ACME Certificates with FreeIPA

Simplify SSL/TLS Management

Josep Andreu Font
Senior Technical Account Manager

José Ángel de Bustos
Senior Specialist Solution Architect

ACME Certificates with FreeIPA: Simplify SSL/TLS Management

Summary

□ 1. Overview ACME protocol. Features, caveats and limitations in FreeIPA/Dogtag CA.

□ 2. Overview mod_md. Fine tuning, limitations. Systemd to the rescue.

□ 3. Demo mod_md renewing and revocation.

□ 3. Overview cert_manager.

□ 4. Demo cert_manager.

□ 4. Conclusions.

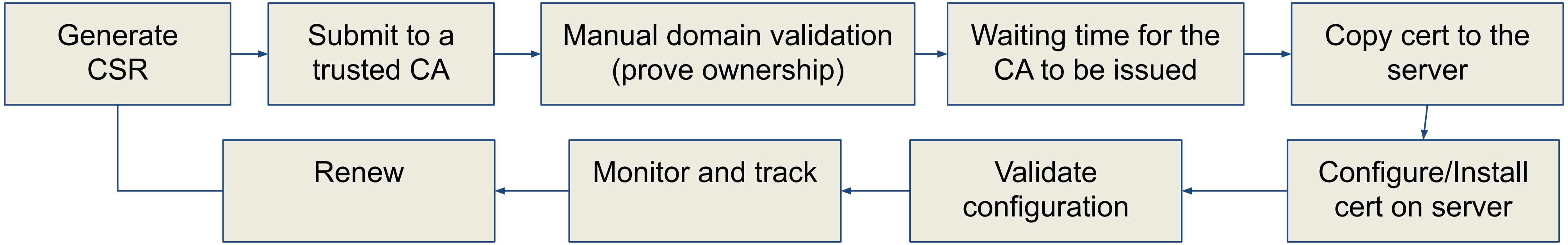
□ 5. Q&A.

Overview ACME Protocol

- 2024 Digital PKI and trust report ~38% of orgs still use spreadsheets and homegrown solutions (databases, scripts, etc.) to manually track certificates -> Many business deploy certs using outdated techniques!
- Limitations of manual management:
  - Inefficiency/Complexity. Dedication to monitor and track -> Security risks increased by errors in monitoring.
  - Time consuming process.
  - Prone to human error that can lead to painful outage.
- Expired or revoked certificate can have a significant impact! Loss of trust, bad reputation, unavailability, etc.
- Automated Certificate Management Environment (ACME) protocol designed by Internet Security Research Group (ISRG) for their CA Let’s Encrypt, enables automation of issuance and renewal of certificates.
- Removes the need of human-interaction, eliminates all human errors. Issuing of domain-validated (DV) certificates.

Overview ACME Protocol

- Traditional process is a tedious process that involves a lot of steps:

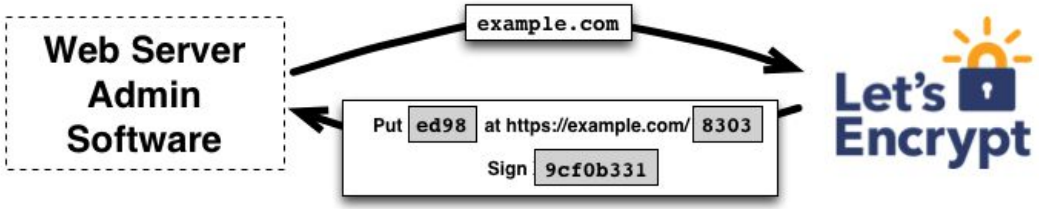

Generate CSR
Submit to a trusted CA
Manual domain validation (prove ownership)
Waiting time for the CA to be issued
Copy cert to the server
Configure/Install cert on server
Validate configuration
Monitor and track
Renew

- ACME server with clients will perform all this steps completely automatically! Avoids a manual and error-prone process.
- With ACME and FreeIPA Dogtag CA you can deploy an automated PKI at a low cost, with relatively low effort.
- FreeIPA with ACME provides short lifetime certificates, by default 3 months (configurable) to be in line with Let's Encrypt profile.
- ACME uses a challenge and response authentication mechanism to prove that a client has control of identifier,

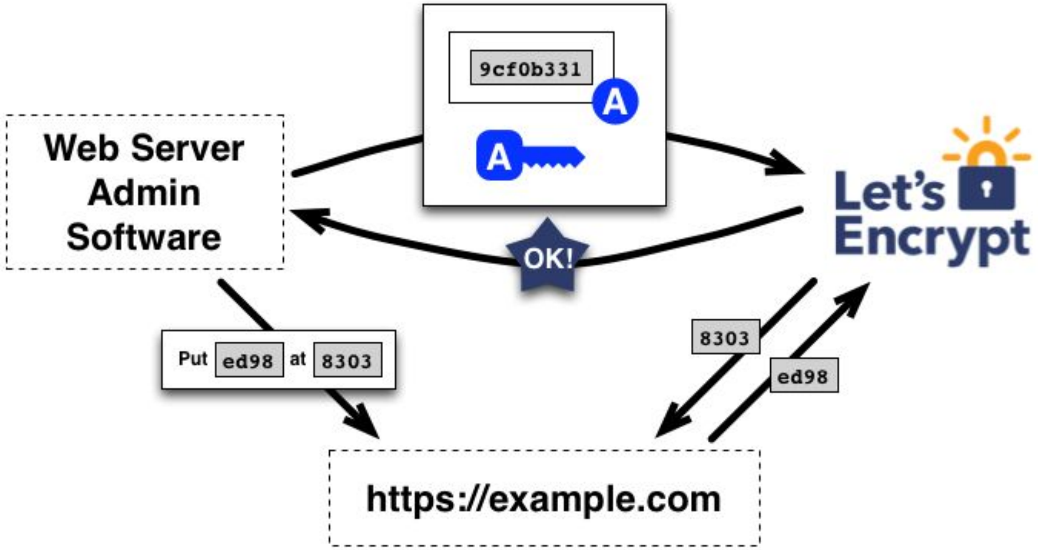
  the origin is legit.

Certificate issuance with ACME Protocol (RFC8555)

The challenge (https)

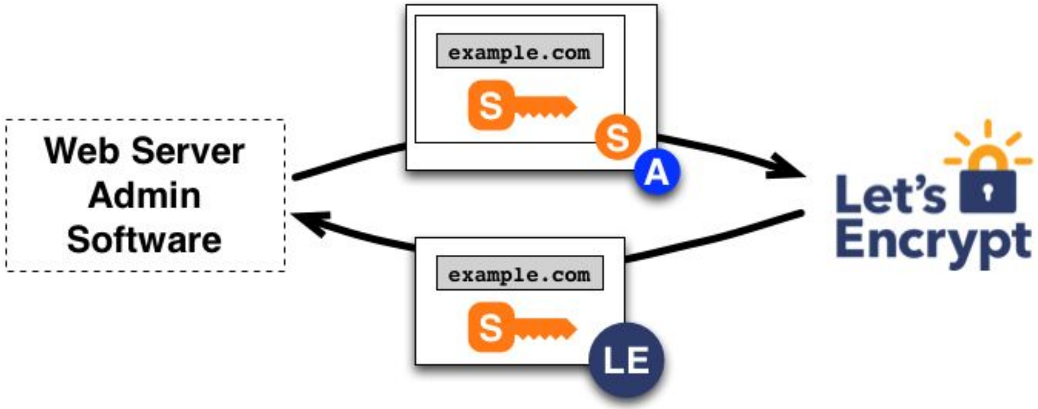

Web Server Admin Software
example.com
Put ed98 at https://example.com/ 8303
Sign 9cf0b331
Let's Encrypt

Source: https://letsencrypt.org/



Source: https://letsencrypt.org/

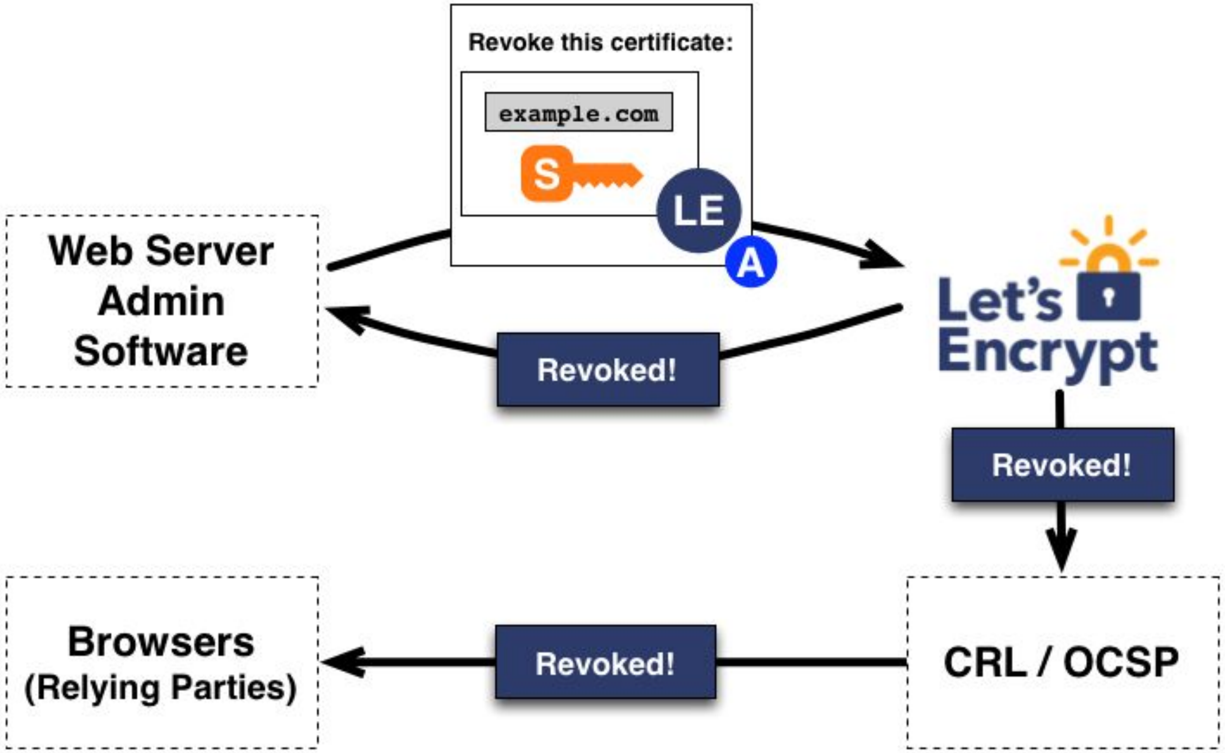
Certificate issuance



Source: https://letsencrypt.org/

Certificate revocation with ACME Protocol (RFC8555)

Certificate revocation



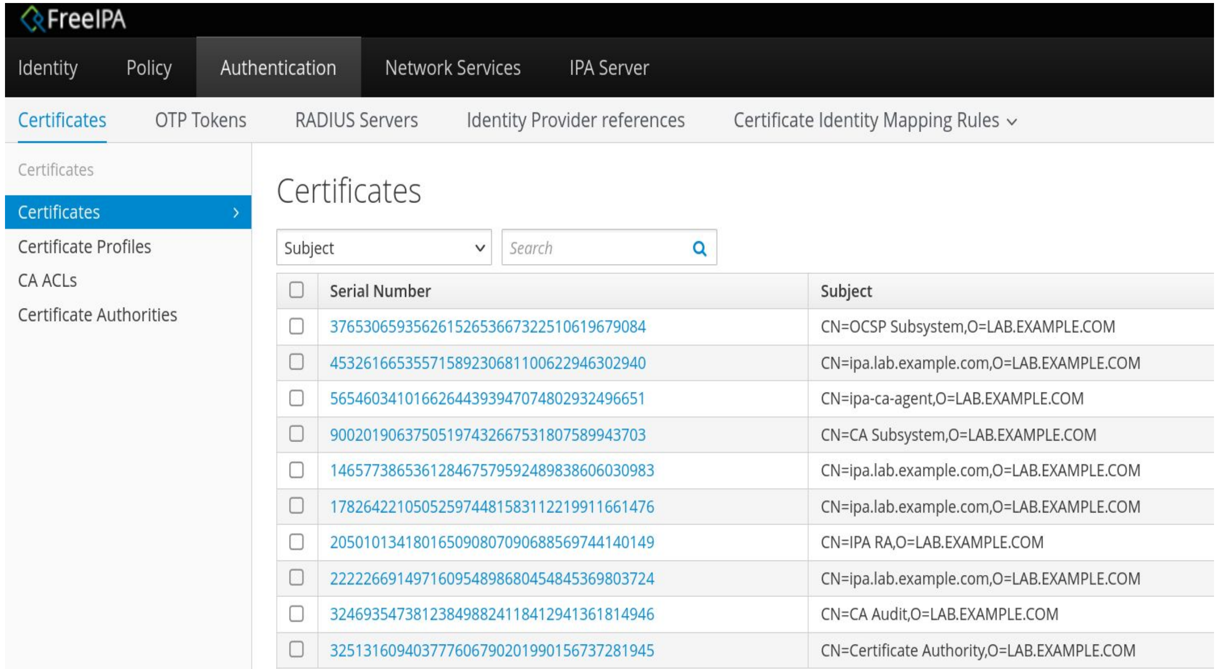
Source: https://letsencrypt.org/

Features, caveats and limitations in FreeIPA/Dogtag CA

- ACME by default is disabled on FreeIPA Dogtag CA. Enabling/Disabling is a deployment-wide operation, because is in the LDAP replicated database, the `ipa-acme-manage` command controls the feature.
- A lot of certificates can accumulate over time!

  So really recommended to install FreeIPA with RSNv3:

  - Certificate pruning in Dogtag CA database requires random serial numbers!
- Existing installations with sequential certificates, need a manual process to delete expired certificates (situation today, a switch is expected to come).



Certificates

□	Serial Number	Subject
□	37653065935626152653667322510619679084	CN=OCSP Subsystem,O=LAB.EXAMPLE.COM
□	45326166535571589230681100622946302940	CN=ipa.lab.example.com,O=LAB.EXAMPLE.COM
□	56546034101662644393947074802932496651	CN=ipa-ca-agent,O=LAB.EXAMPLE.COM
□	90020190637505197432667531807589943703	CN=CA Subsystem,O=LAB.EXAMPLE.COM
□	146577386536128467579592489838606030983	CN=ipa.lab.example.com,O=LAB.EXAMPLE.COM
□	178264221050525974481583112219911661476	CN=ipa.lab.example.com,O=LAB.EXAMPLE.COM
□	205010134180165090807090688569744140149	CN=IPA RA,O=LAB.EXAMPLE.COM
□	222226691497160954898680454845369803724	CN=ipa.lab.example.com,O=LAB.EXAMPLE.COM
□	324693547381238498824118412941361814946	CN=CA Audit,O=LAB.EXAMPLE.COM
□	325131609403777606790201990156737281945	CN=Certificate Authority,O=LAB.EXAMPLE.COM

Overview mod_md

- mod_md provides SSL certificates for your domains from any CA that supports the ACME protocol.
- Robust Online Certificate Status Protocol (OCSP) stapling (browser does not contact CA, instead web server), fast page loading.

  Your Apache will check status of certs regularly, needed to found any revocations.
- mod_ md features:
  - Certificate Request using ACME protocol.
  - Automatic Certificate Renewal for expired and also revoked certificates (new in mod_md 2.4.26).
  - Wildcard Certificate Support.
  - Certificate status monitoring.
  - OCSP stapling support, continuous refresh OCSP responses in the background.
  - Notification when certificates are next to expire or are revoked.

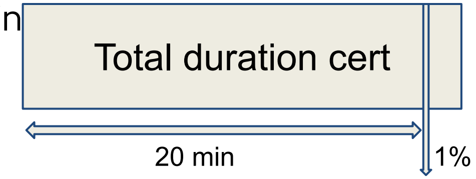
Fine tuning, limitations

- New: version 2.4.26 will trigger a renewal when a revoked status is observed.
- **Needed a graceful reload for new certs to be active**, so does not interrupt ongoing requests.
- **MDStapling** on, enables OCSP stapling by which Apache will check status of certificates regularly.
- **MDCheckInterval** to react quickly to a certificate revocation or expiration, Apache detect all managed domains and refreshes

  OCSP response. Minimum time for httpd to notice any change.

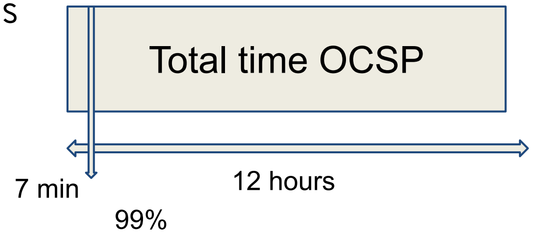
  Shorter check interval will not help if you restart/reload once a day!
- **MDRenewWindow** is the percentage of the total lifetime before the expiration date for mod_md to get a new signed certificate,

  by default will renew certs when a third of their lifetime is left. (Example: 1% of 20 min



- **MDStaplingRenewWindow** will retrieve a fresh OCSP response.

  Example: 99% of 12 hours substracted ~ 7 minutes



Systemd to the rescue

- As said previously, a reload of service is needed to put certificates in the running configuration.
- It will be nice to not have to perform reload operations regularly trying to catch the time when certs are renewed,
- With systemd, we can monitor whether a specific file exists, and when it does we can execute some actions on a service.
- Can be combined with multi-site certificate management. For that, add MDomain for each of your managed domains.
- Create a .path unit file to check the existence of new certs in staging area (usually empty):

```
[Unit]
Description= Triggers the reload of httpd
[Path]
PathExistsGlob=/etc/httpd/state/md/staging/*.lab.example.com/pubcert.pem
[Install]
WantedBy=multi-user.target
```

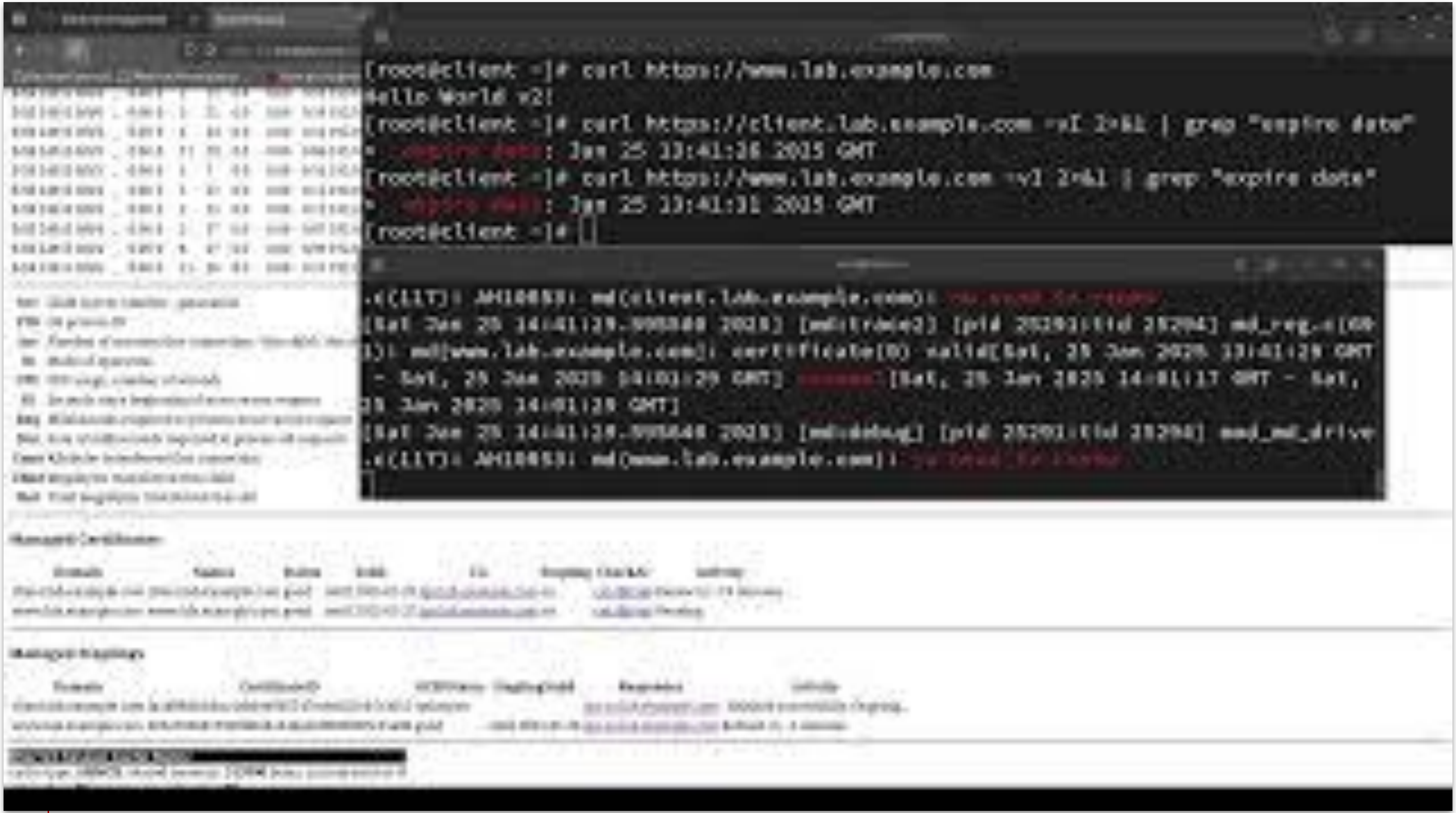
- Create a .service that corresponds to the .path that performs the reload of the service.

```
[Unit]
Description=srv restarter
[Service]
Type=oneshot
ExecStart=/usr/bin/systemctl reload httpd.service
```

- With that we have complete lifecycle covered, fully automated and scalable!

Demo mod_md renewing an expired certificate

EXPIRED



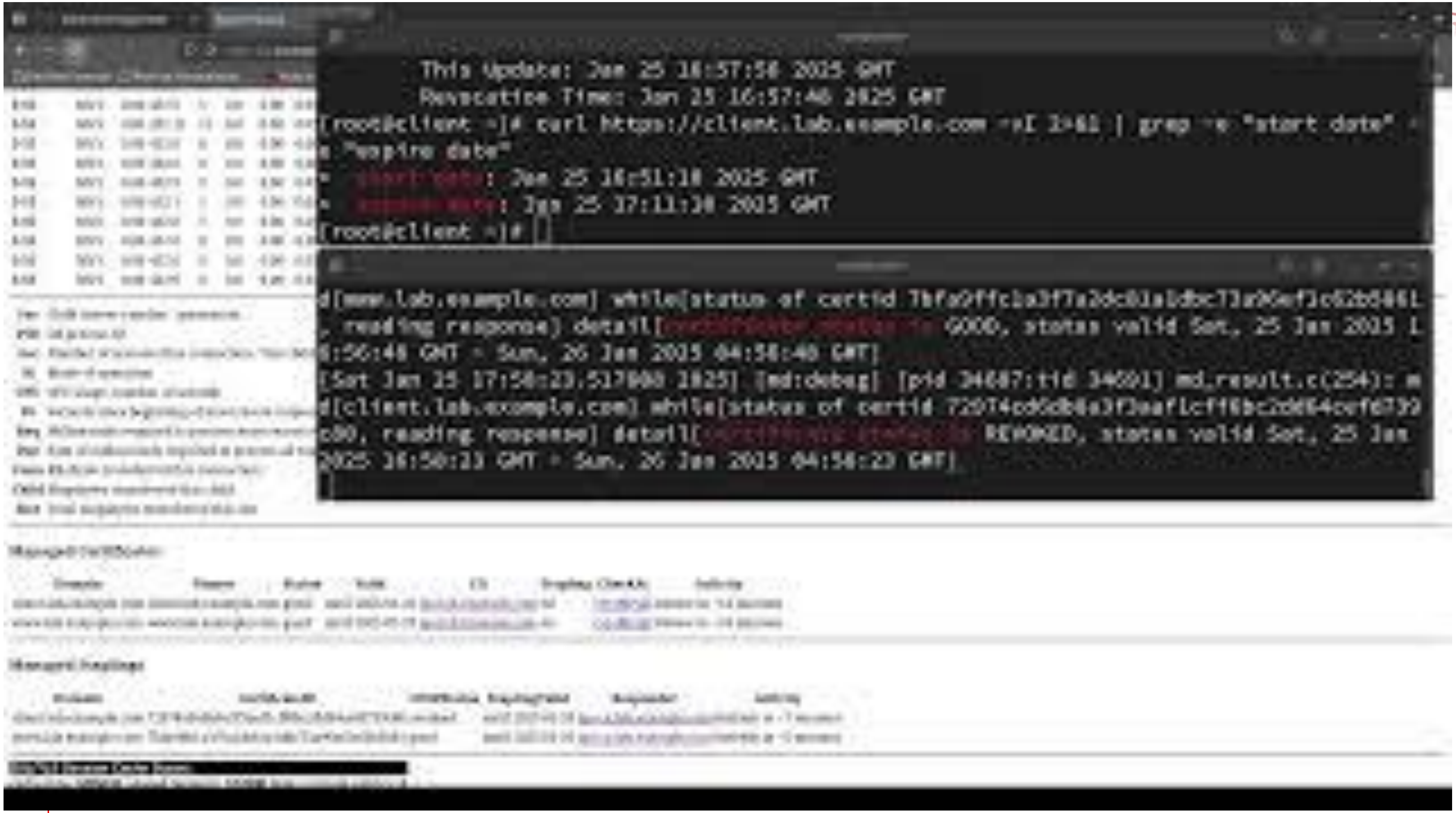
```
[root@client ~]# curl https://www.lab.example.com
Hello World v2!
[root@client ~]# curl https://client.lab.example.com -vI 2>&1 | grep "expire date"
*  expire date: Jan 25 13:41:26 2025 GMT
[root@client ~]# curl https://www.lab.example.com -vI 2>&1 | grep "expire date"
*  expire date: Jan 25 13:41:31 2025 GMT
[root@client ~]#
```

```
.c(111)]: AH10053: md(client.lab.example.com): [illegible]
[Sat Jan 25 14:41:29.995840 2025] [md:trace2] [pid 25293:tid 25294] md_reg.c(10
1)]: md[www.lab.example.com]: certificate[0] valid[Sat, 25 Jan 2025 13:41:29 GMT
 - Sat, 25 Jan 2025 14:01:29 GMT] [illegible] [Sat, 25 Jan 2025 14:01:17 GMT - Sat,
25 Jan 2025 14:01:29 GMT]
[Sat Jan 25 14:41:29.995848 2025] [md:debug] [pid 25293:tid 25294] mod_md_drive
.c(111)]: AH10053: md(www.lab.example.com): [illegible]
```

FreeIPA
Open Source Identity Management Solution

Demo mod_md renewing a revoked certificate

REVOKED



```
        This Update: Jan 25 16:57:56 2025 GMT
        Revocation Time: Jan 25 16:57:46 2025 GMT
[root@client ~]# curl https://client.lab.example.com -vI 2>&1 | grep -e "start date" -
e "expire date"
*  start date: Jan 25 16:51:18 2025 GMT
*  expire date: Jan 25 17:11:18 2025 GMT
[root@client ~]#
```

```
d[www.lab.example.com] while[status of certid 7bfa2ffc1a3f7a2dc01a1dbc73a06ef1c62b5461
, reading response] detail[certificate status is GOOD, status valid Sat, 25 Jan 2025 1
6:56:48 GMT - Sun, 26 Jan 2025 04:56:48 GMT]
[Sat Jan 25 17:58:23.517000 2025] [md:debug] [pid 34687:tid 34691] md_result.c(254): m
d[client.lab.example.com] while[status of certid 72074cd6db6a3f3eaf1cff6bc2d064cefd739
c80, reading response] detail[certificate status is REVOKED, status valid Sat, 25 Jan
2025 16:58:23 GMT - Sun, 26 Jan 2025 04:58:23 GMT]
```

FreeIPA
Open Source Identity Management Solution

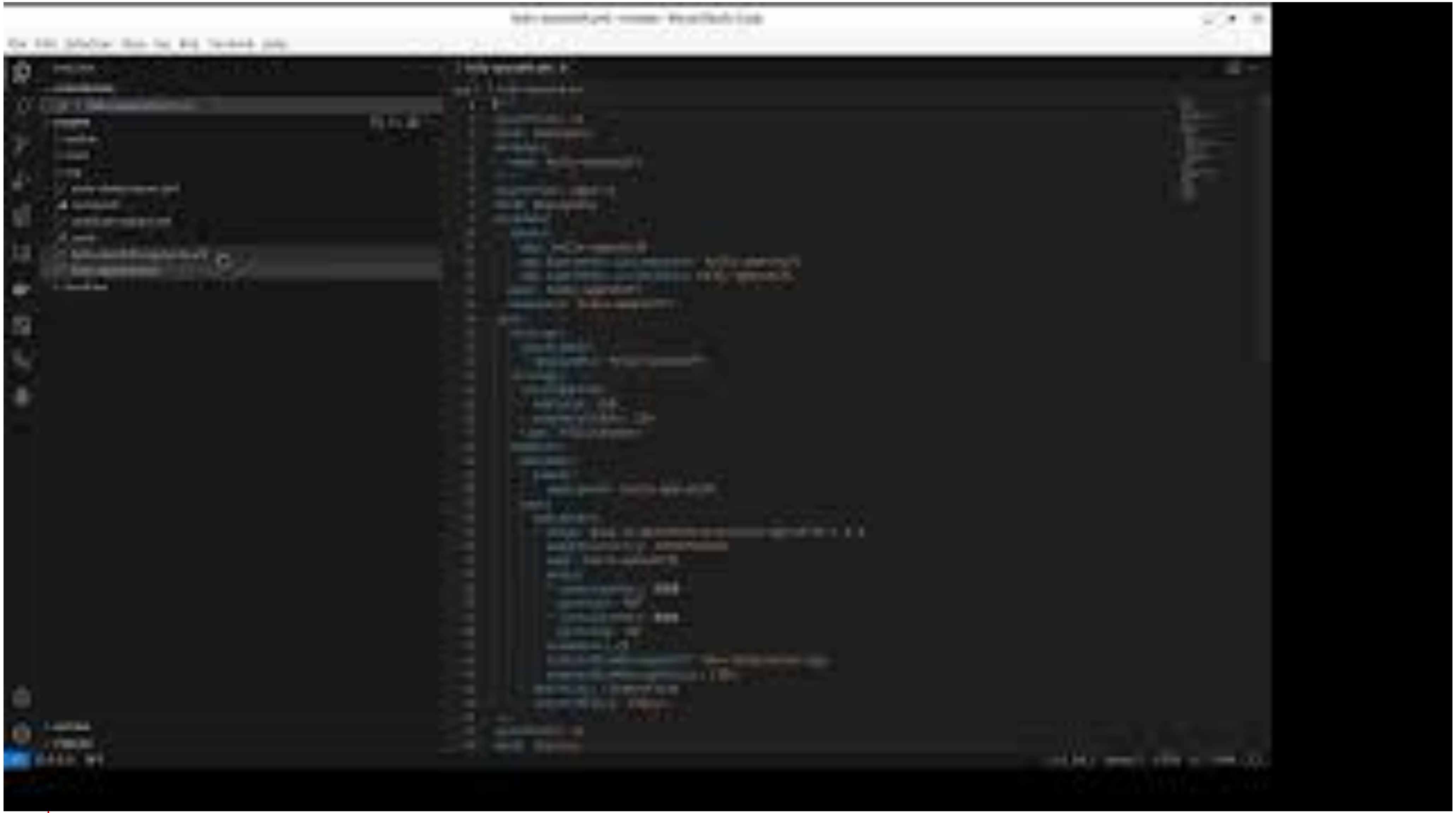
Overview Cert-manager

- Cloud Native Computing Foundation project from November 2020, maturity level on September 2024.
- X.509 Certificate Management for Kubernetes.
- Cert-manager will obtain certificates from a variety of Issuers.
- You can create your own Issuers.
- ACME Issuers are supported.
- You can use private CA using trust-manager to manage and distribute those certificates.

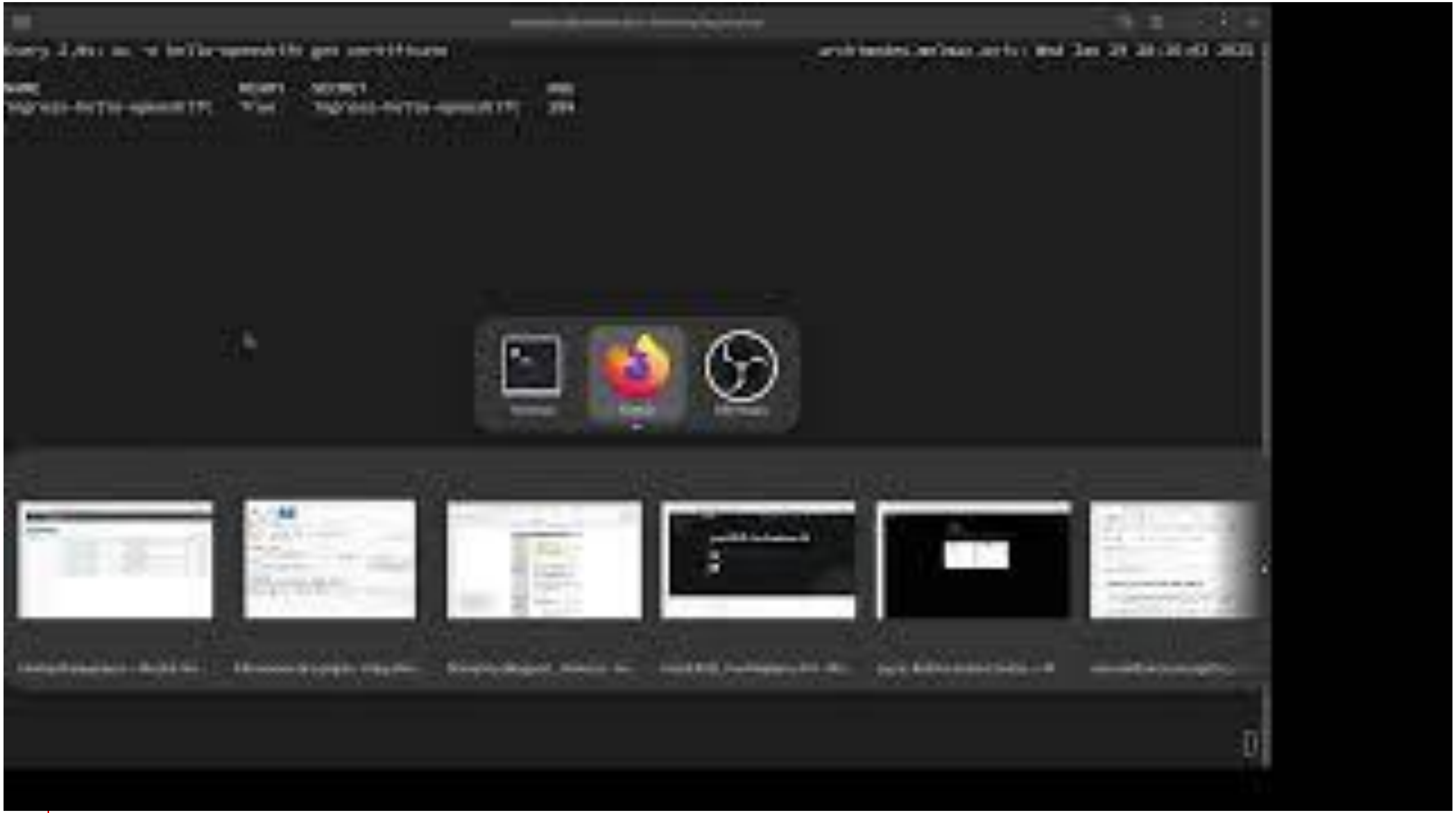
Cert-manager 101

- By default certificates are issued by 90 days, if ***renewBefore*** has not been set. Minimum certificate life 1 hour.
- Certificates will be renewed when ⅔ of their duration is reached.
- If a certificate issuance fails, cert-manager will try to renew the certificate
- Certificates can be re-issued in some situations:
    - Data mismatch between certificate and certificate spec
    - Secret is missing
- You can not send a revocation request from cert-manager to ACME server.

Issuing ACME certificates to Kubernetes applications using FreeIPA



Re-issuing ACME certificates to Kubernetes applications using FreeIPA



```
Every 2.0s: oc -n hello-openshift get certificate          [illegible]: Wed Jan 29 [illegible] 2025

NAME                          READY   SECRET                        AGE
ingress-hello-openshift-tls   True    ingress-hello-openshift-tls   [illegible]
```

Resources

- Managing Automatic Certificate Management Environment (ACME) in Identity Management (IdM)
- Automatically acquire and renew certificates using mod_md and Automated Certificate Management Environment (ACME) in Identity Management (IdM)
- Automatic certificate issuing with IdM and cert-manager operator for OpenShift

Conclusions

- FreeIPA can solve certificate lifecycle management for your applications through an ACME client:
  - cert-manager for Kubernetes environments.
  - mod_md for traditional web applications.
  - Other ACME clients.
- You can create your own private ACME CA, integrated with your PKI.

Thank you

FreeIPA

Open Source Identity Management Solution