How STIR/SHAKEN Functionality Works in VoipNow

Overview

What is STIR/SHAKEN

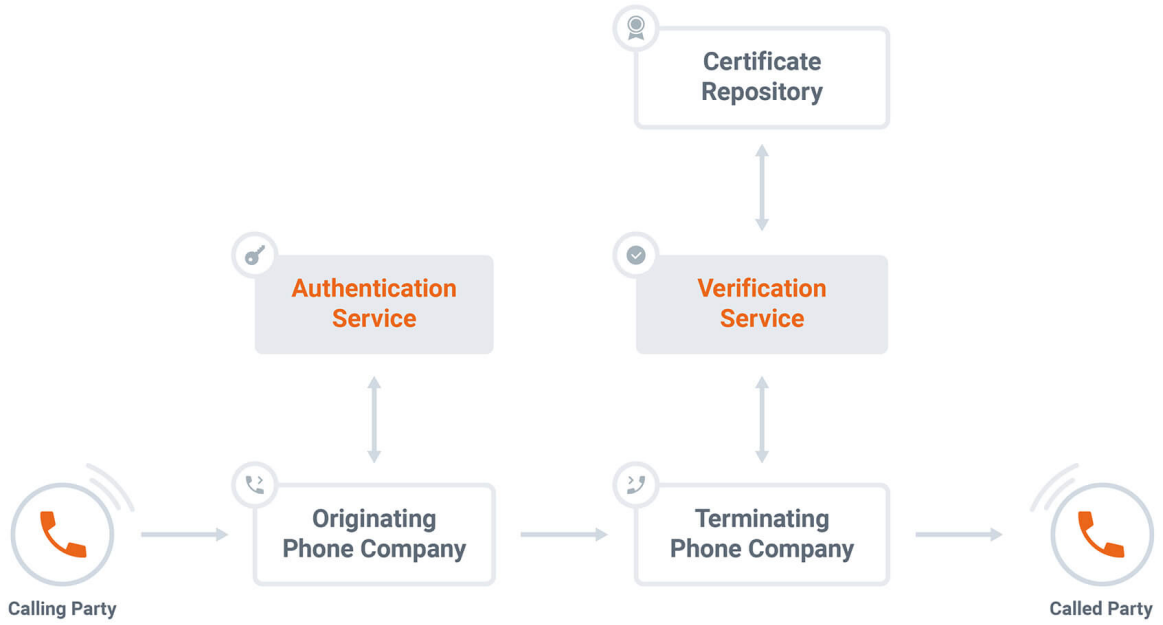
STIR/SHAKEN is a set of protocols and procedures intended to counteract caller ID spoofing on public telephone networks. Caller ID spoofing involves masking the caller's identity or making it appear that the call is coming from a legitimate source, such as a local phone number or a well-known organization. This type of spoofing is often used by robocallers and is common for calls made through voice-over-IP (VoIP) systems, which can be located anywhere in the world. **STIR**, or Secure Telephony Identity Revisited, is a protocol for providing calling party information with a digital signature that can be produced and verified at various locations. **SHAKEN**, or Secure Handling of Asserted information using Tokens, focuses on how **STIR** can be implemented within carrier networks and addresses deployability. While **STIR** focuses on end devices, **SHAKEN** focuses on the carrier network.

The following guide applies for VoipNow version 5.6.0 M1 or higher.

How STIR/SHAKEN works

STIR/SHAKEN uses digital certificates based on public key cryptography to ensure that the calling number of a telephone call is secure. In essence, each telephony service provider obtains a digital certificate from a trusted certificate authority, which allows the called party to verify that the calling number is legitimate and has not been faked. In simpler terms, the certificate technology enables the called party to confirm that the calling number is accurate and not a spoof.

The following call flow diagram illustrates how STIR/SHAKEN works.



1. The originating service provider receives a SIP Invite and determines how to certify the call:

- Full Attestation (A) - The service provider authenticates the calling party AND confirms they are authorized to use this number.
- Partial Attestation (B) - The service provider verifies the call origination but cannot confirm that the call source is authorized to use the calling number. An example would be a calling number from behind an enterprise PBX.
- Gateway Attestation (C) - The service provider authenticates the call's origin but cannot verify the source. An example would be a call received from an international gateway.

2. The service provider creates a SIP identity header and adds it to the Invite that it sends on the egress side.

3. The terminating service provider verifies the identity header and decides what to do with the call. It can also add a verstat string in the PAI header, which means that the call was already verified.

How STIR/SHAKEN works with VoipNow

For VoipNow, the authentication functionality is developed in Kamailio and the verification functionality is developed in Asterisk.

Call authentication

To be able to sign calls with an Identify Header you will need a private key and a certificate from an authorized STI-CA (Secure Telephone Identity Certification Authority). The list with approved certification authorities is published here. The process of obtaining the certificate may differ from one company from another, but all of them will require that the service provider has been assigned an OCN. Further details about the paper work that needs to be completed is available here.

You can verify if a private key matches the certificate with the following command.

```
openssl ec -in server.key -pubout | openssl md5
read EC key
writing EC key
(stdin)= 66d166c47e045425e1dcc4eb05aff896
openssl x509 -in server.crt -noout -pubkey | openssl md5
(stdin)= 66d166c47e045425e1dcc4eb05aff896
```

1. Copy the private key, which you generated with the help of your Certificate Administrator and make sure it has the correct permissions:

```
cp private_key.pem /etc/voipnow/certs/sip/priv-key.pem
chown kamailio:kamailio /etc/voipnow/certs/sip/priv-key.pem
ls -lrth /etc/voipnow/certs/sip/priv-key.pem
-rw-r--r--. 1 kamailio kamailio 302 Nov 15 13:54 /etc/voipnow/certs/sip/priv-key.pem
```

2.Edit the following lines in /etc/kamailio/kamailio.cfg to enable STIR/SHAKEN. The result should look like this.

```
# Enable/Disable stirshaken signing for outgoing calls
#!define ENABLE_STIR_SHAKEN
```

3.Make sure that the following lines in the kamailio.cfg include the correct path for the private key /etc/voipnow/certs/sip/priv-key.pem.

```
#!ifdef ENABLE_STIR_SHAKEN
modparam("stirshaken", "as_default_key", "/etc/voipnow/certs/sip/priv-key.pem")
#!endif
```

4. Edit the kamailio.cfg to add the URL from the Certificate Repository where your certificate is hosted. You will need to replace "url_to_be_added" with the URL provide by the CA.

```
# This is the url where the public certificate can be retrieved. If this is not set,the signing will fail.
 $var(cert_url)="url_to_be_added";
```

5.Restart the Kamailio service.

```
service kamailio restart
```

You should be able to see the identity header in an Invite if you make a test call:

```
Identity:
eyJhbGciOiJFUzI1NiIsInBwdCI6InNoYWtlbiIsInR5cCI6InBhc3Nwb3J0IiwieDV1IjoiMTAtMTUwLTkxLTEzNi40Z3JpZC5ldS9jZXJ0LnBlbSJ9.
eyJhdHRlc3QiOiJCIiwiZGVzdCI6eyJ0biI6WyI2MjYyNjIiXX0sImlhdCI6MTY2ODUyNjA2OCwib3JpZyI6eyJ0biI6IjU1NTU1NTUifSwib3JpZ2lkIjoiNTEwYjk4MTItNDk3Ny00NjU2LTg3ZDEtNGY3MjM0MDAxZTBjIn0.dUVr9JSmF9RN6VNtVw7oGmyAWLqQNp4W4qP6Lensc3et72BBE-Eya94eQNhoWGzTW_jau3oS69RMqBrtp7Ds9A;info=<teststirshaken.com/cert.pem>;alg=ES256;ppt=shaken
```

Verification

VoipNow will process all calls by default without taking into account if the Identity header is missing, present or fails the identity_check. The default action is set to PASS.

When a call arrives on the system, there are three possible identity_check outcomes:

- identity_missing - The Identity header is completely missing
- identity_check_ok - The Identity header contains a valid identity.
- identity_check_failed -The Identity header exists, but the identity is incomplete or invalid.

There are three actions the server can take :

- PASS - Just pass the call forward regardless of the identity check.
- STOP - Drop the call. In the call history, such a call will have the status NOT ALLOWED.
- ALERT - Alert the user by altering the callerid name. You can set values in [alert] section for every identity check outcome: missing_prefix, missing_suffix, check_ok_prefix, check_ok_suffix, check_failed_prefix, check_failed_suffix.

To change the default setup, you will need to follow these steps:

1.Go to file /etc/asterisk/stir_shaken.conf, section identity_check to specify behavior and setup PASS, STOP or ALERT according to your needs.

2.Restart the asterisk service:

```
service asterisk restart
```

3.Install chain root certificate from CA by copying the CA certificates that are found here in /etc/pki/ca-trust/source/anchors/.
A new certificate file needs to be created for every company name from the pdf file to make sure that calls signed with all the STI-CAs can be verified.
Below is an example for a root certificate named comcast.pem belonging to the Comcast company that has the correct format.

```
-----BEGIN CERTIFICATE-----
MIICNzCCAdygAwIBAgIJAOKHGyEWYfhOMAoGCCqGSM49BAMCMG4xCzAJBgNVBAYT
AlVTMRUwEwYDVQQIDAxQZW5uc3lsdmFuaWExFTATBgNVBAcMDFBoaWxhZGVscGhp
YTEQMA4GA1UECgwHQ29tY2FzdDEfMB0GA1UEAwwWQ29tY2FzdCBTSEFLRU4gUm9v
dCBDQTAeFw0yMDAzMTcxNDQ1MTVaFw00MDAzMTIxNDQ1MTVaMG4xCzAJBgNVBAYT
AlVTMRUwEwYDVQQIDAxQZW5uc3lsdmFuaWExFTATBgNVBAcMDFBoaWxhZGVscGhp
YTEQMA4GA1UECgwHQ29tY2FzdDEfMB0GA1UEAwwWQ29tY2FzdCBTSEFLRU4gUm9v
dCBDQTBZMBMGByqGSM49AgEGCCqGSM49AwEHA0IABJSzZzTeNhxovLtywhdzQU10
9JZLkcxXjBV9XB/jgfv9qy9ZJfcP7x9crjSbzBu1+IoG65Qgvg5FGz5W6XR1cKKj
YzBhMB0GA1UdDgQWBBSRkMqxhg5PFl6+tTdRP2l55SMbHDAfBgNVHSMEGDAWgBSR
kMqxhg5PFl6+tTdRP2l55SMbHDAPBgNVHRMBAf8EBTADAQH/MA4GA1UdDwEB/wQE
AwIBhjAKBggqhkjOPQQDAgNJADBGAiEAgfeTR2ucIDYaJvRyWW3VBUyhbAWVrAOQ
7ZhPQpJ+cY8CIQDYYvj3djJDGthqwmbJRyxjX3YpxuHsoHR8plf7bHN5dA==
-----END CERTIFICATE-----
```

4.Refresh the CA certificate used by the server:

```
update-ca-trust
```

5.Reload the asterisk stir shaken config:

```
asterisk -rx "stir_shaken reload"
```

In the asterisk console, you should be able to see something like this if the verification works:

```
VerifyIdentity("SIP/chan4-00000000",
"eyJhbGciOiJFUzI1NiIsInBwdCI6InNoYWtlbiIsInR5cCI6InBhc3Nwb3J0IiwieDV1IjoiMTAtMTUwLTkxLTEzNi40Z3JpZC5ldS9jZXJ0LnBlbSJ9.
eyJhdHRlc3QiOiJCIiwiZGVzdCI6eyJ0biI6WyI2MjYyNjIiXX0sImlhdCI6MTY2ODUyNDg4NSwib3JpZyI6eyJ0biI6IjU1NTU1NTUifSwib3JpZ2lkIjoiM2JlYzVjYjgtZjY3Yy00NDQ5LWFjYmMtZDgyOGU2OGJkMmRlIn0.
_U3L5VI_A1ZzaSP63CCXI0ozGpmBnEMp6q1nzMIUaxKUKAvniXba8MhztUslFalTLZdT9W_lXunN_fsjb8fsgA;info=<teststirshaken.com
/cert.pem>;alg=ES256;ppt=shaken,"5555555","626262"") in new stack
       > Executing [s@macro-stir-call:2] Set("SIP/chan4-00000000", "LOCAL(action)=PASS") in new stack
       > Executing [s@macro-stir-call:3] Set("SIP/chan4-00000000", "LOCAL(callerid_prefix)=") in new stack
       > Executing [s@macro-stir-call:4] Set("SIP/chan4-00000000", "LOCAL(callerid_suffix)=") in new stack
       > Executing [s@macro-stir-call:5] GotoIf("SIP/chan4-00000000", "0?check_failed") in new stack
  == Parsing '/etc/asterisk/stir_shaken.conf': Found
       > Executing [s@macro-stir-call:6] Set("SIP/chan4-00000000", "LOCAL(action)=PASS") in new stack
       > Executing [s@macro-stir-call:7] Set("SIP/chan4-00000000", "LOCAL(callerid_prefix)=(Verified)") in new
stack
       > Executing [s@macro-stir-call:8] Set("SIP/chan4-00000000", "LOCAL(callerid_suffix)=") in new stack
       > Executing [s@macro-stir-call:9] Set("SIP/chan4-00000000", "SECURITY_CHECK=AVAILABLE_PASS") in new stack
       > Executing [s@macro-stir-call:10] Goto("SIP/chan4-00000000", "check_end") in new stack
    -- Goto (macro-stir-call,s,26)
```