How to automate TLSA update

2025-09-28

This article describes how to automatically update the TLSA record for DANE

Introduction

"DNS-based Authentication of Named Entities (DANE)" is specified in rfc6698 and it requires DNSSEC (DANE only works when DNSSEC is enabled). DNSSEC is defined in RFC4033, RFC4034, and RFC4035.

I describe here my process how I updated auotmatically the TLSA record for my mailserver via the deSEC rrsets API. If you like please be so kind and Donate to deSEC

Pre-Requirements:

- jq
- curl
- certbot
- deSEC Account
- own Domain

DeSEC, domain + mail setup

The "Mail setup for deSEC" is described at the link Mail setup for deSEC.

certbot

Certbot offers the option to run some hooks at certificate handling Pre and Post Validation Hooks.

json Payload

The file `tlsa-update.json` have this content.

```
[
    {
        "subname": "_25._tcp.mail",
        "type": "TLSA",
        "ttl": 3600,
        "records": [
            "3 1 1 ${TLSA_SHA}"
        ]
    }
]
```

post-hook

At the end add the following script into the post hook directory `/etc/letsencrypt/renewal-hooks/post/`.

I called it `reload-services.sh`

```
#!/bin/bash

## Update TLSA record

export DESEC_TOKEN=<YOUR_DESEC_TOKEN>
export DOMAIN_NAME=<YOUR_DOMAIN>
export CERT_DOMAIN=<CERT_DOMAIN>.${DOMAIN_NAME}
export TLSA_SHA=$(/usr/bin/openssl x509 -in /etc/letsencrypt/live/
${DOMAIN}/fullchain.pem -noout -pubkey \
  | /usr/bin/openssl pkey -pubin -outform DER \
  | /usr/bin/openssl sha256 2>&1\
  | /usr/bin/cut -f2 -d ' ')

envsubst < tlsa-update.json \
  | curl -sSLX PUT https://desec.io/api/v1/domains/${DOMAIN_NAME}/rrsets/
\
    --header "Authorization: Token ${DESEC_TOKEN}" \
    --header "Content-Type: application/json" \
    --data @- \
  | jq

/usr/bin/systemctl restart nginx.service
/usr/bin/systemctl restart dovecot.service
/usr/bin/systemctl restart postfix.service
```

I know that there is the variable `CERTBOT_DOMAIN` and it could also be used in the script above, if it fit's for your use-case

Finally

Wenn everything works as designed should you never need to update the TLSA record when the LE certificate was changed.