2026. Thus, the observed improvement reflects a reduction in the number of errors per erroneous call rather than a reduction in the fraction of erroneous calls.

5.2 Claimed Attestation

Finding 7: ***C* attestation is increasing in observed data, while *A* decreases and *B* remains stable**.
C attestation, which reflects a provider's inability to identify the caller, increased from 17.0% to 23.9% (+0.37 percentage points per month, $p = 0.00047$, $R^2 = 0.48$). This can affect the Industry Traceback Group's investigative tasks to trace calls back to their original callers [36]. We also found that *A* attestation decreased from around 52.7% to 50.8% (−0.12 percentage points per month, $p = 0.15$, $R^2 = 0.11$), while *B* attestation remained stable over time, with no meaningful trend (+0.06 percentage points per month, $p = 0.64$, $R^2 = 0.01$).

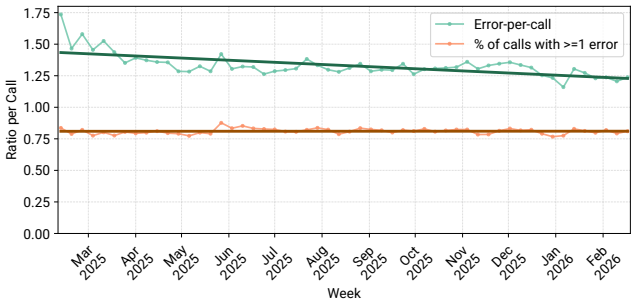

Figure 4: Error count per call decreased from 1.59 to 1.23 over the measurement period. This indicates ongoing improvement despite persistent imperfections, with error clustering within individual calls decreasing over time.

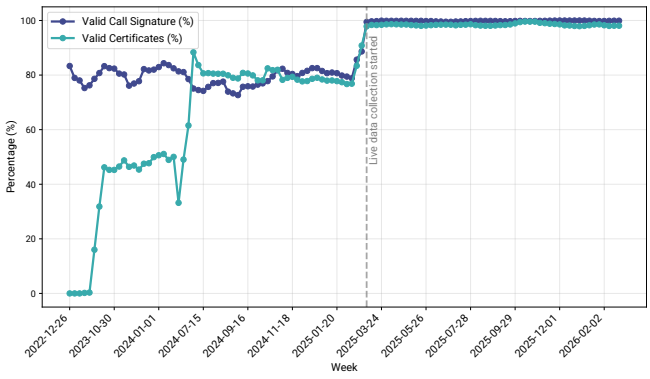

Figure 5: Change in valid call signature and certificate percentages before and after live data collection. The observed shift is driven by time-sensitive verification effects (see Section 8), highlighting issues with retrospective verification.

Finding 8: **Observed attestation periodicity aligns with robocall periodicity**.
Previous work [59] shows that unsolicited call volume follows a weekly cycle, *i.e.,* elevated on weekdays and lower on weekends. We therefore hypothesize that *A* attested calls (less likely to correspond to unsolicited calls under the S/S definition) will be relatively higher on weekends, while *C*-attested calls will be lower. Our data supports this hypothesis: *A* attestation is higher on weekends than on weekdays (62.8% to 52.3%, $p < .001$), while *C* attestation decreases on weekends compared to weekdays (16.8% to 22.5%, $p < .001$). *B* attestation stayed relatively stable.

Finding 9: **Wrong-number calls in our dataset exhibit a higher proportion of *A* attestation compared to the overall unsolicited calls**.
The RRaptor dataset includes a summary field that infers call intent from audio recordings. 3.4% of RRaptor calls are labeled as wrong-number calls. Given the multi-million scale of the dataset,

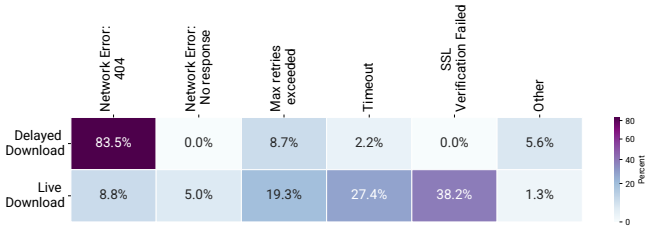

Figure 6: Certificate downloads fail for 0.12% of call-time requests and 12.86% of delayed requests. Delayed failures are dominated by 404 errors (84%), while call-time failures primarily result from TLS verification errors (38.2%) and timeouts (46.7%).

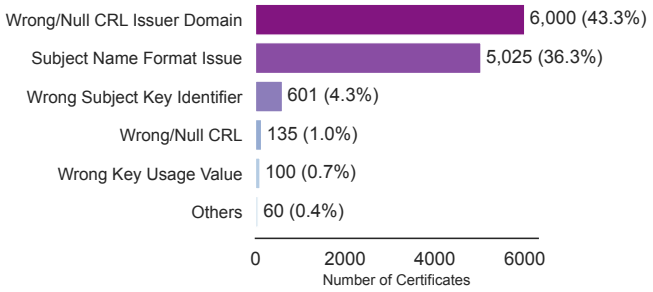

Figure 7: Certificate formatting error distribution: percentages denote the fraction of unique certificates over the entire dataset (not just failed certificates), indicating widespread formatting issues.

this represents a non-trivial subset for analysis. Wrong-number carries higher *A* attestation (72.8%) compared to the overall unsolicited call population (57.4%), alongside a markedly lower *C* attestation (15.2% vs. 26.4%). This shift suggests that misdials are more likely to originate from callers with authenticated relationships with their providers, whereas unsolicited callers typically lack such verified associations. These findings suggest that providers are making progress toward assigning attestations in accordance with S/S guidelines, despite remaining inconsistencies.

Finding 10: ***A* attestation does not guarantee a safe-to-receive call**.
A attestation dominates the dataset (58.4%), followed by *C* (25.9%) and *B* (15.7%). Excluding the small subset of misdials/wrong numbers, we still get 58.2% of calls with *A* attestation. *A* attestation is widely believed to be *safer* in comparison to *B* or *C* attested calls, and often presented to end-users as "verified". Since calls reaching our data sources are unsolicited, they are more likely to be spam calls. We want to emphasize that *A* attestation for around 60% of calls is not incorrect by definition, but it challenges how attestation, and S/S more broadly, is interpreted by end users.

5.3 Validation Results

Finding 11: **48.2% of our collected certificates violate at least one S/S guideline**.
S/S standards [9] specifically require X.509 *Version 3* certificates [18] to support extension fields for S/S. We found 6,687 out of 13,861 certificates were noncompliant. Among failed certificates, 90.6% failed format conformance checks, 3% failed cryptographic validation, and 6.4% failed both. These numbers represent all the certificates we collected.

We found that cryptographic validation failures occurred more for calls with delayed certificate download, as explained in 12. So, we checked the failure percentage for live collection and found 57.6% out of 4,005 certificates were noncompliant. However, for this subset, 94.7% failed format conformance checks, only 0.9% failed cryptographic validation, and 4.4% failed both.

Finding 12: **Certificate validation in S/S is time-sensitive**.
We observe a sharp reduction in cryptographic errors after transitioning to real-time certificate download (Figure 5). Our retrospective analysis shows 27.8% of calls failed certificate verification with the error "`certificate used before valid period`"; under live collection, this drops to 0%.

As described in Listing 1, the originating service provider (OSP) populates the `x5u` field with a URL pointing to the certificate containing the public key. However, the standard does not require OSPs to retain or archive previously issued certificates. Consequently, providers may replace or remove certificates over time without violating the standard, even if doing so impacts retrospective verification, which is needed during traceback [36].

The dramatic change in our data can be explained by this certificate rotation. When these updated certificates are downloaded during delayed analysis, their validity periods no longer align with the original call timestamp, producing the otherwise uncommon "`certificate used before valid period`" error. A similar pattern is observed in signature validation: 18% of calls fail under delayed certificate download, compared to only 0.1% under call time download (Figure 5). This likely reflects cases where the public key from a rotated certificate no longer matches the key used to sign the original PASSporT, even though the signature may have validated correctly at the time of the call.

Certificate download failure also varies. Certificate download fails for 0.12% of calls when the download is requested at call time, and for 12.86% of calls for delayed download requests. The reasons for certificate download failure also differ depending on download timing. Delayed download error is dominated by 404 errors (84%), indicating that previously accessible resources are no longer available. In contrast, call-time downloads usually fail due to errors such as TLS verification failures (38.2%) and timeouts (46.7%), reflecting real-time server constraints.

Finding 13: **Certificate format errors dominate validation failures in our dataset**.
The most prevalent issues include:

- The standard [9] requires the CRL Distribution Point extension to include correct issuer information. 43.3% of certificates contain incorrect or null CRL issuer fields, often despite the presence of the extension.
- The specification mandates that the Subject Common Name follow the `SHAKEN <SPC>` format, yet 36.3% of certificates violate this requirement.
- STI certificates must include a Subject Key Identifier derived as

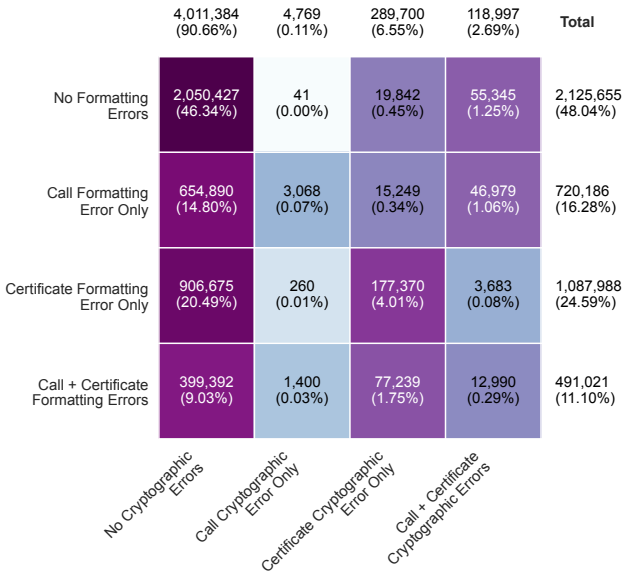

Figure 8: Violation counts across validation checkpoints and their overlaps. Formatting errors (for both certificate and call) dominate. Also, errors rarely occur in isolation.

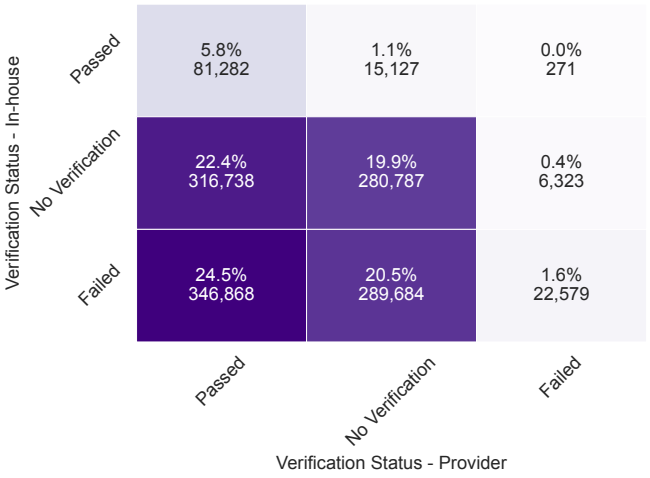

Figure 9: 975,011 (71.7%) of calls exhibit mismatches between our independent validation and the provider's results, with discrepancies concentrated among failed calls. Our validation flags a large subset of provider-classified "pass" or "no validation" calls as failures.

the 160-bit SHA-1 hash of the public key [18]; however, 4.3% of certificates exhibit mismatches. Even after validating against a comprehensive set of alternative hash constructions (including SHA-1 variants, truncated SHA-2/SHA-3 digests, and encodings with and without EC point prefixes), no matches were found.

These results show S/S deployment provides a PKI with relatively few failures in signature validation and trust chain establishment. However, it falls short in enforcing the extensive X.509 customization required by the standards. These results include all certificates in our dataset because formatting errors are not time-sensitive.

Finding 14: **53.7% of all observed calls violate at least one S/S guideline**.
35.7% of total calls collected through Robocall Observatory carry certificate-format violations, making this the largest contributor to validation Fail. Call-level formatting errors affect 27.4% of calls, including telephone-number formatting errors, mismatches between PASSporT and call signaling data, missing values, misconfigured UUID/`origid` fields, etc. Cryptographic failures are less frequent. 2.8% of calls fail call-signature validation and 9.2% fail certificate validation. Figure 8 shows that these failure modes are not independent. Notably, 12,990 calls (0.3%) fail all four validation categories spanning 37 providers. Most of these providers generated very few calls, while others rectified their failures in more recent calls.

We also examined these rates in our live collection. Certificate-formatting and call-level formatting errors occurred in 38% and 27.1% of calls, respectively. Cryptographic failures were less frequent: 0.15% of calls failed signature validation, and 1.42% failed certificate validation. Thus, formatting-error rates remained similar, whereas cryptographic-error rates decreased, consistent with our earlier observations. We excluded data from RRaptor in this analysis as they do not contain PASSporT data, which is required to validate relevant checkpoints.

Finding 15: **For 71.7% of calls, our in-house `verstat` (*verification status*) and provider `verstat` do not match**.
We had access to a single provider's `verstat` for 1,359,659 calls, all collected through Robocall Observatory, which we compared to our in-house validation. In-house validation yields *TN-Validation-Passed or* Pass for 6.9% calls, *TN-Validation-Failed or* Fail for 49.2% calls, and *No-TN-Validation or* NoVer for 43.9% calls. In contrast, the provider reports Pass for 52.7% calls, Fail for 2.1% calls, and NoVer for 41.4% calls.

Overall, 975,011 (71.7%) of calls exhibit mismatches between the two systems. Discrepancies are most pronounced among Fail calls: as shown in Figure 9, our validation classifies a subset of provider's Pass and NoVer calls as Fail. Our pipeline is strict, so one interesting case is the 271 calls that get Pass in our validation but get Fail in the provider's. One plausible explanation is transient network errors during certificate download.

For our live collection (731,544 calls), this mismatch decreased to 64.0%. Concurrent validation reduced the mismatch because it was less affected by cryptographic errors that impacted retrospective validation.

Our validation logic strictly applies policies derived from the relevant standards. Based on our discussion with the provider, their implementation is more permissive toward formatting nonconformance, which is consistent with the observed mismatch. We hypothesize that such flexibility may be necessary to deploy a PKI across a highly interoperable, industry-wide system without unnecessarily disrupting legitimate calls and that similar behavior may occur among other providers. Our next finding further examines this mismatch.

Finding 16: **S/S validation guidelines can result in variable implementation across providers**.

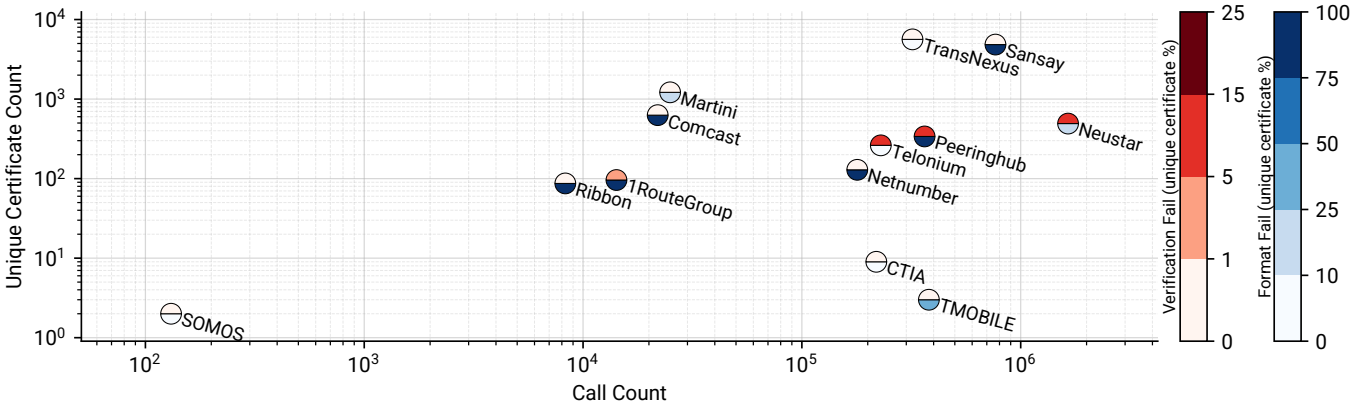

Figure 10: CAs across call volume, certificate issuance, and error rates (in log scale). Few CAs dominate issuance and call signing. Some CAs (e.g., TransNexus, Sansay) serve broad provider bases, while others exhibit self-serving or provider-specific behavior (e.g., T-Mobile, CTIA). Error patterns are also heterogeneous; some CAs achieve near-complete compliance, while others exhibit persistent formatting and some verification failures.

We analyzed the calls that Fail in our validation but Pass with the provider. At least one provider systematically ignores certificate format errors, but flags most call-level format errors. Notably, some certificate-related cryptographic failures, such as the use of expired certificates (1,163 calls) and revoked certificates (3,296 calls) to sign calls, are frequently labeled as NoVer rather than Fail by the provider. The same also occurs for call signature failure due to invalid key sizes or unsupported signature algorithms.

These discrepancies highlight a broader issue we faced during this measurement. From exhaustive examination of standards, we found validation guidance is incomplete, with general principles [8] and specific cases [5, 10] scattered across documents. As a result, consistent interpretation and implementation of S/S validation across TSPs cannot be expected. Furthermore, the standard explicitly defers critical validation decisions to providers on several points. For example, providers may choose the freshness threshold (i.e., the time difference between PASSporT creation and call arrival), with a suggested value of one minute.

5.4 Certificate Authority Practices

Finding 17: Certificate Authorities vary wildly in business models and priorities.
We analyze CA coverage across certificate issuance, provider association, and call volume, revealing systematic differences across CAs. Some CAs (e.g., TransNexus, Sansay) act as infrastructure providers, exhibiting a strong presence across all dimensions. Others demonstrate more specialized behavior: T-Mobile and Comcast certificates are primarily used to sign calls for their own networks. CTIA predominantly serves Verizon (95% of its calls), indicating a narrow, provider-specific role. In contrast, TransNexus is highly provider-oriented, followed by Neustar, Sansay, Peering Hub, and Telonium, in supporting more providers.

Figure 10 shows that issued certificate volume does not always correlate with call volume. T-Mobile issued only 3 certificates that were used to sign 308k calls, while the CTIA issued 9 unique certificates that were used to sign 298k calls. Neustar certificates were used to sign 1.65 million calls, despite them issuing only 492 (3.6%) certificates. Alternately, 85% of all certificates are issued by only three CAs: TransNexus (41.0%), Sansay (35.3%), and Martini (8.8%). Provider coverage is more distributed. TransNexus and Sansay again rank highest, serving 28.2% and 17.4% of providers, respectively; however, unlike certificate issuance, this distribution is less skewed. These patterns, together with the long tail of low-volume CAs (e.g., 1RouteGroup, Ribbon, SOMOS), highlight the diversity of operational strategies within the ecosystem.

Finding 18: Certificate validity periods span orders of magnitude .
The S/S standards do not constrain certificate validity periods. Short-lived certificates are preferable because they limit exposure to compromise, reduce reliance on revocation, and enable faster key rotation and policy updates. Given that S/S policies are still evolving, long certificate validity periods are undesirable.

10,691 (77.6%) of certificates have validity periods less than 30 days, and are used to sign only 9.4% of calls. 71.8% of calls are signed by 1,047 (7.6%) of certificates with a validity of 365 to 370 days. We also observe certificates with unusually long validity (over 1,000 days, including more than 4,000 days).

Finding 19: Calls incorrectly reference root CA certificates instead of the leaf certificates used for signing..
We observed 3,747 calls since February 2025 for which the certificate URI in the PASSporT resolved to Telonium's root *CA* certificate. Although we initially suspected that the root certificate had been used for signing, which would violate S/S's expectations and standard PKI principles, none of the signatures verified with the root certificate's public key.

We therefore brute-forced verification against all Telonium-issued leaf certificates observed in our dataset. This revealed that the calls were signed using leaf certificates issued to the originating providers, while the PASSporT incorrectly referenced Telonium's root certificate. We identified this behavior across three providers.

This misconfiguration causes verifiers that follow the certificate

URI to retrieve the wrong public key, resulting in otherwise valid signatures failing verification. We disclosed the issue to Telonium and the affected providers.

Finding 20: **Some CAs use RSA to sign leaf certificates**.
We observed two certificates that signed 12 calls issued by Neustar using the *sha256WithRSA* algorithm. While SHAKEN mandates ECDSA for leaf certificates, it does not constrain signature algorithms for root or intermediate CAs and permits this variation.

These certificates use 2048-bit RSA keys. Although secure, RSA signatures are larger than their elliptic-curve counterparts, increasing computational and bandwidth overhead during verification. This heterogeneity may also introduce operational complexity by requiring support for multiple cryptographic verification paths within the certificate chain. This observation highlights an area where implementation practices may vary despite end-entity compliance.

Finding 21: **Complete certificate-format compliance is achievable in real-world deployment**.
We consider only certificate-level formatting and cryptographic errors, excluding non-CA-attributable issues (e.g., malformed call signatures). We further exclude validation errors arising from delayed certificate collection, as discussed in Finding 12. *CTIA* and *SOMOS* exhibit no certificate-level formatting or cryptographic errors (Figure 10), demonstrating that even under strict validation, proper implementation can achieve full compliance. *T-Mobile* and *Martini* resolved their formatting errors within the first few months of their operations. Comcast presents a unique anomaly: its Subject Key Identifier is not derived from a SHA-1 hash of the public key or any other standard alternative. Other providers primarily exhibit missing or malformed CRL issuer domains, improperly formatted subject common names, or certificate policy inconsistencies. We analyzed these in Finding 13.

Finding 22: **We observed unregistered CAs in our dataset**.
We identified six CAs in our dataset who are not registered with the PA. They each appeared for short periods and issued 10 certificates in total, which were used to sign 314 calls. They all failed validation and exhibited severe format errors. We excluded them from CA characterization. We also found two international CAs in this category, but we will discuss them separately.

5.5 Originating Provider Practices

Finding 23: **A small fraction of providers dominate signing activity**.
We found 1,434 providers in our dataset, of which the top 15 (1%) signed 50.6% of calls. The top 5% (72) of providers signed 79.5% calls. As shown in Figure 11, providers predominantly use *A*-attestation, with *B* and *C* comparatively rare. Approximately 55.3% of providers use *A* exclusively, while 66.9% never use *B* and 76.4% never use *C*. At the opposite extreme, about 4.7% of providers exclusively use *B* and another 5.1% exclusively use *C*.

Most providers in our dataset operate at low volume, typically signing between 10 and 1,000 calls, while high-volume providers are comparatively rare. We observe that as the fraction of calls containing at least one error increases, the number of errors per call also increases, indicating that errors tend to co-occur rather than appear in isolation.

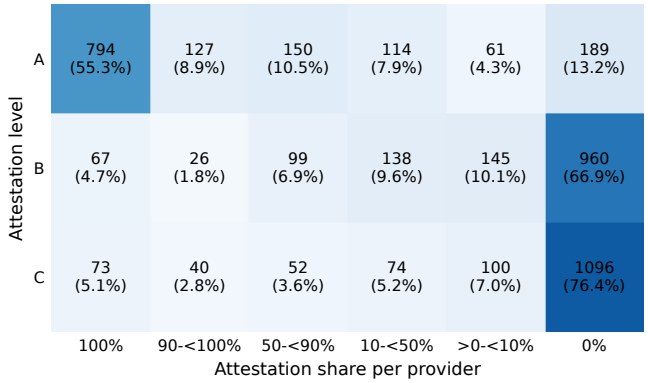

Figure 11: Providers predominantly use *A*-attestation, with *B* and *C* comparatively rare. Approximately 55.3% of providers use *A* exclusively, while 66.9% never use *B* and 76.4% never use *C*. At the opposite extreme, about 4.7% of providers exclusively use *B* and another 5.1% exclusively use *C*.

Finding 24: **A minority of providers made a wide variety of cryptographic errors**.
Signature verification failures occurred for 26 providers (1.8%). Occurrences of self-signed certificate usage (1 provider) and post-revocation certificate usage (4 providers) were limited. Invalid public keys, incorrect signature length, and unsupported algorithm errors were also isolated to individual providers. Additional provider-side issues include misconfigured certificate repositories, incorrect JWT fields (`typ`, `ppt`), and inconsistencies between PASSporT and SIP attestation. These were rare but highlighted residual compliance and implementation gaps.

Finding 25: **Service Provider Codes (SPC) do not uniquely identify service providers**.
The SPC is a new S/S-specific identifier unique to a service provider (Sec. 3.2). A provider may hold multiple SPCs for different services, but a single SPC should not be shared across providers. Certificates are issued to providers based on its SPC, embedding the provider's identity in the subject field. CAs are required to authenticate the request with a certificate from the PA, binding an SPC to a private key.

We identified 1,284 providers by SPC and 1,434 by organization name. The mismatch arises from naming inconsistencies (e.g., "AT&T Services, Inc.," "ATT," "ATT SHAKEN E-E" for SPC 4036) and SPCs mapped to different entities following mergers or acquisitions. We also observe SPC reuse across *unrelated entities* over time. For example, SPC 1001 is sequentially associated with Martini Security, The VoIP Talk, AcmeTelecom, and SIPCALL TELECOM. These last two would seem to be generic test cases, but we only observe them because the calls were found in a live honeypot, once again raising the question of why test infrastructure would sign unsolicited calls. SPC 731K is shared by ChaseData Corp and DialedIn. Additionally, Toly Digital Networks Inc. shares five SPCs (0348, 0496, 0721, 1637, 2039) with multiple providers in overlapping periods.

Finding 26: **Some providers carry calls with unrelated PASSporTs**.
We identified 305 calls in which PASSporT data (originating and destination numbers) in the JWT do not match the call signaling metadata, independent of formatting errors. Among these, 284 involve expired certificates. Despite valid JWT signatures, the delay between token creation and its arrival at the TSP averages more than 7 days (up to 25 days), far exceeding the expected sub-minute window.

One plausible explanation is the reuse of previously valid `Identity` headers by an unaffiliated actor, which would fail under proper validation yet may still appear compliant with FCC S/S requirements. Alternatively, the pattern may reflect severely negligent operational practices by the providers.

Finding 27: **Current provider `origid` practices provide insufficient utility towards traceback**.
The `origid` field in a PASSporT is a globally unique, opaque identifier (UUID) indicating the source of a call within an OSP network [10, 20]. It supports reputation tracking, analytics, and traceback by enabling correlation of suspicious traffic to a consistent source. The most important use of this identifier is for *C*-attestations. The standard recommends fine-grained, near one-to-one `origid` to source attribution [8, 10], because by definition a gateway is not the last link in a traceback chain. For *A*-attestation, coarse-grained `origid` values are allowed.

We saw unique caller ID per `origid` ratios of 1.7, 1.5, and 1.5 for *A*, *B*, and *C*-attestation, respectively. If all users were compliant, we would expect this ratio to be much higher for *A*-attestation, but lower for *B* and *C* attestations.

Among 259 providers that generated *C*-attested calls, 68.0% exhibit low `origid` granularity, reusing a single identifier across multiple calling numbers. Notably, nine providers reuse the same `origid` for more than 50 distinct *C*-attested callers. Moreover, Onvoy, RingCentral, T-Mobile USA, and Vonage each sign over 1,000 such calls using a single `origid`.

We looked into the case of T-Mobile USA, which maintains a large overall pool of `origids` across their traffic, but reuses one `origid` for all of their 59,233 unique *C*-attested callers. This may suggest aggregation at shared ingress points (e.g., common NNIs or gateways). However, there is no defined policy governing its granularity. As a result, observed patterns likely reflect provider-specific internal architectures, limiting our ability to draw definitive conclusions.

Finding 28: **Providers transmit malformed UUID as `origids`, which may result in unwanted identifier overlaps**.
`origid` values are UUID [20], which specifies that UUIDs should be globally unique and encoded in a particular format. When evaluated against the UUID specification [20], 24.3% of calls carrying PASSporTs exhibit malformed `origid` values, including 8.5% with formatting errors, 15.6% with variant inconsistencies, and 0.3% with version violations. We also observe `origid` reuse across providers: 365 `origids` are shared by two providers, 27 by three providers, 6 by four providers, and one `origid` is shared by five providers. Bandwidth Inc. appears most frequently in this set (71 occurrences). As a telephone number-providing organization, this may reflect operational practices in which downstream providers reuse `origid` values associated with numbers acquired from upstream entities rather than generating new identifiers independently.

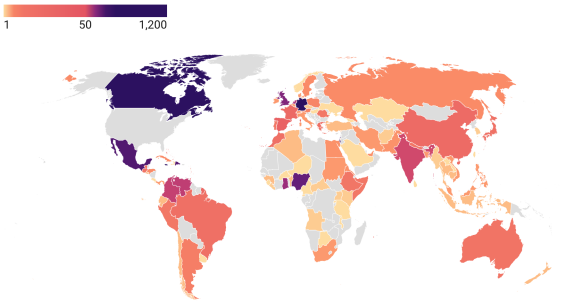

Figure 12: Geographic distribution of calls originating from 120 non-U.S. countries observed in our honeypot

5.6 S/S International Calls

Finding 29: **All international calls do not carry "*C* " attestation by default.**.
Standards [8] often characterize *C*-attestation as "gateway" attestation, leading to the common but incorrect expectation that international calls should carry *C*-attestation [31]. We observed calls originating from 120 countries other than the U.S. (Figure 12). Among the calls, 60.2% carried *C*-attestation, while 20.7% and 13.6% carried *A* and *B*-attestations, respectively. This distribution contrasts with the overall dataset, where *C*-attestation is less prevalent.

A/*B*-attestation in international calls is not inherently incorrect. In limited cases, it may reflect international number portability. More broadly, it indicates global S/S deployment, as reflected in RMD disclosures. Manual inspection shows that international providers often apply S/S (or equivalent frameworks) when handing calls to U.S. networks, frequently via U.S.-based partners that re-sign calls with *A*-attestation under established trust relationships. Consistent with this, *T-Mobile* and *Verizon* account for the highest *A*-attested volumes (2,246 and 1,833 calls, respectively).

We identified 2 French, 3 Canadian, and 327 U.S.-based providers who signed calls originating outside their own countries. 215 providers sign calls for only a single foreign country, while a small set of providers—including *Onvoy*, *T-Mobile*, and *Peerless Network* operate across 83, 41, and 30 countries, respectively.

Finding 30: **The U.S. Policy Administrator does not provide international root certificates as required by standards**.
S/S [7] defines cross-border validation via a Cross-Border Trust List maintained by the PA, enabling validation of calls signed by international providers using the same pipeline as U.S.-based providers. Although a compatible setup (identified by version 1) is currently supported by the PA, we find no international certificates in the PA's trusted root bundle.

A lightweight International SHAKEN registry has also been proposed [6] to facilitate exchange of trusted CA lists across jurisdictions while preserving local trust control; however, we find no evidence of such a mechanism in practice. As a result, validating international calls currently requires deviating from standards or

relying on methods that are not fully cryptographically sound.

We identify two prominent international CAs in our dataset. *Neustar* operates across the U.S. and Canada. Following our validation pipeline, approximately 90% of calls (11,001) signed by certificates issued by the Canadian Neustar CA fail because their certificate chains include a self-signed certificate; the remaining 10% fail chain validation. *Metaswitch*, a CA based in Great Britain, issued certificates that sign 3,106 calls with 28 unique certificates; all of which also failed chain validation.

6 Limitations

Our measurements are based on unsolicited calls received by two telephone honeypots. Consequently, our dataset may over-represent adversarial calls, with significantly fewer benign calls, relative to the broader telephone ecosystem. This sampling bias may affect the temporal and behavioral patterns we observe, the set of providers represented, and each provider's relative share of calls. It may also increase the observed prevalence of anomalous S/S implementations. Furthermore, intermediate providers or non-IP network segments may modify or remove PASSporTs; therefore, a missing or malformed PASSporT cannot always be attributed to the originating provider. Also, provider-generated verification results are available from only one terminating provider. This may not reflect industry-wide validation practices or even that provider's broader operations. Accordingly, **our results characterize S/S deployment among calls reaching our vantage points rather than the entire telephone ecosystem.**

A sufficiently large representative dataset of legitimate or solicited calls is not available to us. So, we could not determine whether, or to what extent, our observations differs from network-wide traffic. We found a small number of industry deployment reports, each with distinct dataset characteristics. These include reports based on telephone numbers protected by active robocall-prevention solutions [70], reports that distinguish between larger and smaller providers [71], and reports without call-level observations [67]. However, the broad trends observed in our dataset are consistent with those reported by industry.

Nevertheless, unsolicited calls are a policy-relevant setting for S/S because mitigating spoofed and abusive calls is a primary motivation for its deployment. Our measurements provide a longitudinal baseline of how S/S operates within this important class of traffic.

Retrospective certificate collection introduces time-dependent measurement effects as discussed in Finding: 12. We carefully distinguished between real-time and retrospective certificate collection, where applicable.

7 Discussion

Throughout this paper, we identified multiple issues that can persist despite standards-compliant deployment. In this section, we highlight underlying policy gaps that contribute to these challenges and discuss potential solutions, including ongoing S/S improvement efforts that aim to address them. We also examine S/S's broader impact and the key factors behind its relative success.

Inconsistent S/S deployment due to non-conclusive standard guidelines. Validation guidelines for TSPs are not concrete or exhaustive, as discussed in Finding 16. Several critical decisions are deferred to general IETF RFCs or individual providers. In the absence of well-defined validation guidelines, S/S cannot be implemented consistently across the telephone network.

TSP's action after validation is ambiguous. Guidelines on the TSP's action after validation are critical. Current suggestions include displaying a warning based on verification [4], which is implemented by a few TSPs. Stricter actions, however, introduce an important complication. Our results show that validation can fail for reasons outside the caller's control. Nevertheless, if a TSP drops the call due to that failure, the caller and receiver are denied service. This is particularly concerning because the core value proposition of telecommunication networks is availability.

Certificate archival is required to make traceback and retrospective validation work. In the current deployment, if a CA ceases to operate within S/S, the PA can remove its root certificate from the trusted root bundle. Consequently, it becomes impossible to verify the cryptographic signature of an old call signed by such a CA, even when the certificate is downloaded at call time. In more prevalent cases, a certificate within a provider's domain is often replaced with another, making it unavailable for later retrieval.

A certificate transparency log [12], a centralized certificate repository (as currently suggested by the standards [5]), or a suitable archival mechanism maintained by the PA could address this issue. Given the relatively small size of the telecommunications ecosystem, archiving all certificates used within it would impose only modest storage requirements.

Basic S/S Assumptions are not Always Correct. Attestation is not a derived metric; it simply reflects the provider–caller relationship. S/S initially permitted the enumeration of authorized numbers (or ranges) in the certificate extension fields. While number-level authorization would strengthen accountability for *A*-attestation, it is impractical due to number portability, ever-changing customer base, and variation in telephone numbers. It also offers limited benefit for *B*/*C* verification. In practice, OSPs specify a Service Provider Code (SPC) instead. There are no concrete guidelines for OSPs on determining attestation levels. Given the complexity and variation within each provider's internal structure, such a guideline is unlikely to be conclusive. Consequently, the most crucial aspect of S/S, determining the attestation level, remains a black box within each provider domain, largely relying on provider discretion and reputation.

Current performance of S/S and contributing factors. Despite its shortcomings, the S/S PKI has performed comparatively well. This is largely because of strong government intervention: strict deadlines, continuous oversight, and defined penalties [27]. Unlike the open Internet, the S/S has overarching guidelines for CA and provider onboarding. S/S's deployment used a top-down approach, ensuring the inclusion of only these registered participants. Having a central trust authority (PA and GA) helped enforce accountability at each stage. The predefined and quantifiable ecosystem size, along with predictable growth, further helped.

As an additional benefit, S/S encouraged widespread provider registration with regulatory bodies, which gives a foundation for future regulatory efforts. It also establishes a structured foundation for future PKI deployments in the telecommunications domain.

8 Conclusion

We conducted a longitudinal study of the STIR/SHAKEN PKI to assess its compliance with the operational policies and technical specifications set by the standard. While S/S advances a federated PKI deployment in telephony, its effectiveness remains limited by inconsistent implementations and a gap between policy expectations and practical capabilities. We highlight concrete directions for strengthening policy and deployment to more effectively mitigate telephone network abuse.

Responsible Disclosure

We notified the relevant Certificate Authorities (CAs) and providers of our findings and are grateful for their timely responses and operational context. Their feedback helped us evaluate alternative explanations, design follow-up experiments, and refine several findings without changing the underlying observations. For example, we initially observed 3,747 calls whose certificate URI pointed to the Telonium root certificate, making them appear to have been signed with the root certificate. Based on Telonium's response and subsequent verification, we confirmed that the calls were instead signed with providers' valid leaf certificates; the issue was a misconfigured certificate URI that referenced the Telonium root certificate rather than the leaf certificate actually used for signing.

We contacted Peering Hub regarding a Subject Common Name format that deviated from the standard. Peering Hub explained the operational reason for its format and confirmed that the deviation did not cause validation failures in practice. Nevertheless, they confirmed plans to align the Subject Common Name format with the standard to eliminate the apparent non-compliance.

We contacted Comcast regarding missing CRLIssuer fields and Subject Key Identifier values that deviated from the STIR/SHAKEN requirements. Comcast agreed with our observations and informed us that the Subject Key Identifier issue had already been corrected in late January 2026, near the end of our measurement period. Comcast also confirmed that they are working to add the CRLIssuer field to its certificate issuance pipeline.

Data Availability and Reproducibility

Our data-collection, processing, and validation code is available at https://github.com/wspr-ncsu/STIR_SHAKEN_Validation_Pipeline. Our agreements with partner providers prohibit us from sharing the call-signaling data and, by extension, the associated PASSporT and provider-generated verification-status (*verstat*) data, as discussed in Section A. However, researchers with comparable SIP-trunk access can collect, process, and validate similar data using our pipeline. The X.509 certificates we study are already publicly retrievable by service providers and certificate authorities via their certificate URLs. We have also made our dataset of 13,861 unique certificates available at https://github.com/wspr-ncsu/STIR_SHAKEN_Certificates. The repository contains the certificates themselves, without call-level records, telephone numbers, or mappings that could reveal relationships between certificates and PII-bearing signaling data.

Acknowledgments

The authors thank the shepherd and the anonymous reviewers for their constructive comments and insights, which strengthened this work. We thank Bandwidth Inc. for providing VoIP service, metadata, and telephone numbers to the Robocall Observatory, which made this study possible. We also thank David Frankel and ZipDX for sharing data, and Alex Nahapetyan and Moshe Ikechukwu for their assistance with code review.

This material is based upon work supported by the National Science Foundation under Grant No. CNS-2142930 and was partially supported by funds from the 2020 Internet Defense Prize. Any opinions, findings, conclusions, or recommendations expressed in this material are those of the authors and do not necessarily reflect the views of the National Science Foundation or other financial supporters.

References

[1] David Adei, Varun Madathil, Sathvik Prasad, Bradley Reaves, and Alessandra Scafuro. 2024. Jäger: Automated Telephone Call Traceback. In *Proceedings of the 2024 on ACM SIGSAC Conference on Computer and Communications Security* (Salt Lake City, UT, USA) *(CCS '24)*. Association for Computing Machinery, New York, NY, USA, 2042–2056. doi:10.1145/3658644.3690290

[2] David Adei, Varun Madathil, Bradley Reaves, et al. 2025. Secure and Efficient Out-of-band Call Metadata Transmission. *arXiv preprint arXiv:2509.12582* (2025).

[3] Devdatta Akhawe, Johanna Amann, Matthias Vallentin, and Robin Sommer. 2013. Here's my cert, so trust me, maybe? understanding TLS errors on the web. In *Proceedings of the 22nd International Conference on World Wide Web* (Rio de Janeiro, Brazil) *(WWW '13)*. Association for Computing Machinery, New York, NY, USA, 59–70. doi:10.1145/2488388.2488395

[4] Alliance for Telecommunications Industry Solutions (ATIS). [n. d.]. Signature-based Handling of Asserted Information Using toKENs (SHAKEN): Governance Authority and Policy Administrator. https://access.atis.org/higherlogic/ws/public/download/45033/ATIS-1000081.pdf. ATIS-1000081; Accessed: 2026-04-26.

[5] Alliance for Telecommunications Industry Solutions (ATIS). 2019. ATIS-1000082.v002: Technical Report on SHAKEN API for a Centralized Signing and Signature Validation Server (Revision 1). ATIS Technical Report. https://access.atis.org/higherlogic/ws/public/document?document_id=65715.

[6] Alliance for Telecommunications Industry Solutions (ATIS). 2020. *ATIS-1000091, Mechanism for International Signature-based Handling of Asserted information using toKENs (SHAKEN).* Technical Report ATIS-1000091. Alliance for Telecommunications Industry Solutions, Washington, DC, USA. https://access.atis.org/higherlogic/ws/public/document?document_id=54501

[7] Alliance for Telecommunications Industry Solutions (ATIS). 2022. *ATIS-1000087.v002, Mechanism for Initial Cross-Border Signature-based Handling of Asserted information using toKENs (SHAKEN).* Technical Report ATIS-1000087.v002. Alliance for Telecommunications Industry Solutions, Washington, DC, USA. https://access.atis.org/higherlogic/ws/public/document?document_id=75191

[8] Alliance for Telecommunications Industry Solutions (ATIS). 2023. ATIS-1000074.003: Signature-based Handling of Asserted information using toKENs (SHAKEN). ATIS Standard. https://access.atis.org/higherlogic/ws/public/document?document_id=67436.

[9] Alliance for Telecommunications Industry Solutions (ATIS) / ATIS/SIP Forum IP-NNI Task Force. 2025. ATIS-1000080.v006: Signature-based Handling of Asserted Information using toKENs (SHAKEN): Governance Model and Certificate Management (Revision 5). ATIS Workspace Public Document. https://access.atis.org/higherlogic/ws/public/document?document_id=82892&wg_id=8ba10810-ca63-4d03-8155-018d2489bfb6.

[10] ATIS. 2017. *ATIS-1000088: A Framework for SHAKEN Attestation and Origination Identifier.* Technical Report. ATIS.

[11] ATIS Secure Telephone Identity Governance Authority. 2025. STI-GA: Secure Telephone Identity Governance Authority. STI-GA Official Website. https://sti-ga.atis.org/.

[12] Josh Brown, Paul Grubbs, and Matthew Hardeman. 2026. STIR/SHAKEN: A Cocktail of Cryptographic Clumsiness . In *2026 IEEE Symposium on Security and Privacy (SP)*. IEEE Computer Society, Los Alamitos, CA, USA, 1725–1744. doi:10.1109/SP63933.2026.00093

[13] Andrew Chi, Brandon Enright, and David McGrew. 2023. Detecting Weak Keys in Manufacturing Certificates: A Case Study. In *Proceedings of the 39th Annual Computer Security Applications Conference* (Austin, TX, USA) *(ACSAC '23)*. Association for Computing Machinery, New York, NY, USA, 759–771. doi:10.1145/3627106.3627120

[14] Taejoong Chung, Emile Aben, Tim Bruijnzeels, Balakrishnan Chandrasekaran, David Choffnes, Dave Levin, Bruce M. Maggs, Alan Mislove, Roland van Rijswijk-Deij, John Rula, and Nick Sullivan. 2019. RPKI is Coming of Age: A Longitudinal Study of RPKI Deployment and Invalid Route Origins. In *Proceedings of the Internet*

Measurement Conference (Amsterdam, Netherlands) *(IMC '19)*. Association for Computing Machinery, New York, NY, USA, 406–419. https://doi.org/10.1145/3355369.3355596

[15] Taejoong Chung, Yabing Liu, David Choffnes, Dave Levin, Bruce MacDowell Maggs, Alan Mislove, and Christo Wilson. 2016. Measuring and Applying Invalid SSL Certificates: The Silent Majority. In *Proceedings of the 2016 Internet Measurement Conference* (Santa Monica, California, USA) *(IMC '16)*. Association for Computing Machinery, New York, NY, USA, 527–541. doi:10.1145/2987443.2987454

[16] Taejoong Chung, Roland van Rijswijk-Deij, Balakrishnan Chandrasekaran, David Choffnes, Dave Levin, Bruce M. Maggs, Alan Mislove, and Christo Wilson. 2017. A Longitudinal, End-to-End View of the DNSSEC Ecosystem. In *26th USENIX Security Symposium (USENIX Security 17)*. USENIX Association, Vancouver, BC, 1307–1322. https://www.usenix.org/conference/usenixsecurity17/technical-sessions/presentation/chung

[17] Jeremy Clark and Paul C. van Oorschot. 2013. SoK: SSL and HTTPS: Revisiting Past Challenges and Evaluating Certificate Trust Model Enhancements. In *2013 IEEE Symposium on Security and Privacy*. 511–525. doi:10.1109/SP.2013.41

[18] David Cooper, Stefan Santesson, Stephen Farrell, Sharon Boeyen, Russ Housley, and Tim Polk. 2008. Internet X.509 Public Key Infrastructure Certificate and Certificate Revocation List (CRL) Profile. RFC 5280. https://datatracker.ietf.org/doc/html/rfc5280.

[19] Ram Dantu and Prakash Kolan. 2005. Detecting Spam in VoIP Networks. In *Steps to Reducing Unwanted Traffic on the Internet Workshop (SRUTI 05)*. USENIX Association, Cambridge, MA. https://www.usenix.org/conference/sruti-05/detecting-spam-voip-networks

[20] Kyzer R. Davis, Brad Peabody, and P. Leach. 2024. Universally Unique IDentifiers (UUIDs). RFC 9562. doi:10.17487/RFC9562

[21] Zakir Durumeric, James Kasten, Michael Bailey, and {J. Alex} Halderman. 2013. Analysis of the HTTPS certificate ecosystem. In *IMC 2013 - Proceedings of the 13th ACM Internet Measurement Conference (Proceedings of the ACM SIGCOMM Internet Measurement Conference, IMC)*. 291–303. doi:10.1145/2504730.2504755 Copyright: Copyright 2014 Elsevier B.V., All rights reserved.; 13th ACM Internet Measurement Conference, IMC 2013 ; Conference date: 23-10-2013 Through 25-10-2013.

[22] dw. 2024. German police bust Europe's 'largest' scam call center – DW – 05/02/2024. https://www.dw.com/en/german-police-bust-europes-largest-scam-call-center/a-68980954

[23] Federal Communications Commission. [n. d.]. National Do Not Call Registry. https://www.donotcall.gov/. FTC.

[24] Federal Communications Commission. 2019. FCC Mandates STIR/SHAKEN to Combat Spoofed Robocalls. https://www.fcc.gov/document/fcc-mandates-stirshaken-combat-spoofed-robocalls. Accessed: 2026-04-26.

[25] Federal Communications Commission. 2019. Report and Order and Further Notice of Proposed Rulemaking: Call Authentication Trust Anchor. FCC Report and Order, WC Docket No. 17–97. https://docs.fcc.gov/public/attachments/DOC-362932A1.pdf.

[26] Federal Communications Commission. 2022. FCC Announces Effective Date for Providers to Block Calls from Do-Not-Originate Lists. https://www.fcc.gov/document/fcc-announces-effective-date-providers-block-dno-list. Accessed: 2026-04-25.

[27] Federal Communications Commission. 2024. Call Authentication Trust Anchor; Implementation of TRACED Act Section 6(a) — Sixth Report and Order. https://docs.fcc.gov/public/attachments/DOC-414073A1.pdf. FCC 24-24; Released March 2024.

[28] Federal Communications Commission. 2025. Call Authentication Trust Anchor. Federal Register, 90 FR (Aug. 19, 2025). https://www.federalregister.gov/documents/2025/08/19/2025-15809/call-authentication-trust-anchor.

[29] Federal Communications Commission. 2025. FCC Robocall Mitigation Database Portal. FCC ServiceNow Portal. https://fccprod.servicenowservices.com/rmd?id=rmd_welcome.

[30] Jens Friess, Haya Schulmann, and Michael Waidner. 2023. Revocation Speedrun: How the WebPKI Copes with Fraudulent Certificates. *Proc. ACM Netw.* 1, CoNEXT3, Article 26 (Nov. 2023), 20 pages. doi:10.1145/3629148

[31] Katia Gonzalez. 2023. *Thinking Beyond STIR/SHAKEN: What Can Enterprises Do Today to Fight Robocalls?* BICS. https://www.bics.com/blog/blog-robocalls-stir-shaken/ Accessed: 2026-04-17.

[32] GSMA Foundry. 2026. Open Verifiable Calling. https://www.gsma.com/solutions-and-impact/technologies/security/scams/gsma_resources/open-verifiable-calling-innovations-to-restoring-trust-in-voice-communications/. Accessed: 2026-04-28.

[33] Ralph Holz, Lothar Braun, Nils Kammenhuber, and Georg Carle. 2011. The SSL landscape: a thorough analysis of the x.509 PKI using active and passive measurements. In *Proceedings of the 2011 ACM SIGCOMM Conference on Internet Measurement Conference* (Berlin, Germany) *(IMC '11)*. Association for Computing Machinery, New York, NY, USA, 427–444. doi:10.1145/2068816.2068856

[34] iconectiv. [n. d.]. iconectiv STIR/SHAKEN Authentication Services. https://authenticate.iconectiv.com/.

[35] IETF. [n. d.]. IETF. https://www.ietf.org/.

[36] Industry Traceback Group. 2026. Tracebacks.org. https://tracebacks.org/. Accessed: 2026-04-26.

[37] Internet Engineering Task Force (IETF). [n. d.]. STIR Working Group (Secure Telephone Identity Revisited). https://datatracker.ietf.org/group/stir/about/. Accessed: 2026-04-27.

[38] Skyler Johnson, Katherine Ferro, L. Jean Camp, and Hilda Hadan. 2021. Human and Organizational Factors in Public Key Certificate Authority Failures. In *Proceedings of the 2021 ACM SIGSAC Conference on Computer and Communications Security* (Virtual Event, Republic of Korea) *(CCS '21)*. Association for Computing Machinery, New York, NY, USA, 2414–2416. doi:10.1145/3460120.3485360

[39] Michael Jones, John Bradley, and Nat Sakimura. 2015. JSON Web Algorithms (JWA). RFC 7518. https://datatracker.ietf.org/doc/html/rfc7518.

[40] Michael B. Jones, John Bradley, and Nat Sakimura. 2015. JSON Web Token (JWT). RFC 7519. doi:10.17487/RFC7519

[41] Doowon Kim, Haehyun Cho, Yonghwi Kwon, Adam Doupé, Sooel Son, Gail-Joon Ahn, and Tudor Dumitras. 2021. Security Analysis on Practices of Certificate Authorities in the HTTPS Phishing Ecosystem. In *Proceedings of the 2021 ACM Asia Conference on Computer and Communications Security* (Virtual Event, Hong Kong) *(ASIA CCS '21)*. Association for Computing Machinery, New York, NY, USA, 407–420. doi:10.1145/3433210.3453100

[42] Doowon Kim, Bum Jun Kwon, Kristián Kozák, Christopher Gates, and Tudor Dumitras. 2018. The Broken Shield: Measuring Revocation Effectiveness in the Windows Code-Signing PKI. In *27th USENIX Security Symposium (USENIX Security 18)*. USENIX Association, Baltimore, MD, 851–868. https://www.usenix.org/conference/usenixsecurity18/presentation/kim

[43] James Larisch, David Choffnes, Dave Levin, Bruce M. Maggs, Alan Mislove, and Christo Wilson. 2017. CRLite: A Scalable System for Pushing All TLS Revocations to All Browsers. In *2017 IEEE Symposium on Security and Privacy (SP)*. 539–556. doi:10.1109/SP.2017.17

[44] Huichen Li, Xiaojun Xu, Chang Liu, Teng Ren, Kun Wu, Xuezhi Cao, Weinan Zhang, Yong Yu, and Dawn Song. 2018. A Machine Learning Approach to Prevent Malicious Calls over Telephony Networks. In *2018 IEEE Symposium on Security and Privacy (SP)*. 53–69. doi:10.1109/SP.2018.00034

[45] Jienan Liu, Babak Rahbarinia, Roberto Perdisci, Haitao Du, and Li Su. 2018. Augmenting Telephone Spam Blacklists by Mining Large CDR Datasets. In *Proceedings of the 2018 on Asia Conference on Computer and Communications Security* (Incheon, Republic of Korea) *(ASIACCS '18)*. Association for Computing Machinery, New York, NY, USA, 273–284. doi:10.1145/3196494.3196553

[46] Yabing Liu, Will Tome, Liang Zhang, David Choffnes, Dave Levin, Bruce Maggs, Alan Mislove, Aaron Schulman, and Christo Wilson. 2015. An End-to-End Measurement of Certificate Revocation in the Web's PKI. In *Proceedings of the 2015 Internet Measurement Conference (IMC '15)*. Association for Computing Machinery, New York, NY, USA. doi:10.1145/2815675.2815685

[47] Zane Ma, James Austgen, Joshua Mason, Zakir Durumeric, and Michael Bailey. 2021. Tracing your roots: exploring the TLS trust anchor ecosystem. In *Proceedings of the 21st ACM Internet Measurement Conference (IMC '21)*. Association for Computing Machinery, New York, NY, USA. doi:10.1145/3487552.3487813

[48] Zane Ma, Aaron Faulkenberry, Thomas Papastergiou, Zakir Durumeric, Michael D. Bailey, Angelos D. Keromytis, Fabian Monrose, and Manos Antonakakis. 2023. Stale TLS Certificates: Investigating Precarious Third-Party Access to Valid TLS Keys. In *Proceedings of the 2023 ACM on Internet Measurement Conference* (Montreal QC, Canada) *(IMC '23)*. Association for Computing Machinery, New York, NY, USA. doi:10.1145/3618257.3624802

[49] Najmeh Miramirkhani, Oleksii Starov, and Nick Nikiforakis. 2017. Dial One for Scam: A Large-Scale Analysis of Technical Support Scams. In *Proceedings 2017 Network and Distributed System Security Symposium*. Internet Society. doi:10.14722/ndss.2017.23163

[50] Shishir Nagaraja and Ryan Shah. 2021. VoIPLoc: passive VoIP call provenance via acoustic side-channels. In *Proceedings of the 14th ACM Conference on Security and Privacy in Wireless and Mobile Networks* (Abu Dhabi, United Arab Emirates) *(WiSec '21)*. Association for Computing Machinery, New York, NY, USA, 323–334. doi:10.1145/3448300.3467816

[51] National Institute of Standards and Technology (NIST). [n. d.]. RPKI Monitor: Route Origin Validation (ROV) - AS 4. https://rpki-monitor.antd.nist.gov/ROV/A/4. Accessed: 2026-04-28.

[52] Ravi Netravali, Vikram Nathan, James Mickens, and Hari Balakrishnan. 2018. Vesper: Measuring Time-to-Interactivity for Web Pages. In *15th USENIX Symposium on Networked Systems Design and Implementation (NSDI 18)*. USENIX Association, Renton, WA, 217–231. https://www.usenix.org/conference/nsdi18/presentation/netravali-vesper

[53] Sharbani Pandit, Jienan Liu, Roberto Perdisci, and Mustaque Ahamad. 2021. Applying Deep Learning to Combat Mass Robocalls. In *2021 IEEE Security and Privacy Workshops (SPW)*. 63–70. doi:10.1109/SPW53761.2021.00018

[54] Sharbani Pandit, Krishanu Sarker, Roberto Perdisci, Mustaque Ahamad, and Diyi Yang. 2023. Combating Robocalls with Phone Virtual Assistant Mediated Interaction. In *32nd USENIX Security Symposium (USENIX Security 23)*. USENIX Association, Anaheim, CA, 463–479. https://www.usenix.org/conference/usenixsecurity23/presentation/pandit

[55] Jon Peterson. 2014. Secure Telephone Identity Threat Model. RFC 7375. doi:10.17487/RFC7375
[56] Jon Peterson. 2024. *Out-of-Band STIR for Service Providers.* Internet-Draft draft-ietf-stir-servprovider-oob-06. Internet Engineering Task Force. https://datatracker.ietf.org/doc/draft-ietf-stir-servprovider-oob/06/ Work in Progress.
[57] Jon Peterson, Cullen Fluffy Jennings, and Mark Watson. 2002. Private Extensions to the Session Initiation Protocol (SIP) for Asserted Identity within Trusted Networks. RFC 3325. doi:10.17487/RFC3325
[58] Jon Peterson, Henning Schulzrinne, and Hannes Tschofenig. 2018. Authenticated Identity Management in the Session Initiation Protocol (SIP). RFC 8224. https://datatracker.ietf.org/doc/rfc8224/.
[59] Sathvik Prasad, Elijah Bouma-Sims, Athishay Kiran Mylappan, and Bradley Reaves. 2020. Who's Calling? Characterizing Robocalls through Audio and Metadata Analysis. In *29th USENIX Security Symposium (USENIX Security 20)*. USENIX Association, 397–414. https://www.usenix.org/conference/usenixsecurity20/presentation/prasad
[60] Sathvik Prasad, Trevor Dunlap, Alexander Ross, and Bradley Reaves. 2023. Diving into Robocall Content with SnorCall. In *32nd USENIX Security Symposium (USENIX Security 23)*. USENIX Association, Anaheim, CA, 427–444. https://www.usenix.org/conference/usenixsecurity23/presentation/prasad
[61] Sathvik Prasad, Aleksandr Nahapetyan, and Bradley Reaves. 2025. Characterizing Robocalls with Multiple Vantage Points. In *2025 IEEE Symposium on Security and Privacy (SP)*. 19–36. doi:10.1109/SP61157.2025.00096
[62] Bradley Reaves, Logan Blue, Hadi Abdullah, Luis Vargas, Patrick Traynor, and Thomas Shrimpton. 2017. AuthentiCall: Efficient Identity and Content Authentication for Phone Calls. In *26th USENIX Security Symposium (USENIX Security 17)*. USENIX Association, Vancouver, BC, 575–592. https://www.usenix.org/conference/usenixsecurity17/technical-sessions/presentation/reaves
[63] Bradley Reaves, Logan Blue, and Patrick Traynor. 2016. AuthLoop: End-to-End Cryptographic Authentication for Telephony over Voice Channels. In *25th USENIX Security Symposium (USENIX Security 16)*. USENIX Association, Austin, TX, 963–978. https://www.usenix.org/conference/usenixsecurity16/technical-sessions/presentation/reaves
[64] Richard Roberts, Yaelle Goldschlag, Rachel Walter, Taejoong Chung, Alan Mislove, and Dave Levin. 2019. You Are Who You Appear to Be: A Longitudinal Study of Domain Impersonation in TLS Certificates. In *Proceedings of the 2019 ACM SIGSAC Conference on Computer and Communications Security* (London, United Kingdom) *(CCS '19)*. Association for Computing Machinery, New York, NY, USA, 2489–2504. doi:10.1145/3319535.3363188
[65] Richard Roberts and Dave Levin. 2019. When Certificate Transparency Is Too Transparent: Analyzing Information Leakage in HTTPS Domain Names. In *Proceedings of the 18th ACM Workshop on Privacy in the Electronic Society* (London, United Kingdom) *(WPES'19)*. Association for Computing Machinery, New York, NY, USA, 87–92. doi:10.1145/3338498.3358655
[66] RRAPTOR Project. 2024. What is RRAPTOR? RRAPTOR Project Website. https://rraptor.org/what-is-rraptor/.
[67] Secure Telephone Identity Governance Authority. 2026. *2025 STI-GA SHAKEN Report.* Public Report. Secure Telephone Identity Governance Authority. https://cdn.atis.org/sti-ga.atis.org/2026/02/20165621/2025-STIGA-Public-Report-Final.pdf
[68] Hemant Sengar. 2014. VoIP Fraud: Identifying a Wolf in Sheep's Clothing. In *Proceedings of the 2014 ACM SIGSAC Conference on Computer and Communications Security* (Scottsdale, Arizona, USA) *(CCS '14)*. Association for Computing Machinery, New York, NY, USA, 334–345. doi:10.1145/2660267.2660284
[69] Xiaofeng Shi, Shouqian Shi, Minmei Wang, Jonne Kaunisto, and Chen Qian. 2021. On-device IoT Certificate Revocation Checking with Small Memory and Low Latency. In *Proceedings of the 2021 ACM SIGSAC Conference on Computer and Communications Security* (Virtual Event, Republic of Korea) *(CCS '21)*. Association for Computing Machinery, New York, NY, USA, 1118–1134. doi:10.1145/3460120.3484580
[70] Transaction Network Services. 2026. *2026 Half-Year Robocall Investigation Report.* Industry Report. Transaction Network Services. https://tnsi.com/wp-content/uploads/2026/07/TNS_2026_HalfYear_Robocall-Report_US_FINAL-1.pdf
[71] TransNexus. 2026. STIR/SHAKEN Statistics from July 2026. https://transnexus.com/blog/2026/shaken-statistics-july/
[72] Truecaller. 2024. The True Cost of Spam and Scam Calls in America. https://www.truecaller.com/blog/insights/the-true-cost-of-spam-and-scam-calls-in-america Accessed: 2024-09-24.
[73] Truecaller. 2026. Truecaller. truecaller Website. https://www.truecaller.com/.
[74] Daniele Ucci, Roberto Perdisci, Jaewoo Lee, and Mustaque Ahamad. 2020. Towards a Practical Differentially Private Collaborative Phone Blacklisting System. In *Proceedings of the 36th Annual Computer Security Applications Conference* (Austin, USA) *(ACSAC '20)*. Association for Computing Machinery, New York, NY, USA, 100–115. doi:10.1145/3427228.3427239
[75] Martin Ukrop, Lydia Kraus, and Vashek Matyas. 2020. Will You Trust This TLS Certificate? Perceptions of People Working in IT (Extended Version). *Digital Threats* 1, 4 (Dec. 2020). doi:10.1145/3419472
[76] U.S. Congress. 2019. Pallone-Thune Telephone Robocall Abuse Criminal Enforcement and Deterrence Act. Public Law 116–105, 133 Stat. 3274 (Dec. 30, 2019). https://www.congress.gov/116/statute/STATUTE-133/STATUTE-133-Pg3274.pdf.
[77] Benjamin VanderSloot, Johanna Amann, Matthew Bernhard, Zakir Durumeric, Michael Bailey, and J. Alex Halderman. 2016. Towards a Complete View of the Certificate Ecosystem. In *Proceedings of the 2016 Internet Measurement Conference* (Santa Monica, California, USA) *(IMC '16)*. Association for Computing Machinery, New York, NY, USA. doi:10.1145/2987443.2987462
[78] Chris Wendt and Mary Barnes. 2019. Personal Assertion Token (PaSSporT) Extension for Signature-based Handling of Asserted information using toKENs (SHAKEN). RFC 8588. doi:10.17487/RFC8588
[79] Chris Wendt, Richard Barnes, Phil Sedlacek, Jon Peterson, and Chris Romano. 2018. PASSporT: Personal Assertion Token. RFC 8225. https://datatracker.ietf.org/doc/html/rfc8225.
[80] Chris Wendt, Eric Rescorla, Jon Peterson, and Henning Schulzrinne. 2018. Secure Telephone Identity Credentials: Certificates. RFC 8226. https://datatracker.ietf.org/doc/html/rfc8226.
[81] Wikipedia contributors. 2025. HTTPS. Wikipedia, The Free Encyclopedia. https://en.wikipedia.org/wiki/HTTPS.
[82] Daegeun Yoon, Taejoong Chung, and Yongdae Kim. 2023. Delegation of TLS Authentication to CDNs using Revocable Delegated Credentials. In *Proceedings of the 39th Annual Computer Security Applications Conference* (Austin, TX, USA) *(ACSAC '23)*. Association for Computing Machinery, New York, NY, USA, 113–123. doi:10.1145/3627106.3627144

A Ethics

Ethics and Data Protection

This study was reviewed and approved by our University IRB. Our data partners did not initiate calls or interfere with call delivery. Our dataset contains telephone numbers and call-signaling data, including PASSporTs, that may constitute personally identifiable information (PII). Calling numbers were used only for aggregate analyses, and we did not attempt to identify subscribers or individual callers.

Data Protection and Data Sharing Our agreements with partner providers prohibit us from sharing the call-signaling data and, by extension, the associated PASSporT and provider-generated verification-status (*verstat*) data. Our data is stored on-site and meets institutional data-protection requirements. Access is restricted to researchers only.

Risk and research value. The primary risks of this study are the potential disclosure of caller information and the possibility that provider-specific findings could create reputational or operational consequences. We mitigate these risks through access restrictions, aggregate analysis, non-disclosure of call-level records, and responsible disclosure of relevant findings to affected providers. The study does not expose individuals to additional calls or alter their telephone service. We believe these limited and mitigated risks are justified by the value of independently assessing a security framework deployed across critical communications infrastructure, particularly within unsolicited traffic that S/S was designed in part to address.

We further reviewed and adhered to the IMC's ethical guidelines. Our measurement and analysis are data-driven, unbiased, and conducted with a focus on responsible and ethical research practices.

B Validation Pipeline

We are elaborating our method section here with following three tables describing checkpoints used in the validation process.

CP	Category	Validation Check	Reference
1	PASSporT	The originating number in the JWT matches the SIP P-Asserted-Identity (PAID).	ATIS-1000074
2	PASSporT	When PAID is absent, the JWT originating number matches the SIP From number.	ATIS-1000074
3	PASSporT	The SIP PAID and SIP From numbers are consistent with each other.	ATIS-1000074
4	PASSporT	The called number in SIP follows valid E.164 formatting.	ATIS-1000074
5	PASSporT	The destination number in the JWT matches the SIP called number.	ATIS-1000074
6	PASSporT	The certificate URL (`x5u`) in the SIP header matches the URL in the JWT header.	ATIS-1000074
7	PASSporT	The `x5u` URL uses HTTPS and a secure port (e.g., 443 or 8443).	ATIS-1000074
8	PASSporT	The `x5u` URL does not contain insecure components, such as query strings or fragments.	ATIS-1000074
9	PASSporT	The `x5u` URL does not rely on HTTP redirection.	ATIS-1000074
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-1000074
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-1000074
14	PASSporT	The destination type in the JWT is specified as a telephone number (`tn`).	ATIS-1000074
15	PASSporT	The JWT issuance time is within an acceptable window (e.g., within one minute of the call).	ATIS-1000074

Table 1: PASSporT and Call Data Compliance Checkpoints

CP	Category	Validation Check	Reference
16	Certificate	The certificate version is X.509 v3.	ATIS-1000080
17	Certificate	The certificate serial number is unique within the issuing authority.	ATIS-1000080
18	Certificate	The signature algorithm uses an approved ECDSA variant (e.g., SHA-256 or SHA-384).	ATIS-1000080
19	Certificate	The subject common name follows the format `SHAKEN <SPC>`.	ATIS-1000080
20	Certificate	The Service Provider Code (SPC) in the subject common name matches the value in the TNAuthList extension.	ATIS-1000080
21	Certificate	The certificate is valid at the time of the call (i.e., the call occurs after `notBefore`).	ATIS-1000080
22	Certificate	The certificate is not expired at the time of the call (i.e., the call occurs before `notAfter`).	ATIS-1000080
23	Certificate	The public-key algorithm is Elliptic Curve (EC).	ATIS-1000080
24	Certificate	The public-key size corresponds to an approved curve (e.g., 256 or 384 bits).	ATIS-1000080
25	Certificate	The public-key structure is valid and correctly encoded.	ATIS-1000080
26	Certificate	The certificate uses a valid NIST elliptic curve (P-256 or P-384).	ATIS-1000080
27	Certificate	The Subject Key Identifier (SKI) is derived from the public-key hash.	RFC 5280; ATIS-1000080
28	Certificate	The Authority Key Identifier (AKI) matches the issuer's key identifier.	ATIS-1000080
29	Certificate	The Key Usage extension is marked as critical.	ATIS-1000080
30	Certificate	The Key Usage value is appropriate: `digitalSignature` for an end-entity certificate or `keyCertSign` for a CA certificate.	ATIS-1000080
31	Certificate	The Basic Constraints extension is present and marked as critical.	ATIS-1000080
32	Certificate	The Basic Constraints extension correctly specifies the CA status (`TRUE` for a CA certificate and `FALSE` for an end-entity certificate).	ATIS-1000080
33	Certificate	The CRL Distribution Point is correctly specified for revocation checking.	ATIS-1000080
34	Certificate	The TNAuthList extension contains one valid SPC and no telephone numbers.	ATIS-1000080

Table 2: Certificate Structural Compliance Checkpoints

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-1000074
42	Cryptographic	The certificate chain is successfully validated against trusted authorities.	ATIS-1000074
43	Cryptographic	The PASSporT signature is successfully verified using the public key.	ATIS-1000074

Table 3: Cryptographic Integrity Checkpoints