

Sinergy Networks, LLC. RMD0018482

OVERVIEW:

Sinergy Networks is committed to meeting the requirements of the Robocall Mitigation Database. We have verified that the information in our CORES account is active/current regarding our FRN# 0023803117. We are revising to meet the deficiencies that were brought to our attention. I humbly ask for leniency in accepting this submittal and working with us to resolve any issues.

Sinergy Networks Robo-call Mitigation Program Description

- Sinergy Networks certifies that all calls it originates on its network are subject to a robocall mitigation program. In accordance with its robocall mitigation program:
- Sinergy Networks agrees that any prior certification has not been removed by Commission action and it has not been prohibited from filing in the RMD.
- Sinergy Networks has fully implemented STIR/SHAKEN on the Internet Protocol portions of its network.

Sinergy Networks uses a third-party provider, Momentum, for its STIR/SHAKEN implementation and frameworks. Below follows a description of:

1. The effective measures Sinergy Networks are taking to prevent new and renewing customers from originating illegal robocalls.
2. A description of any call analytic system(s) that it utilizes with PBXware.
3. A description of the procedures it is using to know its upstream providers

1. Call Filtering on Slave Tenant

STIR/SHAKEN Call Filtering works in a way where it is expected from providers to complete the whole process of Caller ID verification and pass a parameter value in the P-Asserted-Identity SIP header which is by default named 'verstat'. The users can reject calls depending on the value of the **verstat** parameter by enabling call filtering.

Enable Call Filtering option can be enabled per tenant and the user can choose the statuses for which he wants the calls to be rejected.

STIR/SHAKEN

PAI Header Parameter Name:

Pass PAI Header to UAD:

Enable Call Filtering:

Drop Calls with Verification Status:

This means that PBXware does not perform any kind of validation or call signing. It just checks if the value under the verstat parameter matches one of the values that are listed in the Drop Calls with Verification Status dropdown.

Here is an example of the PAI header verstat parameter.

P-Asserted-Identity: <sip:+1234567890;verstat=TN-Validation-Failed-B@xx.xxx.x.xxx:xxxx>.

It is also possible that the 'P-Asserted-Identity' header has one of the following values: 'TN-Validation-Passed', 'TN-Validation-Failed', or 'No-TN-Validation', while the level can be seen in a new header, for example: 'P-Attestation-Indicator: B'.

P-Asserted-Identity: <sip:+1234567890;verstat=TN-Validation-Failed@xx.xxx.x.xxx:xxxx>

P-Attestation-Indicator: B

In case a user selects 'TN-Validation-Failed-B' and 'No-TN-Validation' as values for 'Drop Calls with Verification Status', the call will be dropped as it matches 'TN-Validation-Failed' plus 'B'.

There are three options in the STIR/SHAKEN section that can be configured per Tenant Level:

- **PAI Header Parameter Name**

Set this field to a desired value

(E.g. 'verstat')

NOTE: This parameter is parsed for the caller ID validation and it is generally named 'verstat'. Other variations depend on the Trunk provider.

- **Enable Call Filtering**

Enable PBXware STIR/SHAKEN Call Filtering

(E.g. Yes/No)

- **Drop Calls with Verification status**

Select for which verification status calls will be dropped

(E.g. 'TN-Validation-Failed')

The PAI header value will be parsed and if the given parameter is set and contains any of the selected values from the 'Drop Calls with Verification status' list, the call will be dropped.

Please refer to the list of verification statuses:

- **No-TN-Validation**

- No validation was performed on the telephone number.

- Possible reasons: network limitations, non-participation in STIR/SHAKEN, or calls originating from legacy systems.
- **TN-Validation-Failed**
 - The validation process failed.
 - Indicates that the caller's identity could not be verified, suggesting a potential spoofed or illegitimate caller ID.
- **TN-Validation-Passed-B**
 - Indicates **Partial Attestation (B-level)**:
 - The originating network validated that the call originated from one of its subscribers or endpoints but could not confirm the actual telephone number used.
 - Trust level is moderate.
- **TN-Validation-Passed-C**
 - Indicates **Gateway Attestation (C-level)**:
 - The originating network knows only the source of the call (e.g., a gateway) but cannot authenticate the caller ID.
 - Trust level is low.
- **TN-Validation-Failed-A**
 - The validation failed for a call that should have had **Full Attestation (A-level)**.
 - Suggests that the caller ID was expected to be fully validated but couldn't be authenticated.
 - This is a stronger failure indication compared to general validation failure.
- **TN-Validation-Failed-B**
 - Validation failed for a call with **Partial Attestation (B-level)**.
 - Indicates issues in verifying the subscriber or endpoint within the network.
- **TN-Validation-Failed-C**
 - Validation failed for a call with **Gateway Attestation (C-level)**.
 - Indicates issues with even the minimal validation expected from the gateway level.

NOTE: Please note that verification statuses are case insensitive which means that all three of the following options are acceptable: 'No-TN-Validation', 'NO-TN-VALIDATION', and 'No-tn-Validation'.

This will only work for calls from Trunks.

Case #1

Enable Call Filtering: **Yes**

Drop Calls with Verification Status: **TN-Validation-Failed-B, No-TN-Validation**

Validate Incoming Calls: **No**

If we take a look at the CLI report we will see something like this:

STIR/SHAKEN Call Filtering enabled ...	200 result=1
get full variable \${PJSIP_HEADER(read,P-Asserted-Identity)}	200 result=1 (verstat=TN-Validation-Failed-B)
get full variable \${PJSIP_HEADER(read,P-Attestation-Indicator)}	200 result=1 ()
STIR/SHAKEN Caller ID verification failed with status 'TN-Validation-Failed-B' ...	200 result=1
get variable MASTER_CHANNEL(CF_LINE_UNAVAIL)	200 result=1 ()

In SNGREP we see the following:

Call flow for 9096967a-18a2-45f6-b40a-9880f63da989 (Color by Request/Response)

185.59.92.229:5060 → 185.59.92.136:5060

08:32:02.662859 → INVITE (SDP)

08:32:02.663711 → 180 Trying

08:32:03.014844 → 603 Decline

08:32:03.015243 → CANCEL

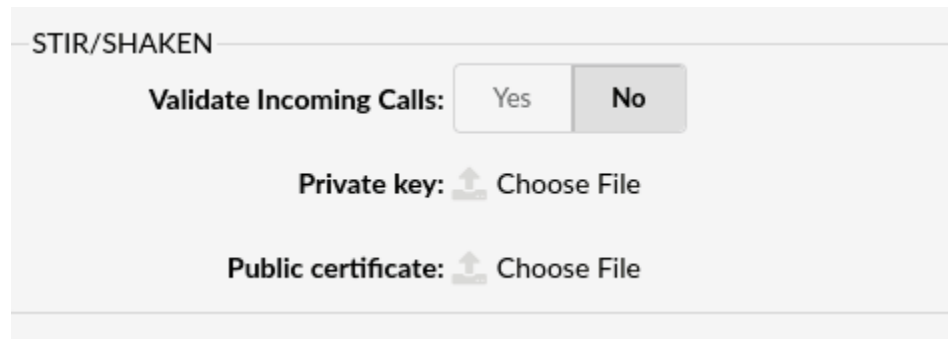
INVITE sip:44201122334455@185.59.92.136:5060 SIP/2.0
Via: SIP/2.0/UDP 185.59.92.229:5060;rport;branch=z9hG4bKPj3f9d5a31-399c-46d6-ab92-b1a85fcb4dc2
From: "AdisaMTv5" <sip:44201117777@185.59.92.229>;tag=a4a90ba3-36af-4c20-b4c2-39d03d3550ad
To: <sip:44201122334455@185.59.92.136>
Contact: <sip:asterisk@185.59.92.229:5060>
Call-ID: 9096967a-18a2-45f6-b40a-9880f63da989
CSeq: 28864 INVITE
Allow: OPTIONS, REGISTER, SUBSCRIBE, NOTIFY, PUBLISH, INVITE, ACK, BYE, CANCEL, UPDATE, PRACK, MESSAGE, REFER
Supported: 100rel, replaces, noferaub, histinfo
P-Asserted-Identity: <sip:12486303000;verstat=TN-Validation-Failed-B@4.55.42.227:5060>
Privacy: none
Max-Forwards: 70
User-Agent: Asterisk
Content-Type: application/sdp
Content-Length: 261
v=0
o=- 253058461 253058461 IN IP4 185.59.92.229
s=Asterisk
c=IN IP4 185.59.92.229
t=0 0
m=audio 14062 RTP/AVP 0 8 101
a=rtpmap:0 PCMU/8000
a=rtpmap:8 PCMA/8000
a=rtpmap:101 telephone-event/8000
a=fmt:101 0-16
a=ptime:20
a=maxptime:150
a=sendrecv

This indicates that the Call Filtering was enabled and in PAI there was 'TN-Validation-Failed-B' sent. As that value was set under filters to drop calls with that value in PAI, the call was dropped on the PBXware side.

2. Call validation on Master Tenant

Besides Call Filtering using the PAI header, PBXware also added its implementation of STIR/SHAKEN which allows signing and validating calls with valid STIR/SHAKEN certificates that customers own. These options are added on Master Tenant and in order to have these options, STIR/SHAKEN needs to be enabled in license.

The certificate that was obtained is uploaded to Master Tenant.



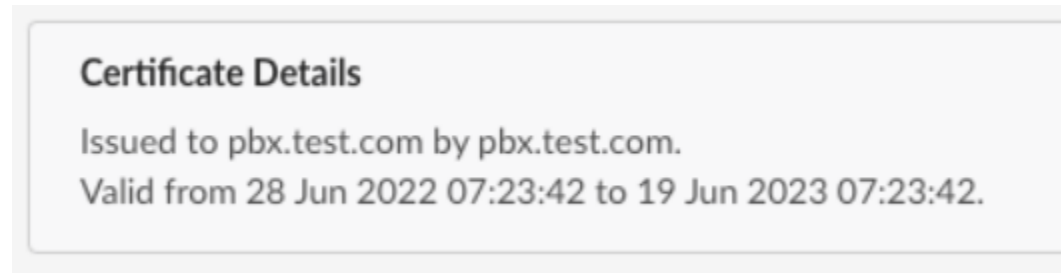
The screenshot shows a configuration panel titled "STIR/SHAKEN". Inside the panel, there is a section labeled "Validate Incoming Calls:" with two buttons: "Yes" and "No". The "No" button is currently selected. Below this, there are two fields for file uploads: "Private key:" and "Public certificate:". Each field has an upward arrow icon and the text "Choose File".

If the 'Validate Incoming Calls' option is set to 'Yes', the Identity header will be checked for incoming calls, and STIR/SHAKEN validation will be done. If the Identity header is not present or is invalid, the call will be dropped.

Please note that once the certificate and key are uploaded, they will be verified. If the verification fails (e.g. the certificate is invalid or a certificate/key pair is not correct), the following error message will be displayed:

Failed to verify that the uploaded certificate corresponds to the private key.
Please make sure to upload the correct certificate/key pair.

In case the verification is successful, users will be able to see more information including the certificate expiry date.



Case #2

Enable Call Filtering: **Yes**

Drop Calls with Verification Status: **TN-Validation-Failed-B, No-TN-Validation**

Validate Incoming Calls: **Yes**

In this case, the Call Filtering check will be executed first and after that, the Identity header will be checked. If the verstat parameter contains the same value in the PAI header as in the previous example (TN-Validation-Failed-B) the result will be the same, no matter if the Identity header is set or not. The call will be dropped because the PAI status matches the selected TN-Validation-Failed-B status.

STIR/SHAKEN Call Filtering enabled ...	200 result=1
get full variable \${PJSIP_HEADER(read,P-Asserted-Identity)}	200 result=1 ()
get full variable \${PJSIP_HEADER(read,P-Attestation-Indicator)}	200 result=1 ()
STIR/SHAKEN Caller ID verification failed with status 'No-TN-Validation' ...	200 result=1
get variable MASTER_CHANNEL(CF_LINE_UNAVAIL)	200 result=1 ()

Case #3

Enable Call Filtering: **Yes**

Drop Calls with Verification Status: **TN-Validation-Failed-C, No-TN-Validation**

Validate Incoming Calls: **Yes**

Let's say that the verstat value does not match any selected status and the Call Filtering does not result with rejecting the call. Here is an example of sngrep log:

INVITE sip:24843636000108.60.153.175:9395 SIP/2.0

Via: SIP/2.0/UDP64.136.173.31:5060;branch=z9hG4bKlsansav556738916rdb15303

Record-Route:<sip:sansay556738916rdb15303@64.136.173.31:5060;lr;transport=udp>

To:

<sip:

[2484363600](tel:2484363600)

@108.60.153.175>

From:

"VOIP OFFICE" <sip:

[12486303000](tel:12486303000)

@64.136.173.31>; tag=sansay556738916rdb15303

Call-ID:166140215-0-55328010@64.136.173.225

CSeg: 1 INVITE

Contact:

<sip:

[12486303000](tel:12486303000)

@64.136.173.31:5060>

Supported: timer

Session-Expires:1800;refresher=uac

Min-SE: 90

P-Asserted-Identity:

"VOIP OFFICE" <sip:

[+12486303000](tel:+12486303000)

```
;verstat-TN-Validation-Failed-B@4.55.42.227:5060>
```

[illegible]

Max-Forwards: 147

Content-Type: application/sdp

Content-Length: 299

In this case, after the PAI header check is completed and the call is not dropped, the incoming call validation will be executed (the Identity header will be checked). If the Identity header is not set or it is set but not valid, the call will be dropped and in asterisk log these messages can be seen:

*** MISSING ***

```
== agi://127.0.0.1:[1654699374.18] STIR/SHAKEN Call Filtering enabled ...
```

```
== agi://127.0.0.1: [1654699374.18] STIR/SHAKEN call check starting
```

```
== agi://127.0.0.1: [1654699374.18] Missing identity header, STIR/SHAKEN Caller ID verification failed
```

*** VALIDATION FAILED ***

```
== agi://127.0.0.1:[1654699374.18] STIR/SHAKEN Call Filtering enabled ...
```

```
== agi://127.0.0.1:[1654699374.18] STIR/SHAKEN call check starting
```

```
== agi://127.0.0.1: [1654699374.18] Validation request did not return valid value, STIR/SHAKEN
Caller ID verification failed
```

In case the validation is completed successfully the following messages will be in the asterisk log:

```
== agi://127.0.0.1:[1654699374.18] STIR/SHAKEN Call Filtering enabled ...
```

== agi://127.0.0.1: [1654699374.18] STIR/SHAKEN call check starting

== agi://127.0.0.1: [1654699374.18] STIR/SHAKEN check passed successfully

Call Signing

Based on the uploaded certificate the call will be signed and the Identity header will be set.

== agi://127.0.0.1: [1654699386.73] Setting SIP header 'Identity' ...

== agi://127.0.0.1: [1654699386.73] Setting SIP header 'Date' ...

If the certificate is missing the following message will be displayed in asterisk log:

agi://127.0.0.1: [1654693785.4] Could not find certificate file on this system, can't sign
STIR/SHAKEN call correctly

NOTE: In this case, the call will not be dropped, it will just not be signed (the Identity header will not be set).

Outbound calls

PBXware does not currently perform caller ID verification or signing based on its validation. However, if a valid certificate provided by the service provider is uploaded to PBXware, a hidden option can be enabled to ensure that all calls are signed with A-level attestation.

NOTE: A hidden option is available from 6.7.5 PBXware and before the mentioned version, a patch needs to be applied.

To verify that A-attestation is sent on the outbound call, the 'Identity header' needs to be obtained from the SIP trace and decoded. For decoding, we can use [JWT](#).

Here, we paste the Identity header and check the payload.

Encoded

PASTE A TOKEN HERE

```
eyJhbGciOiAiA1RVMYNTYiLCJwchQiOiAic2hha2V  
uIiwidHlwIjogInBhc3Nwb3J0IiwieDV1IjogIm  
h0dHBzOi8vY2VydG1maWNhdGVzLmNsZWYyaXAUy  
29tL2IxNWQ3Y2M5LTBmMjYtNDZjMi04M2VhLWEz  
ZTYzYTgyZWMzYS83Y2M0ZGI2OTVhMTN1ZGFkYTR  
kMMWY5ODYxYjliODBMZS5jcnQifQ.eyJhdHRlc3Q  
iOiAiQSIsImRlc3QiOiB7InRuIjogWyIxNDA0NT  
I2NjA2MCJdfSwiaWF0IjogMTU0ODg1OTk4Miwib  
3JpZyI6IHsidG4iOiAiMTgwMDEyMjcifSwi  
b3JpZ2lkIjogIjNhNDdjYTlzlWQ3YWItdNDQ2Yi0  
4MjFkLTZDVkZWVhYmVhNCJ9.S_vqkgCk88ee9  
rtk89P6a6ru0ncDfSrdB1GyK_mJj-10hsLW-  
dMF7eCjDYARLR7EZSZwi0fd4H_QD_9Z5U2bg;i  
nfo=  
<https://certificates.clearip.com/b15d7  
cc9-0f26-46c2-83ea-  
a3e63a82ec3a/7cc4db695d13edada4d1f9861b  
9b80fe.crt>alg=ES256;ppt=shaken
```

Decoded

EDIT THE PAYLOAD AND SECRET

HEADER: ALGORITHM & TOKEN TYPE

```
{  
  "alg": "ES256",  
  "ppt": "shaken",  
  "typ": "passport",  
  "x5u": "https://certificates.clearip.com/b15d7cc9-  
0f26-46c2-83ea-  
a3e63a82ec3a/7cc4db695d13edada4d1f9861b9b80fe.crt"  
}
```

PAYLOAD: DATA

```
{  
  "attest": "A",  
  "dest": {  
    "tn": [  
      "14045266060"  
    ]  
  },  
  "iat": 1548859982,  
  "orig": {  
    "tn": "18001234567"  
  },  
  "origid": "3a47ca23-d7ab-446b-821d-33d5deedbed4"  
}
```

VERIFY SIGNATURE

```
ECDSASHA256(  
  base64UrlEncode(header) + "." +  
  base64UrlEncode(payload),  
  Public Key in SPKI, PKCS #1,  
  X.509 Certificate, or JWK stri  
  ng format.
```

Sinergy Networks uses Momentum's PBXWare as a hosted third-party provider UCaSS solution provider for its' customer implementations. Below are descriptions of:

1. Monitoring
2. Traceback Cooperation with Bulk Solutions

Monitoring

Sinergy Networks, LLC. has monitoring and reporting systems in place to analyze high-volume voice network traffic to identify and monitor patterns consistent with robocalls. Our monitoring systems provide alerts on calling patterns with unusual spikes, traffic patterns, or attempted use of non-validated Telephone Number (TN) to detect patterns consistent with illegal robocalls.

If Sinergy Networks, LLC. detects a pattern consistent with illegal robocalls, or we have reason to suspect illegal robocalling or spoofing is taking place over our network, we will seek to identify the party that is using our network to originate, route, or terminate these calls. and take appropriate action.

Appropriate action may include:

- Validating that the originating party is authorized to use the TN.
- Suspending calling party's ability to originate, route, or terminate calls on Sinergy Networks, LLC. network.

Traceback Cooperation

Sinergy Networks, LLC. commits to responding in a timely manner and supporting all traceback requests from the FCC, law enforcement, and the [Industry Traceback Group \(ITG\)](#).

Bulk Solutions Robocall Mitigation Solution Overview

- General information
 - Robocall scoring is based on the annual +100B carrier calls that Bulk Solutions processes as part of the Caller Name service.
 - STIR/SHAKEN Transaction Detail Records (TDRs) are now being added as an additional data source.
 - Each call is assessed through the Bulk Solutions model, leading to constantly refreshed view of call behavior and probability of a given number currently being used for robocalling.
 - Active numbers are assessed by the model for behavioral attributes typically associated with robocalling including:
 - Neighbor spoofing events
 - Sudden spikes in volume, such as driven by call spoofing
 - Do-Not-Originate (DNO) numbers are also deemed to be robocalls if they are the calling party number. This is sourced from industry (e.g., US Telecom) and directly from enterprises.
 - The service covers both US domestic and international TNs. Sinergy Networks does not service International TNs.
- Calls originating from your network (i.e., Robocall Protection)
 - Provides detailed reporting identifying suspected illegal robocalls and alerts if calls originate where the calling number is invalid, unallocated, on a Do-Not-Originate list.
 - If the platform detects a suspected robocalling patterns Sinergy Networks, LLC. will take appropriate action which may include suspending or terminating the subscriber.
 - Supports a real time query to service to determine if a number originating on your network could be a robocall. Such calls can be blocked, or the terminating party can be notified via CNAM.
 - For each new instance of robocalling using the Operating Service Provider (OSP)TNs, an alert is sent to the OSP in near real time. This alert will result in the OSP (manually) blocking the TN and all TSPs being alerted via CNAM , through an overlay such as "ROBOCALLER". The CNAM alerting helps address instances of spoofing of TNs that are not going through the OSP that owns the number.
- Termination (i.e., Robocall Mitigation)

- Supports a real-time query to service to determine if a number terminating on your network could be a robocall. This protects subscribers from calls that come from networks that cannot authoritatively attest to the end user caller (i.e., all Communications Service Providers (CSPs) that do not have STIR/SHAKEN and all CSPs *with* STIR/SHAKEN, but who do not have a direct and vetted end user relationship.)
- Such calls can be blocked or the called party can be notified via CNAM.