martini security

Martini Security
Enrolling for STIR/SHAKEN Certificates Using Olive

Version 1.0

Enrolling for STIR/SHAKEN Certificates Using Olive and Martini Security

Background

This document outlines the steps to enroll for a certificate using Olive, which is a Martini Security ACME (RFC 8555) and ATIS-1000080 client. Olive helps you enroll for a certificate by following the instructions in this document.

Sample Configuration Notes

The information provided in this document has been tested on Ubuntu Server 22 LTS using the latest packages available as of April 4, 2023.

Although not guaranteed, it is assumed that other Debian-based distributions or RHEL/Fedora systems may also be compatible. This guide assumes that the reader understands how to configure their SIP server to perform STIR/SHAKEN signing and verification and has familiarity with the ATIS STIR/SHAKEN specifications, which would be beneficial.

Getting Started

Before deploying, you must first create an account with Martini Security and obtain an API key. This process involves four steps:

1. Register for an account with Martini Security and acquire an API key.
2. Submit your FCC 499 filer ID.
3. Select a subscription plan and complete payment.
4. Have the registered 499 filer approve the request to represent their organization.

Account creation typically takes only a few minutes.

After registering, obtain your API key by copying the key and its ID, which will be used to configure STIR/SHAKEN.

For more information, watch this video: https://www.youtube.com/watch?v=CXvR-jyJVx4&t=1s

Additionally, you will need your STI-PA API credentials and OCN, which can be found in the credentials you created at iConectiv's STIR/SHAKEN provider portal.

Getting your first certificate

First, we need to install Olive. This is the Martini Security-developed command-line ACME client that will be used for ordering and renewing STIR/SHAKEN certificates.

```
wget https://storage.googleapis.com/martini-security/download/olive
chmod a+x olive
```

To simplify the process, let's configure two variables for the ACME credentials. These can be obtained after creating a new ACME client within the Martini Security web application.

```
export ACME_KEY_ID=<acme key id>
export ACME_KEY=<acme key>
```

Next, we need to register our ACME account.

```
olive acme register --key-id ${ACME_KEY_ID} --key ${ACME_KEY} \
--contact <your email> --agree-tos
```

This will create a hidden directory in your `$HOME` directory where we will need to store our STI-PA credentials for the certificate we are about to request.

```
cat <<EOF >> ~/.mrtsec/.stipa.yaml
```

```
user_id: <STI-PA API userid>
password: <STI-PA API password>
ocn: <your OCN>
EOF
```

Now we can request an SPC token and then order our first STIR/SHAKEN certificate.

```
olive stipa token --key-id ${ACME_KEY_ID} \
--config ~/.mrtsec/.stipa.yaml --out=/tmp/spc.json

olive acme order --key-id ${ACME_KEY_ID} --spc /tmp/spc.json
```

Within moments, we should have the certificate, key, and cert repository (X5U URL). Note that subsequent calls to order will automatically renew when the validity period is less than 7 days until expiry. An SPC token should always be requested before ordering or renewing a certificate.

Later on, we will script the auto-renewal and reload of signing cert data.

Scripting Certificate Renewal

When the certificate is close to expiring, we can automate the renewal and configuration reload using a shell script. Here is an example of such a script.

```
#!bin/bash

# You could choose to pass this in as a param…
ACME_KEY_ID=<acme key id>

# Clear and prep for ACME result
echo "" > /tmp/acme_result
ACME_RESULT=/tmp/acme_result

# Get an SPC Token and Proceed to attempt to renew cert
olive stipa token --key-id ${ACME_KEY_ID} --config ~/.mrtsec/.stipa.yaml \
  --out=/tmp/spc.json \
  && olive acme order --key-id ${ACME_KEY_ID} --spc /tmp/spc.json > $ACME_RESULT

# (continued on next page)
# If this failed, we will try again tomorrow
if [ $? -ne 0 ]
then
    exit
Fi

# Parse the output from Olive
```

```
while IFS=":" read -r key value; do
    case "$key" in
      "found valid certificate") valid=1 ;;
      "key") key="$value" ;;
      "repository") repo="$value" ;;
    esac
done < "$ACME_RESULT"

# If we are outside of 7 days of expiration, Olive informs us that we already have a key
# A renewal can be forced with --renew on our "acme order" command
if [ $valid -eq 1 ]
then
    exit
Fi

# Olive will overwrite the cert and private key in the .mrtsec directory.
# Copy the private key somewhere else to make this transition seamless
MYDATE=`date +%F`
NEWKEY=`mktemp --suffix=.$MYDATE /etc/kamailio/XXXXXXXXXX` || exit 1
cp -f "$key" "$NEWKEY"
```