A Comprehensive Lab Guide :

Deployment and Configuration of Dogtag PKI on Fedora Server 42

Done by :

- **Ait Benalla Chayma**

Table of Contents:

Introduction

This report documents the complete installation and configuration of a Dogtag PKI (Public Key Infrastructure) system, an enterprise-grade Certificate Authority solution developed by Red Hat. The deployment was conducted in a lab environment to establish a functional PKI infrastructure capable of managing digital certificates, keys, and security policies.

For this implementation, Fedora Server 42 was selected as the operating platform, as Dogtag PKI is natively designed for Red Hat-based distributions including Fedora, CentOS, and RHEL. This compatibility ensures optimal package availability, streamlined dependency management, and proven stability for PKI operations.

The project encompasses the full deployment lifecycle—from initial system preparation and network configuration through Dogtag PKI subsystem installation, 389 Directory Server integration, and final operational testing of certificate management workflows. The resulting infrastructure provides a robust foundation for issuing, revoking, and managing digital certificates in enterprise environments.

1. Prepare the fedora machine

Deployment of a Fedora Server VM on GCP via EVE-NG

We deployed a Fedora Server virtual machine in the GCP (Google Cloud Platform) environment using EVE-NG.
We installed the following version: **Fedora Server 42 QEMU qcow2** for Intel and AMD x86_64 systems, sourced from The Fedora Project.

- Install this version from Fedora Server | The Fedora Project.
- Recommended: ≥4 GB RAM, ≥8 GB disk for a VM.

Initial System Configuration for Fedora Server 42

Upon first boot, Fedora Server 42 presents an interactive text-based menu for initial system configuration.

Procedure:

1. After the system boots, a setup menu will automatically appear.
2. Use the keyboard arrow keys to navigate through the menu options.
3. The following configurations were performed:
    - **Network Configuration:** Set up the network interface using the menu options.
    - **Root Password:** The root password was set to chayma123.
    - **User Account:** A user account named root was confirmed or created.

Verification:
After completing the menu setup, the system was ready for use with these credentials.

Hostname Configuration

Proper hostname configuration is essential for Dogtag PKI deployment, as the system's FQDN is used to generate certificates and establish secure communication between PKI components.

- Set the FQDN: **sudo hostnamectl set-hostname pki.exemple.com**

- Verify: **hostnamectl status** should display the static hostname
- Check that **/etc/hosts** include proper entries:

```
text                                                    Copy  Download

127.0.0.1   localhost localhost.localdomain
192.168.1.100 pki.example.com pki
```

Important: Make sure your FQDN resolves to the correct IP address, either in /etc/hosts or via DNS.

- Check hostname: **hostname** and **hostname -f**
- Test name resolution**:**
  ```
  getent hosts pki.exemple.com
  ping -c 2 pki.exemple.com
  ```
- For the changes to take full effect across all services, reboot the system: **sudo reboot**

2. Installation of Dogtag PKI and 389 Directory Server

Package Installation

The Dogtag PKI meta-package and 389 Directory Server were installed to provide the PKI infrastructure and backend directory service:

```
# Install Dogtag PKI suite
sudo dnf install -y dogtag-pki

# Install 389 Directory Server base package
sudo dnf install -y 389-ds-base
```

Installed Subsystems:

- **Core Components:** dogtag-pki-server, dogtag-pki-base, dogtag-pki-tools
- **PKI Subsystems:** CA (Certificate Authority), KRA (Key Recovery Authority), TKS (Token Key Service)
- **Support Services:** OCSP (Certificate Status), EST (Secure Enrollment), ACME protocol
- **Additional Packages:** Java libraries, web themes, documentation, and test utilities

Package	Role / Description
dogtag-pki-base	Core libraries and common files required by all subsystems.
dogtag-pki-ca	Certificate Authority (CA) – issues, renews, revokes certificates.
dogtag-pki-kra	Key Recovery Authority (KRA) – archives and recovers private keys.
dogtag-pki-tks	Token Key Service (TKS) – manages cryptographic tokens (smart cards).
dogtag-pki-tps	Token Processing System (TPS) – processes token certificate requests.

Package	Role / Description
dogtag-pki-ocsp	Online Certificate Status Protocol (OCSP) – real-time certificate validation.
dogtag-pki-est	Enrollment over Secure Transport (EST) – simplifies certificate enrollment for devices.
dogtag-pki-server	Backend server components (Tomcat + PKI services).
dogtag-pki-tools	Command-line tools for managing Dogtag PKI.
dogtag-pki-theme	Web UI themes (appearance) for browser-based administration.
dogtag-pki-java	Java libraries needed for Dogtag operations.
dogtag-pki-javadoc	Documentation in Javadoc format.
dogtag-pki-tests	Test scripts and tools for verifying the installation.
dogtag-pki-acme	ACME protocol support – automates certificate issuance (e.g., Let's Encrypt).

Key Points

- The system has **all major subsystems installed**: CA, KRA, TKS, TPS, OCSP, and EST.
- Optional components like ACME, theme, tools, tests, and Java libraries are also present.
- Some subsystems like **RA (Registration Authority)** are integrated into the CA package in modern Dogtag versions, so we won't see a separate package.

Directory Server Instance Creation

A 389 Directory Server instance was configured to serve as Dogtag's internal database:

```
# 1. Use dscreate to make a template
sudo dscreate create-template /etc/dirsrv/setup.inf

# 2. Edit the template with your settings
sudo nano /etc/dirsrv/setup.inf
```

The file content :

```
[general]
config_version = 2
full_machine_name = pki.exemple.com
strict_host_checking = false
suite_spot_group = nobody
suite_spot_userid = nobody
```

```
[slapd]
instance_name = pki-tomcat
port = 389
root_dn = cn=Directory Manager
root_password = Password
self_sign_cert = true
suffix = dc=exemple,dc=com
```

```
# 3. Create the instance
sudo dscreate from-file /etc/dirsrv/setup.inf

# 4. Check if the instance was created
sudo dsctl --list


# 5. Start and enable the service
sudo systemctl start dirsrv@pki-tomcat
sudo systemctl enable dirsrv@pki-tomcat

# 6. Verify it's working
sudo dsctl pki-tomcat status

# 7. Check status
sudo systemctl status dirsrv@pki-tomcat
```

3. PKI Certificate Authority Setup

PKI Configuration Preparation

The CA configuration file was created with necessary parameters for the Dogtag PKI deployment:

```
# Create PKI configuration directory
sudo mkdir -p /etc/pki

# Create CA configuration file
sudo nano /etc/pki/ca.cfg
```

Configuration File Content:

```
[DEFAULT]
pki_admin_email=admin@pki.exemple.com
pki_admin_name=caadmin
pki_admin_password=Secret.123
```

```
pki_client_database_password=Secret.123
pki_client_pkcs12_password=Secret.123

pki_ds_base_dn=dc=exemple,dc=com
pki_ds_database=pki-tomcat
pki_ds_hostname=localhost
pki_ds_password=Password
pki_ds_port=389

pki_security_domain_name=EXEMPLE
pki_security_domain_user=caadmin
pki_security_domain_password=Secret.123

pki_hostname=pki.exemple.com
pki_https_port=8443
pki_http_port=8080

[CA]
pki_ca_signing_nickname=ca_signing
pki_ocsp_signing_nickname=ca_ocsp_signing
pki_audit_signing_nickname=ca_audit_signing
pki_sslserver_nickname=sslserver
pki_subsystem_nickname=subsystem
```

PKI Subsystem Deployment

The CA subsystem was deployed using **pkispawn**:

```
# Install pki-server if not already installed
sudo dnf install pki-server

# Run pkispawn to create the CA subsystem using configuration file

sudo pkispawn -f /etc/pki/ca.cfg -s CA -vvv
```

Installation Verification

The installation completed successfully with the following summary:

```
==============================================================================
                                INSTALLATION SUMMARY
==============================================================================

    Administrator's username:             caadmin
    Administrator's PKCS #12 file:
        /root/.dogtag/pki-tomcat/ca_admin_cert.p12

    To check the status of the subsystem:
        systemctl status pki-tomcatd@pki-tomcat.service

    To restart the subsystem:
        systemctl restart pki-tomcatd@pki-tomcat.service

    The URL for the subsystem is:
        https://pki.example.com:8443/ca

    PKI instances will be enabled upon system boot

==============================================================================
```

Service Status Verification:

```
# Check PKI service status
sudo systemctl status pki-tomcatd@pki-tomcat

# Check directory server status
sudo systemctl status dirsrv@pki-tomcat
```

Service Port Verification

Confirm all essential Dogtag PKI and directory service ports are open and listening.

Check Open Ports on Fedora Server: 389/tcp (LDAP), 8080/tcp (HTTP), 8443/tcp (HTTPS/admin UI).

```
# Verify all required services are listening
sudo netstat -tulpn | grep -E ':(389|8080|8443)'
# OR using ss command (modern alternative)
sudo ss -tulpn | grep -E ':(389|8080|8443)'
```

Expected Results:

```
tcp    LISTEN   0   100   0.0.0.0:389    0.0.0.0:*    users:(("ns-
```

```
slapd",pid=1234,fd=12))
tcp    LISTEN   0   100   0.0.0.0:8080   0.0.0.0:*
users:(("java",pid=5678,fd=45))
tcp    LISTEN   0   100   0.0.0.0:8443   0.0.0.0:*
users:(("java",pid=5678,fd=67))
```

4. Accessing the CA Subsystem

Locate Admin Certificate

The administrator PKCS#12 certificate was generated during installation:

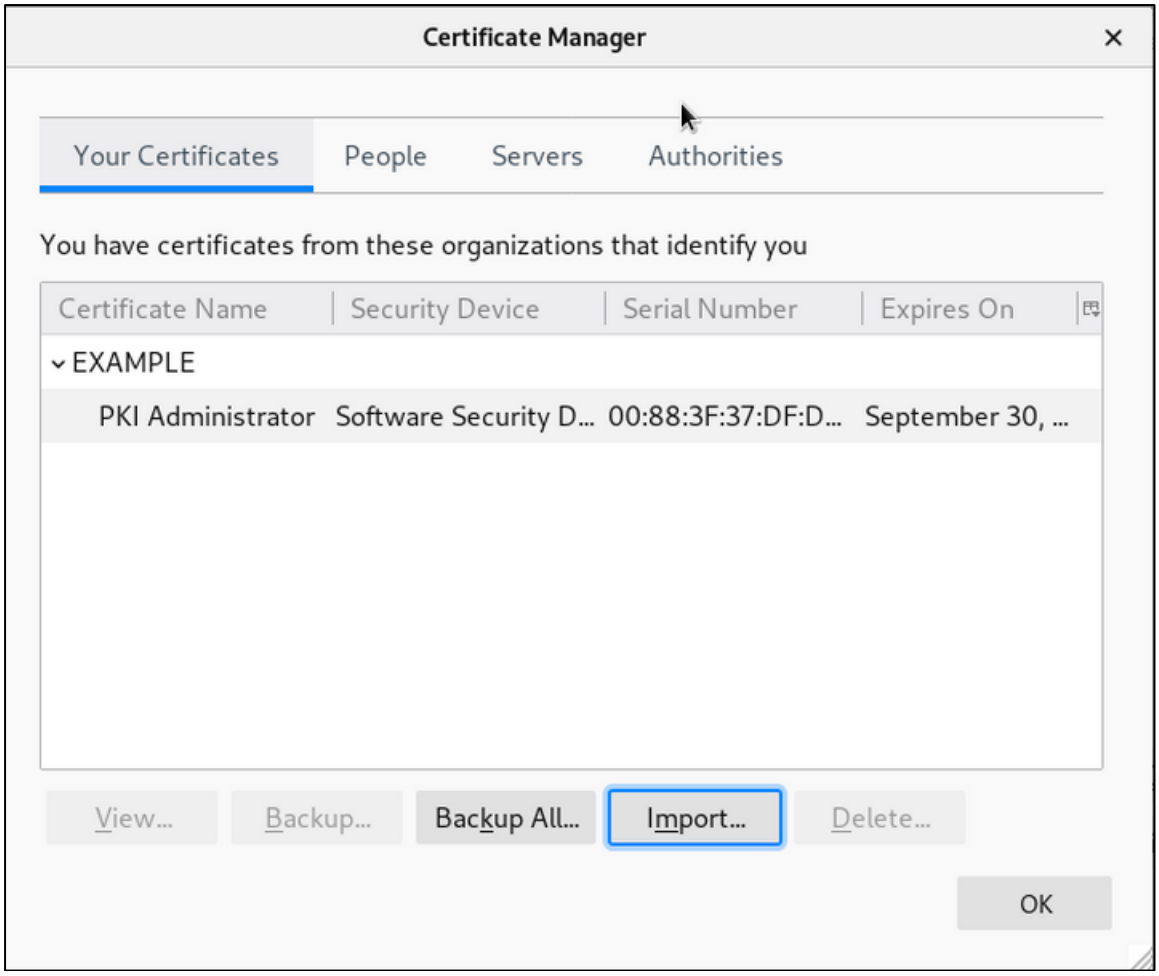
```
# Locate the admin certificate file
sudo find / -name "*admin*.p12" -type f 2>/dev/null

# Expected location and verification
ls -la /root/.dogtag/pki-tomcat/ca_admin_cert.p12
```

Import Certificate into Browser

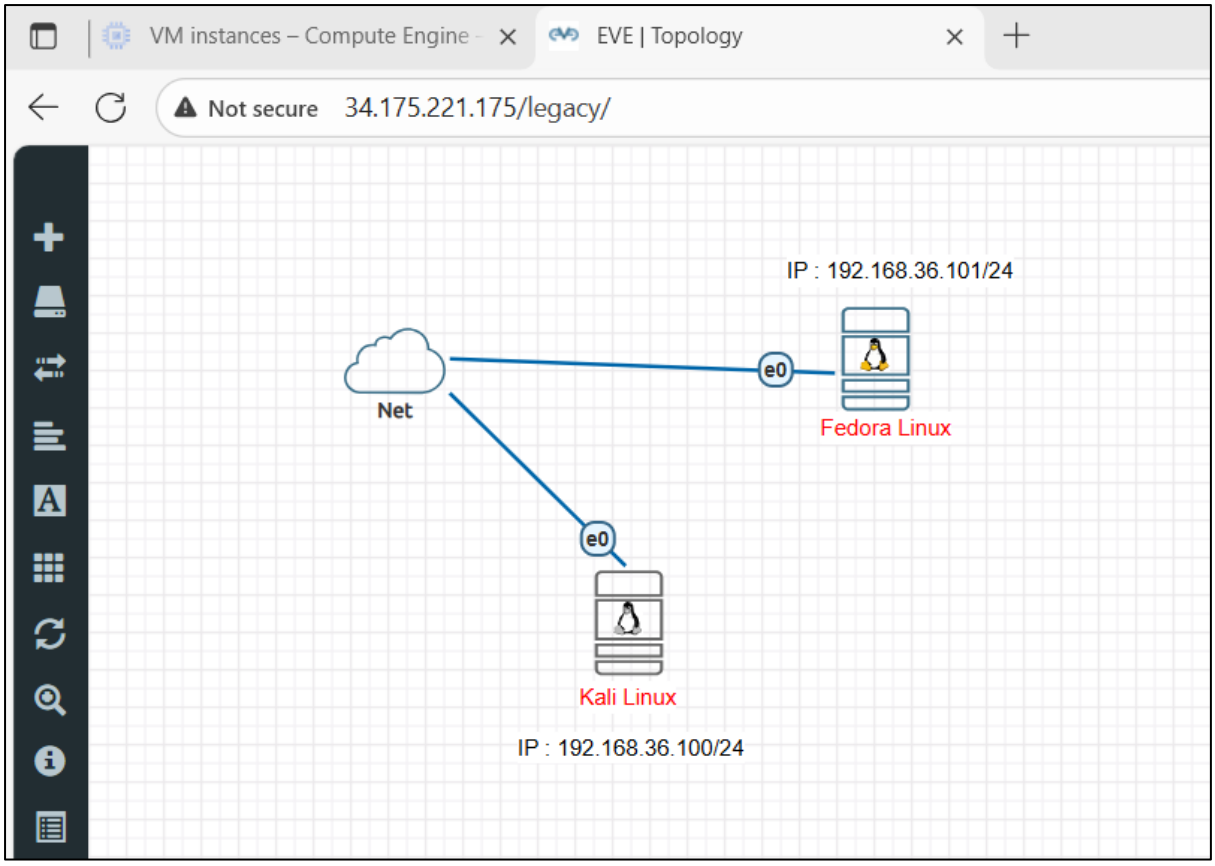
For Firefox:

- Navigate to: **Preferences → Privacy & Security → Certificates**
- Click "**View Certificates**"
- Select the "**Your Certificates**" tab
- Click "**Import**"
- Browse to: /root/.dogtag/pki-tomcat/ca_admin_cert.p12
- Enter password: **Secret.123** (as configured in ca.cfg)



Remote Access Configuration for EVE-NG/GCP Environment

Environment Context: The Dogtag PKI deployment is running on Fedora Server within an EVE-NG lab on Google Cloud Platform. To access the web interface, a Kali Linux GUI machine is deployed in the same network.



Security Note: This configuration is for lab use. In production, consider using SSH keys instead of password authentication and restrict root login.

Step 1: Deploy Kali Linux GUI Machine

- Launched Kali Linux with desktop environment in the same GCP project

- Configured network connectivity to Fedora server's subnet

- Verified network reachability to PKI server IP

Step 2: Configure Fedora Server Firewall

```
# Open HTTPS port for Dogtag web interface
sudo firewall-cmd --add-port=8443/tcp --permanent
sudo firewall-cmd --reload

# Verify Tomcat binding
sudo ss -tulpn | grep 8443
```

Step 3: Enable Secure File Transfer

```
# Enable SSH password authentication
sudo vi /etc/ssh/sshd_config

# Set the following parameters:
```

```
PasswordAuthentication yes
PermitRootLogin yes

# Restart SSH service
sudo systemctl restart sshd
```

Step 4: Transfer Admin Certificate to Kali Linux

On the Kali Linux machine:

```
# Copy admin certificate from Fedora server
scp root@192.168.36.100:/root/.dogtag/pki-tomcat/ca_admin_cert.p12
/home/kali/Downloads/

# Enter root password when prompted
```

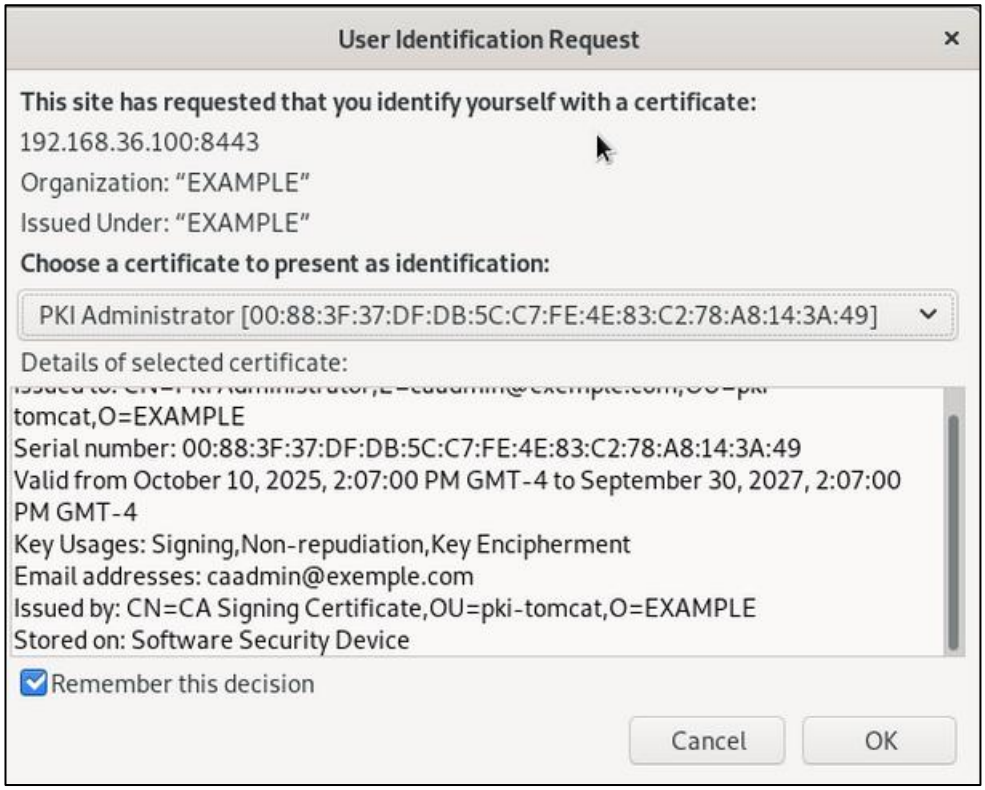
Step 5: Access Dogtag Web Interface

1. **Import certificate** in Kali Firefox:

   - Preferences → Privacy & Security → Certificates → Import

   - Select: `/home/kali/Downloads/ca_admin_cert.p12`

   - Password: `Secret.123`



2. **Access CA console:**

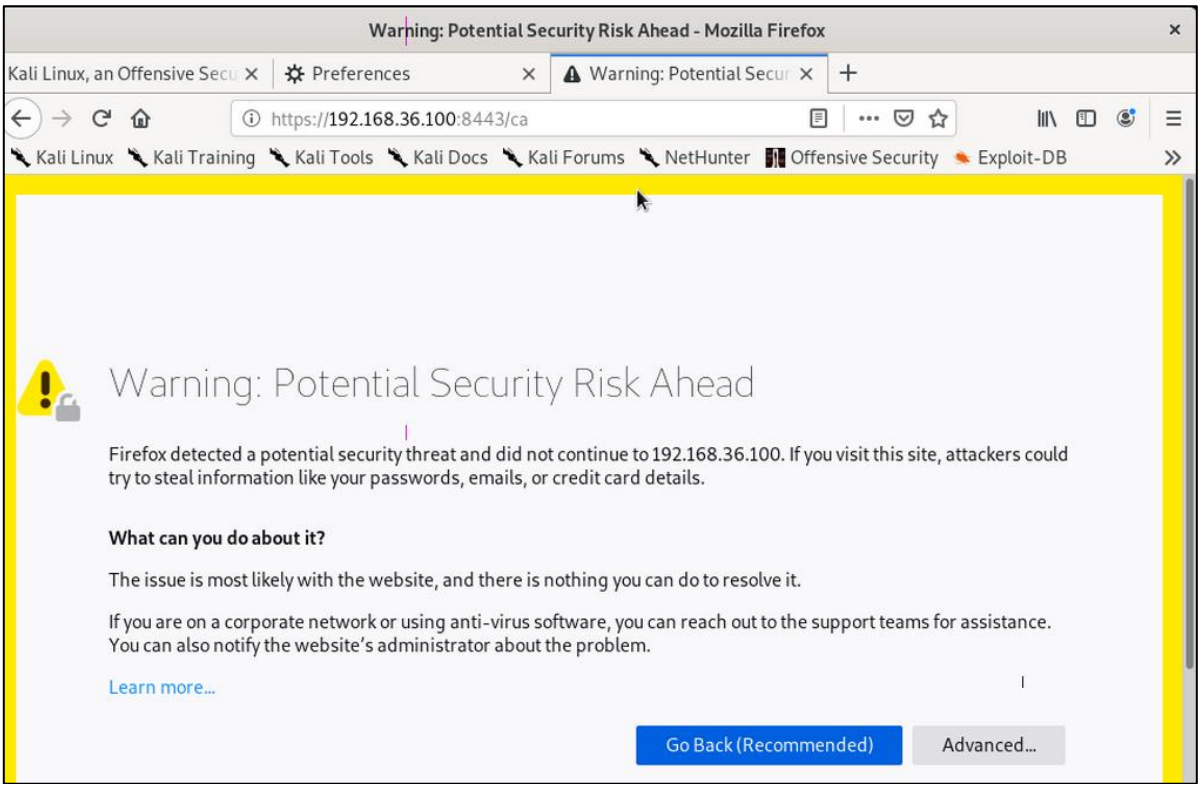
- **URL:** https://pki.exemple.com:8443/ca

3. Accept Security Warning

- A security warning will appear due to the self-signed certificate
- Click "**Advanced**" → "**Accept the Risk and Continue**"

4. Accept Login to Certificate Authority

- **Username**: caadmin (from ca.cfg configuration)
- **Password**: Secret.123 (from ca.cfg configuration)

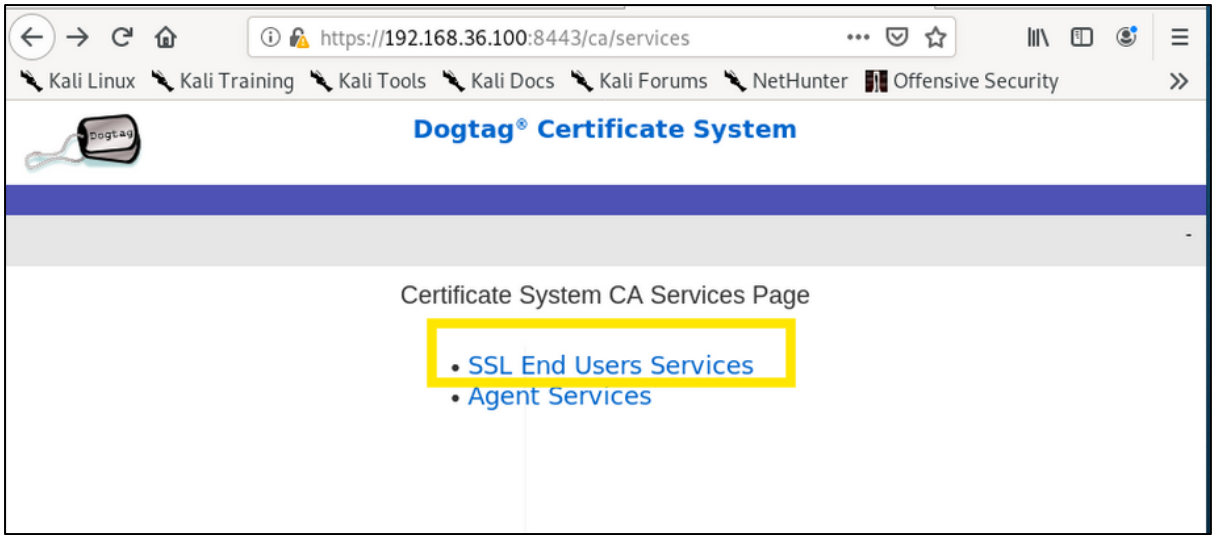


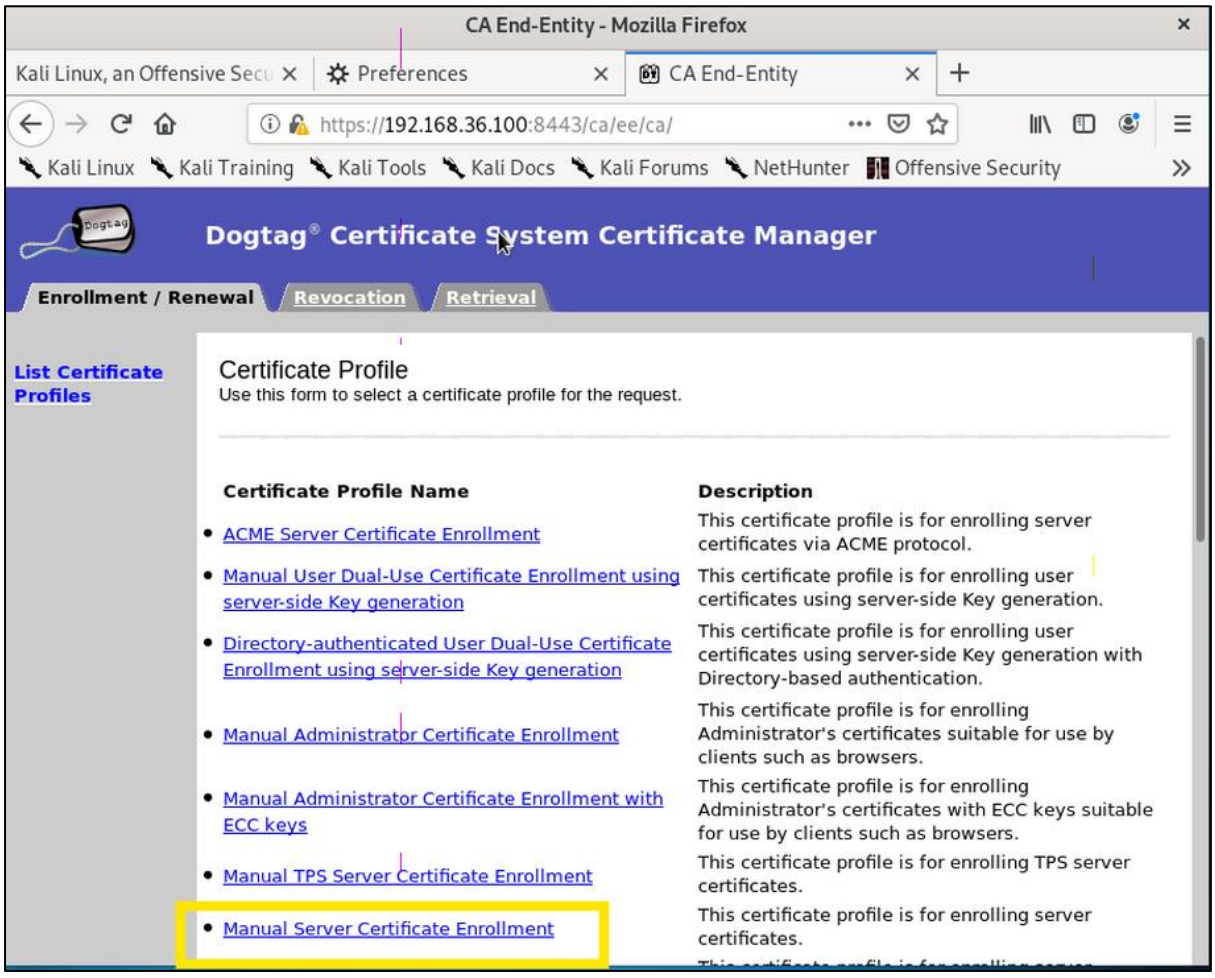
5. Certificate Authority Operations Demonstration

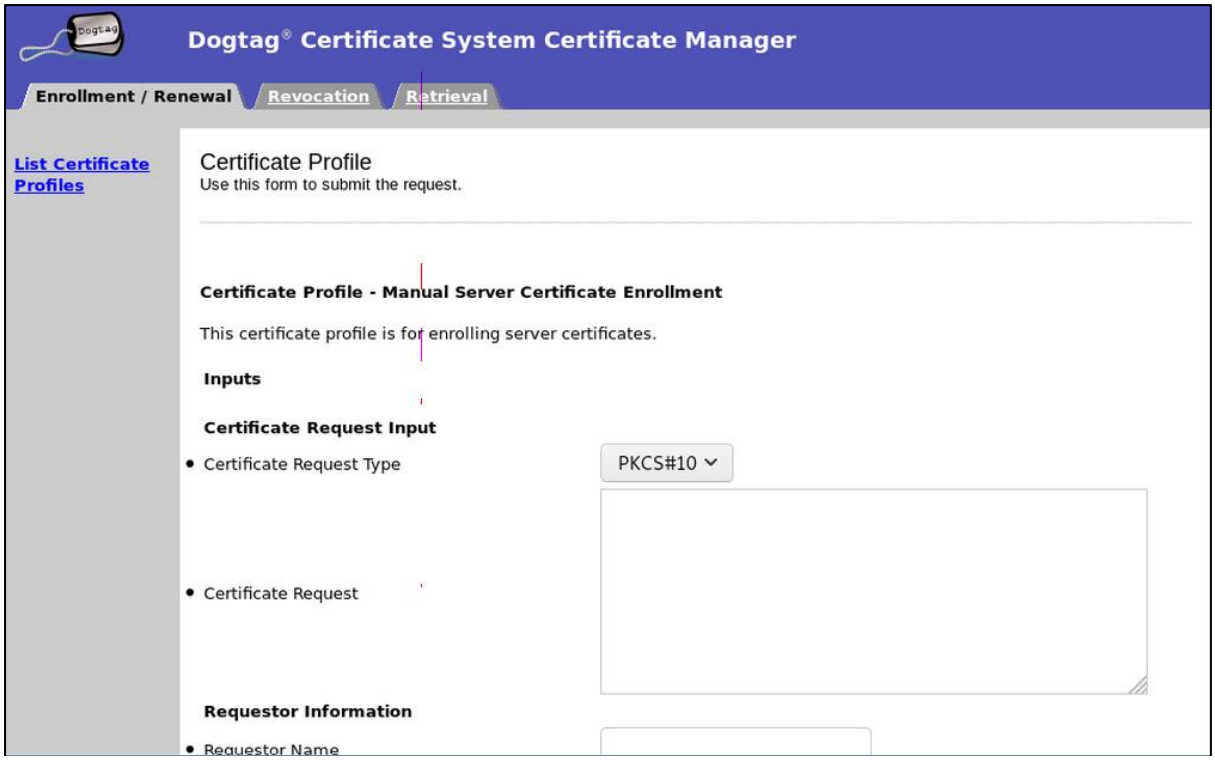
Certificate Creation and Issuance

Request Certificate

let's firstly select **'Manual Server Certificate Enrolment'**:


https://192.168.36.100:8443/ca/services
Kali Linux
Kali Training
Kali Tools
Kali Docs
Kali Forums
NetHunter
Offensive Security
Dogtag® Certificate System
Certificate System CA Services Page
• SSL End Users Services
• Agent Services


CA End-Entity - Mozilla Firefox
Kali Linux, an Offensive Sec
Preferences
CA End-Entity
https://192.168.36.100:8443/ca/ee/ca/
Kali Linux
Kali Training
Kali Tools
Kali Docs
Kali Forums
NetHunter
Offensive Security
Dogtag® Certificate System Certificate Manager
Enrollment / Renewal
Revocation
Retrieval
List Certificate Profiles
Certificate Profile
Use this form to select a certificate profile for the request.
Certificate Profile Name
Description
ACME Server Certificate Enrollment
This certificate profile is for enrolling server certificates via ACME protocol.
Manual User Dual-Use Certificate Enrollment using server-side Key generation
This certificate profile is for enrolling user certificates using server-side Key generation.
Directory-authenticated User Dual-Use Certificate Enrollment using server-side Key generation
This certificate profile is for enrolling user certificates using server-side Key generation with Directory-based authentication.
Manual Administrator Certificate Enrollment
This certificate profile is for enrolling Administrator's certificates suitable for use by clients such as browsers.
Manual Administrator Certificate Enrollment with ECC keys
This certificate profile is for enrolling Administrator's certificates with ECC keys suitable for use by clients such as browsers.
Manual TPS Server Certificate Enrollment
This certificate profile is for enrolling TPS server certificates.
Manual Server Certificate Enrollment
This certificate profile is for enrolling server certificates.



Generate Private Key and Certificate Signing Request (CSR)

- **On Linux machine:**

```
# Generate a 2048-bit RSA private key
openssl genrsa -out computer.key 2048

# Generate Certificate Signing Request (CSR)
openssl req -new -sha256 -key computer.key -out computer.csr
```

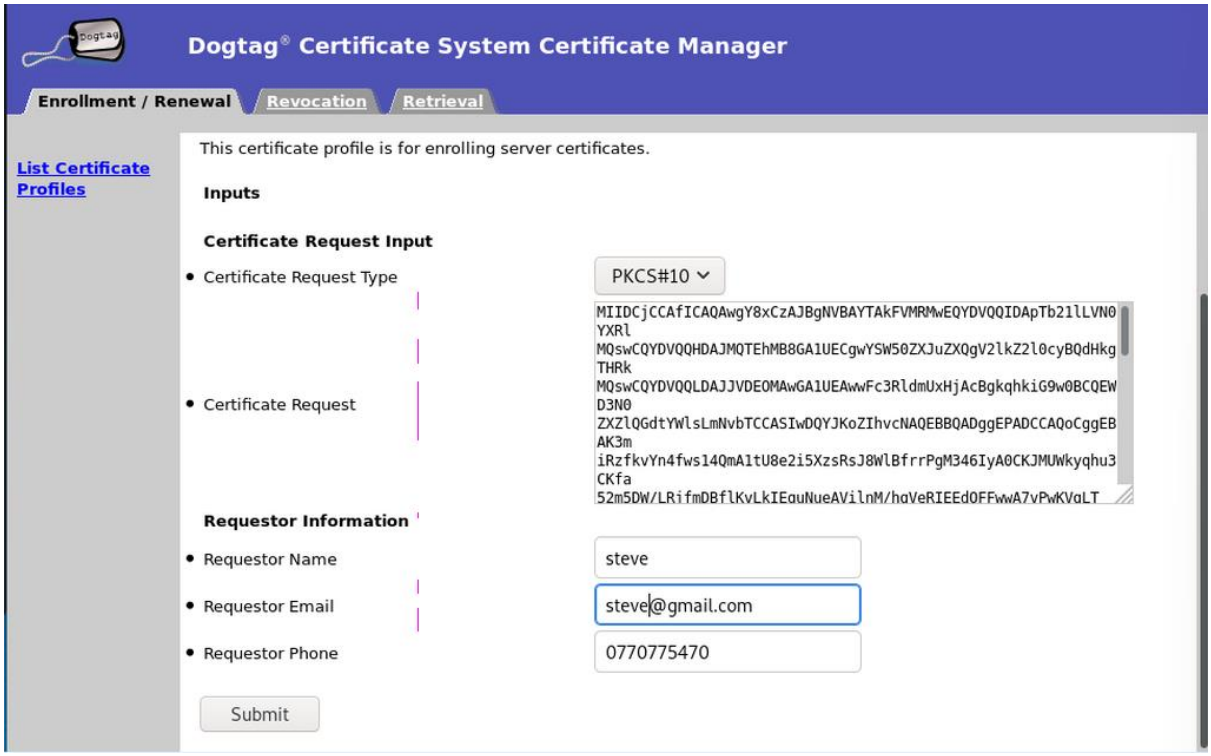
```
root@kali:~/Desktop# openssl genrsa -out computer.key 2048
Generating RSA private key, 2048 bit long modulus (2 primes)
...........+++++
root@kali:~/Desktop# openssl req -new -sha256 -key computer.key -out computer.csr
You are about to be asked to enter information that will be incorporated
into your certificate request.
What you are about to enter is what is called a Distinguished Name or a DN.
There are quite a few fields but you can leave some blank
For some fields there will be a default value,
If you enter '.', the field will be left blank.
-----
Country Name (2 letter code) [AU]:
State or Province Name (full name) [Some-State]:
Locality Name (eg, city) []:LA
Organization Name (eg, company) [Internet Widgits Pty Ltd]:
Organizational Unit Name (eg, section) []:IT
Common Name (e.g. server FQDN or YOUR name) []:steve
Email Address []:steve@gmail.com

Please enter the following 'extra' attributes
to be sent with your certificate request
A challenge password []:chayma123extra
An optional company name []:DIGIT
```

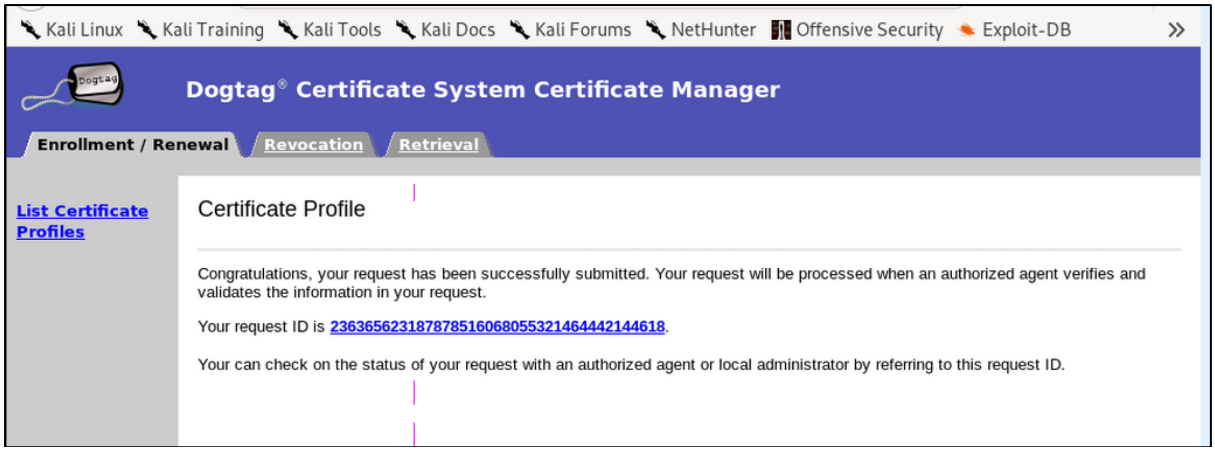
- **View the CSR content:**

```
root@kali:~/Desktop# cat computer.csr
-----BEGIN CERTIFICATE REQUEST-----
MIIDCjCCAfICAQAwgY8xCzAJBgNVBAYTAkFVMRMwEQYDVQQIDApTb21lLVN0YXRl
MQswCQYDVQQHDAJMQTEhMB8GA1UECgwYSW50ZXJuZXQgV2lkZ2l0cyBQdHkgTHRk
MQswCQYDVQQLDAJJVDEOMAwGA1UEAwwFc3RldmUxHjAcBgkqhkiG9w0BCQEWD3N0
ZXZlQGdtYWlsLmNvbTCCASIwDQYJKoZIhvcNAQEBBQADggEPADCCAQoCggEBAK3m
iRzfkvYn4fws14QmA1tU8e2i5XzsRsJ8WlBfrrPgM346IyA0CKJMUWkyqhu3CKfa
52m5DW/LRjfmDBflKvLkIEquNueAVilnM/hgVeRIEEdOFFwwA7vPwKVgLT/IdEsH
R5dRI0Sn31Qbjkwgz1ubY+662lqzw1HuGiWdLF8etH37JYkZnjW+JU0MJjsYj7jP
M5SZP0VBnRFsHSGvYGYzS5mYkl6hB6iXxRNEdAZI2vggkNEzusM+xrB1k+YBzc7T
nQqBHOG1KwxLKWbKi0Mr9COzS8ucKVxef/OOdUtWxIkk5CjxqBISrDRVAHTsbqZn
nPzQk5PNd4PMvDFtXjcCAwEAAaA1MBQGCSqGSIb3DQEJAjEHDAVESUdJVDAdBgkq
hkiG9w0BCQcxEAwOY2hheW1hMTIzZXh0cmEwDQYJKoZIhvcNAQELBQADggEBAIvD
wmEeXEeLutNbo7ABWM5brd6tnaPTvYY4yUp/hc8c8DwKQ8YD3n15sALYGlp7NGeO
/3wqu7xGs4sA/kDsRgALVU0BzWVBTpqaXZOYRTvcPTVkjgX9vj815CirgJ81GEig
rxTHSQ4Ev/bE0HMnh9Ccavr7Q4FS5/jOKahrvKW2wJijZYyqTbXnzGSrJwlAT26P
DAmjYrCfv5lDv1LHOlcEkBZou6tKP1VLELO5e3ZV06dhlmjfGSUIxll9HdJa+aGf
tNs+7kYHLTRA7svgrpgWjW9agYTbVjI2ILs0+X90ydKY0vKUKIb9z+O6TdAgDPx4
+4PYoLonr9+l2CcWGeA=
-----END CERTIFICATE REQUEST-----
```

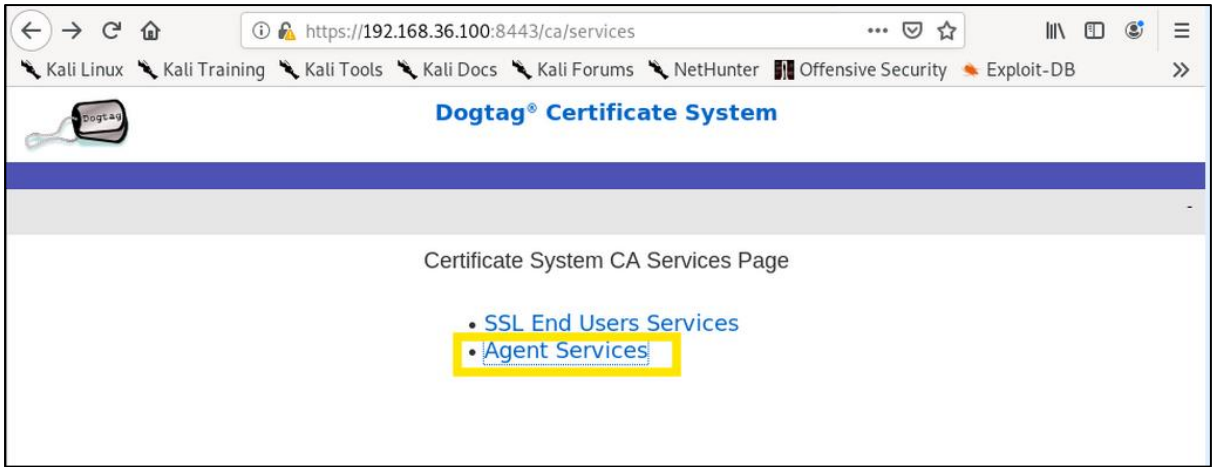
- **and paste the certificate in as below:**

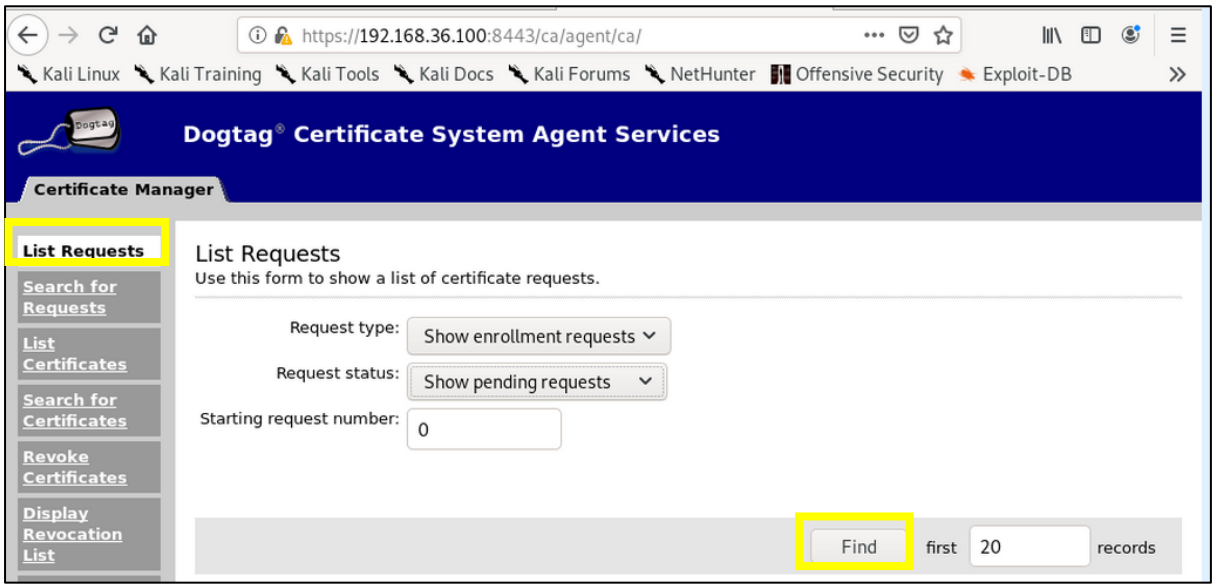


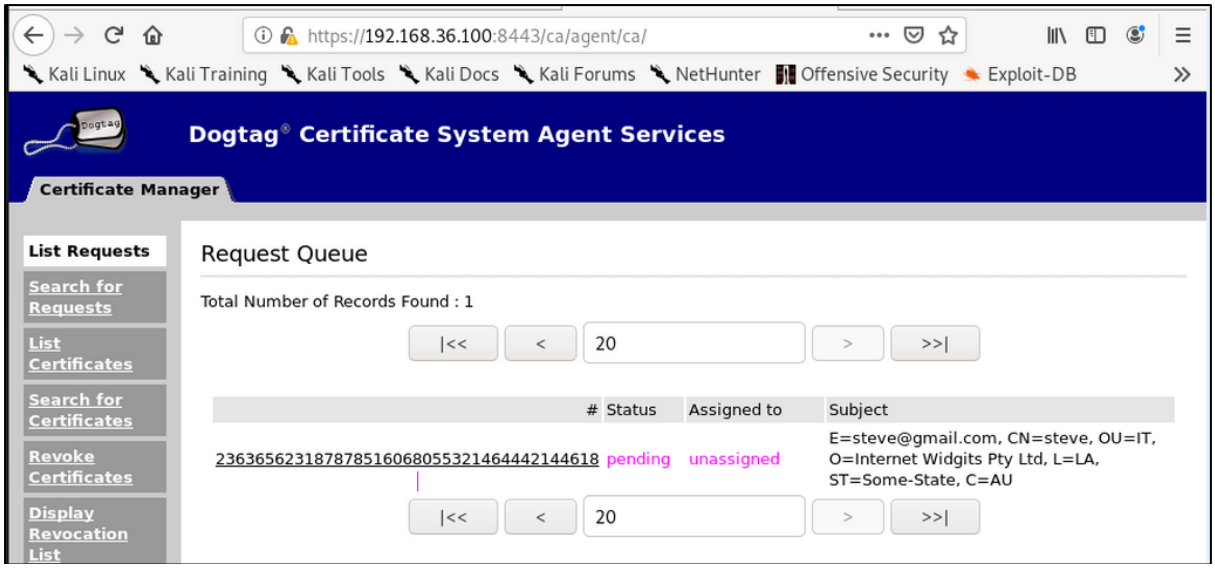
- Hopefully then (after hitting submit) we'll see:



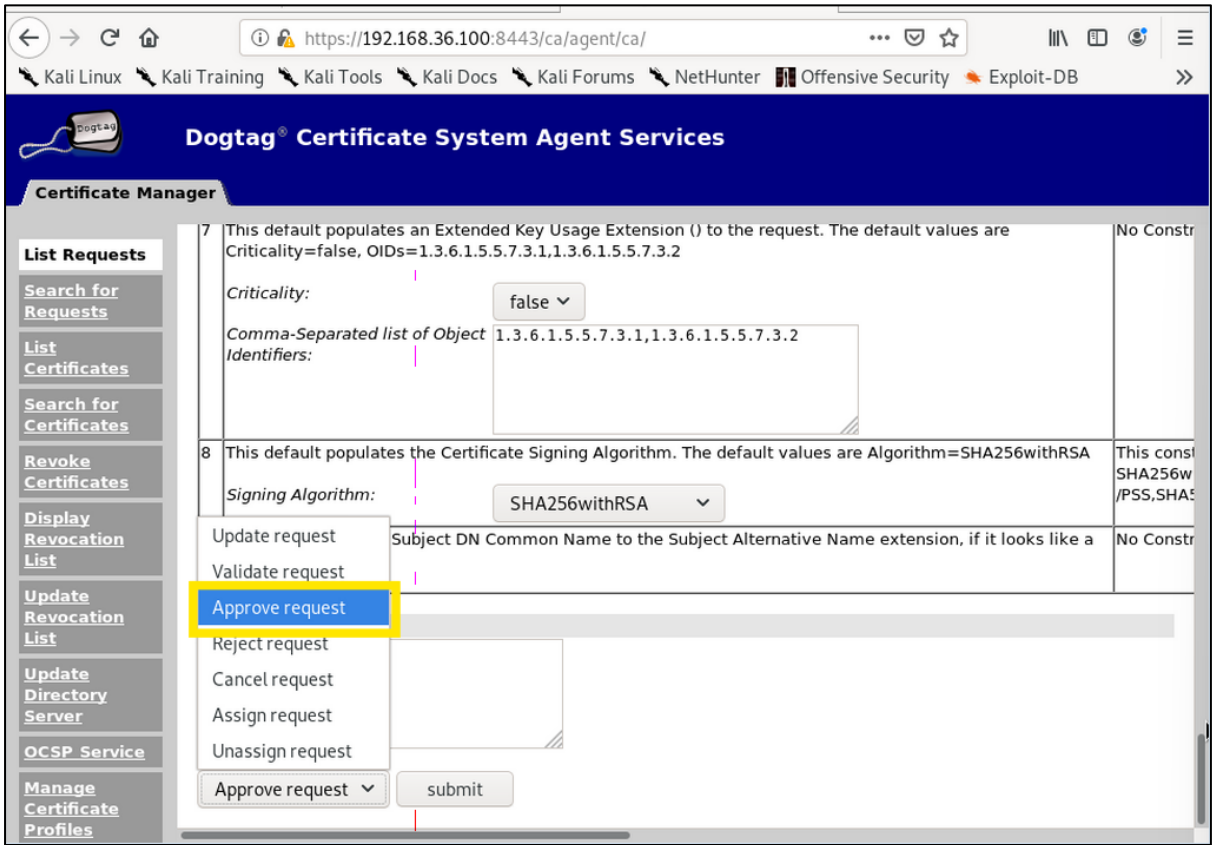
- Now - let's head to the admin section and approve the request:



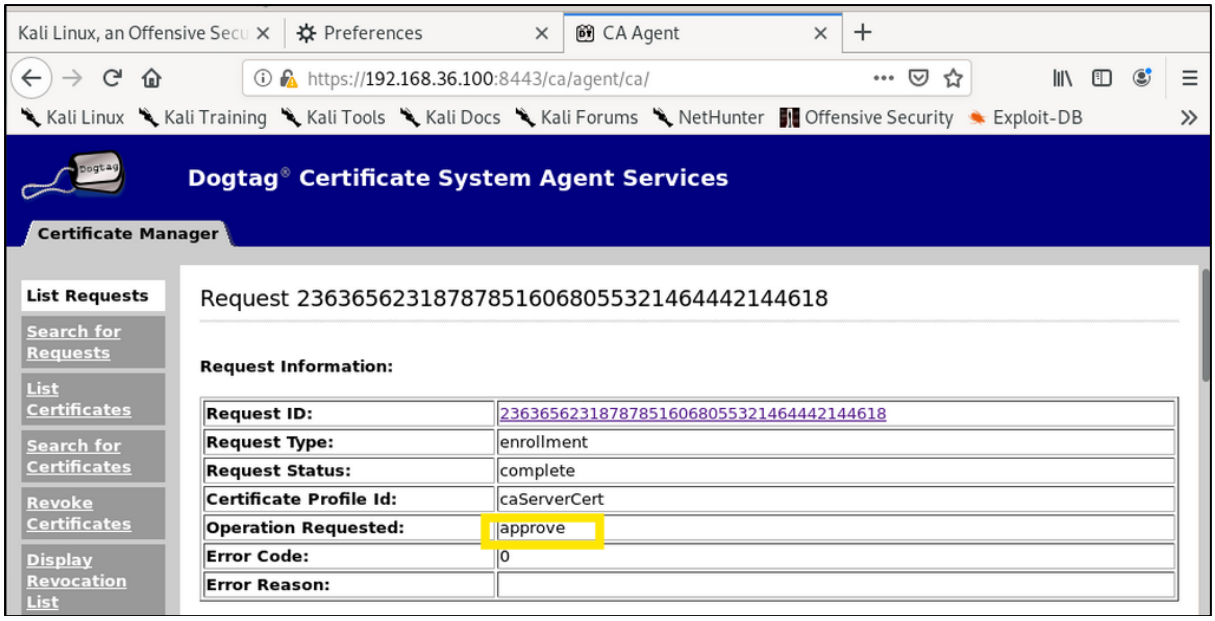


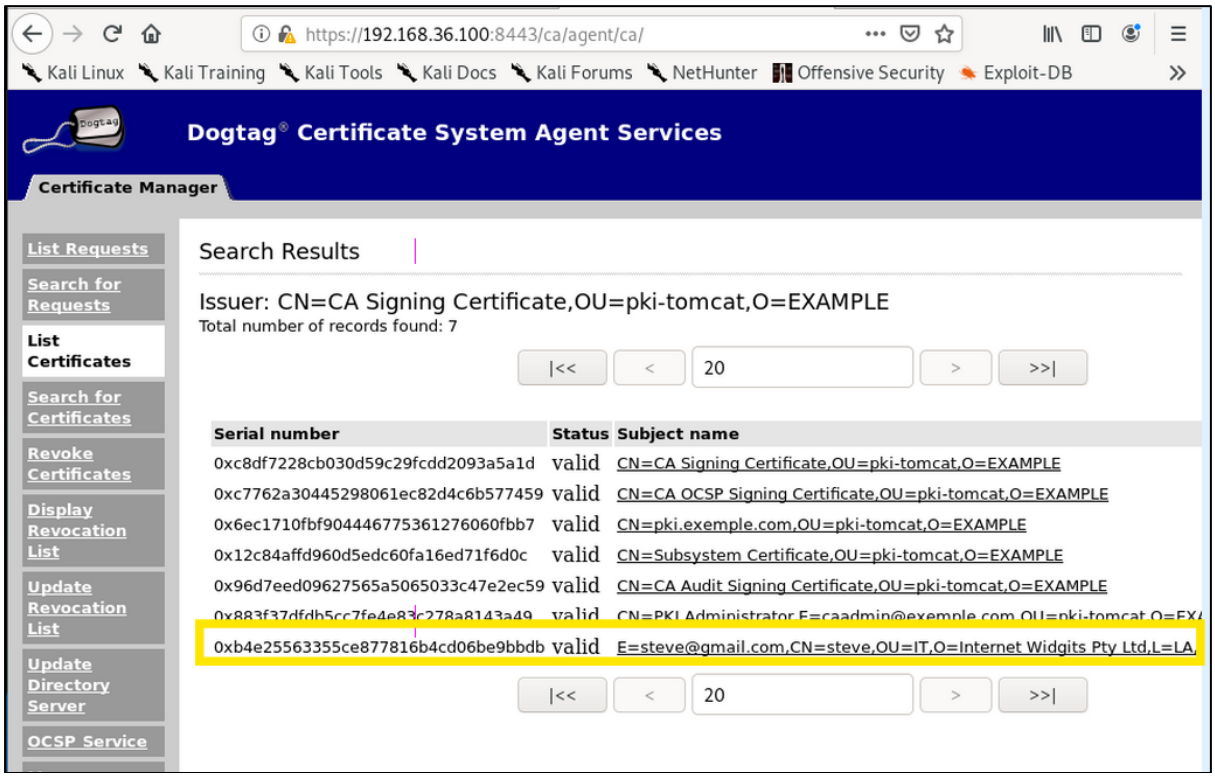


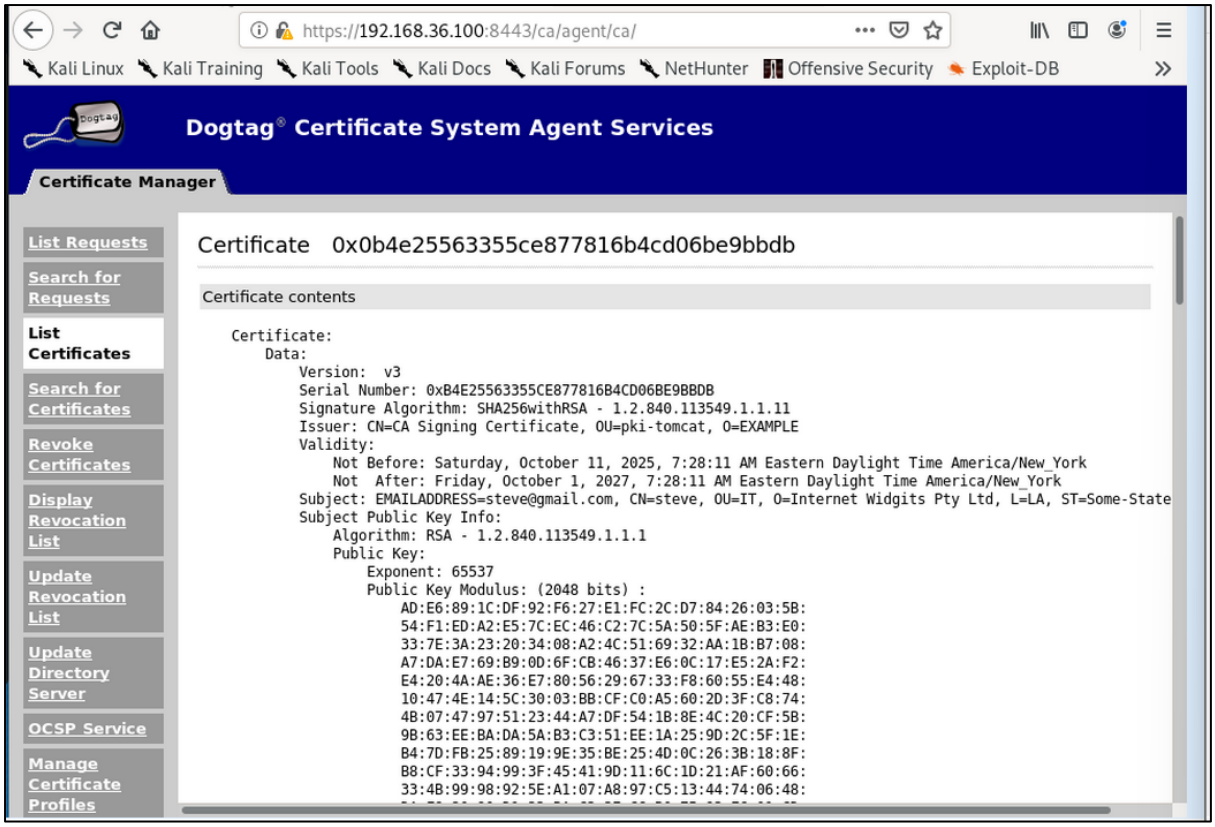
- **Click on the request, check the details etc. and finally hit 'Approve' at the bottom.**



- **Result:**


Kali Linux, an Offensive Secu
Preferences
CA Agent
https://192.168.36.100:8443/ca/agent/ca/
Kali Linux
Kali Training
Kali Tools
Kali Docs
Kali Forums
NetHunter
Offensive Security
Exploit-DB
Dogtag® Certificate System Agent Services
Certificate Manager
List Requests
Search for Requests
List Certificates
Search for Certificates
Revoke Certificates
Display Revocation List
Request 236365623187878516068055321464442144618
Request Information:
Request ID: 236365623187878516068055321464442144618
Request Type: enrollment
Request Status: complete
Certificate Profile Id: caServerCert
Operation Requested: approve
Error Code: 0
Error Reason:

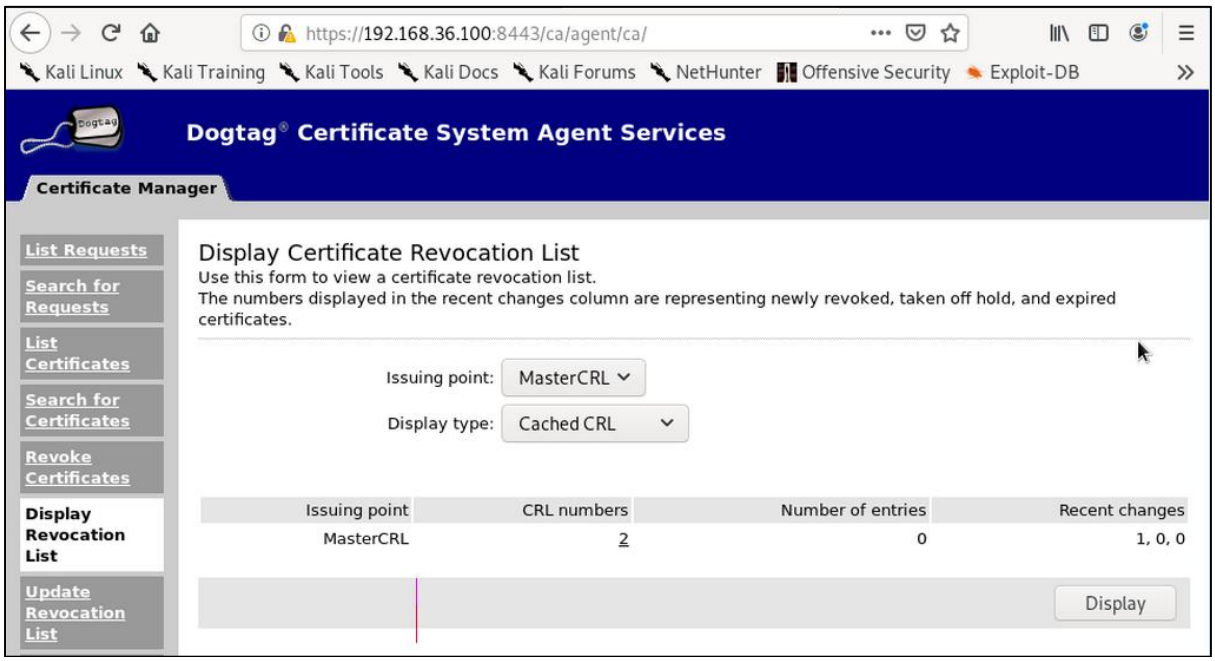

https://192.168.36.100:8443/ca/agent/ca/
Kali Linux
Kali Training
Kali Tools
Kali Docs
Kali Forums
NetHunter
Offensive Security
Exploit-DB
Dogtag® Certificate System Agent Services
Certificate Manager
List Requests
Search for Requests
List Certificates
Search for Certificates
Revoke Certificates
Display Revocation List
Update Revocation List
Update Directory Server
OCSP Service
Search Results
Issuer: CN=CA Signing Certificate,OU=pki-tomcat,O=EXAMPLE
Total number of records found: 7
|<< < 20 > >>|
Serial number Status Subject name
0xc8df7228cb030d59c29fcdd2093a5a1d valid CN=CA Signing Certificate,OU=pki-tomcat,O=EXAMPLE
0xc7762a30445298061ec82d4c6b577459 valid CN=CA OCSP Signing Certificate,OU=pki-tomcat,O=EXAMPLE
0x6ec1710fbf904446775361276060fbb7 valid CN=pki.exemple.com,OU=pki-tomcat,O=EXAMPLE
0x12c84affd960d5edc60fa16ed71f6d0c valid CN=Subsystem Certificate,OU=pki-tomcat,O=EXAMPLE
0x96d7eed09627565a5065033c47e2ec59 valid CN=CA Audit Signing Certificate,OU=pki-tomcat,O=EXAMPLE
0xb4e25563355ce877816b4cd06be9bbdb valid E=steve@gmail.com,CN=steve,OU=IT,O=Internet Widgits Pty Ltd,L=LA,
|<< < 20 > >>|



Certificate Revocation Process

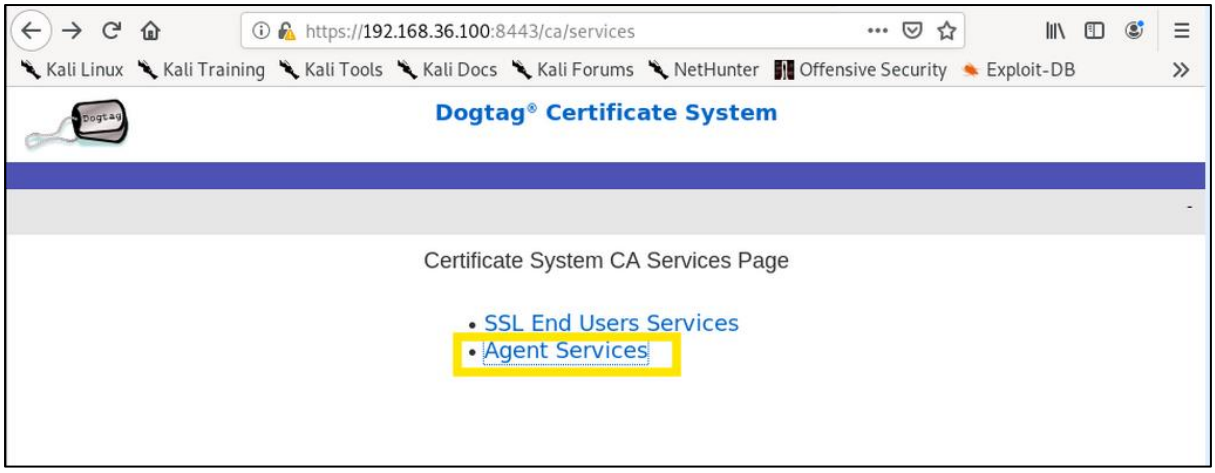
Pre-Revocation Status:

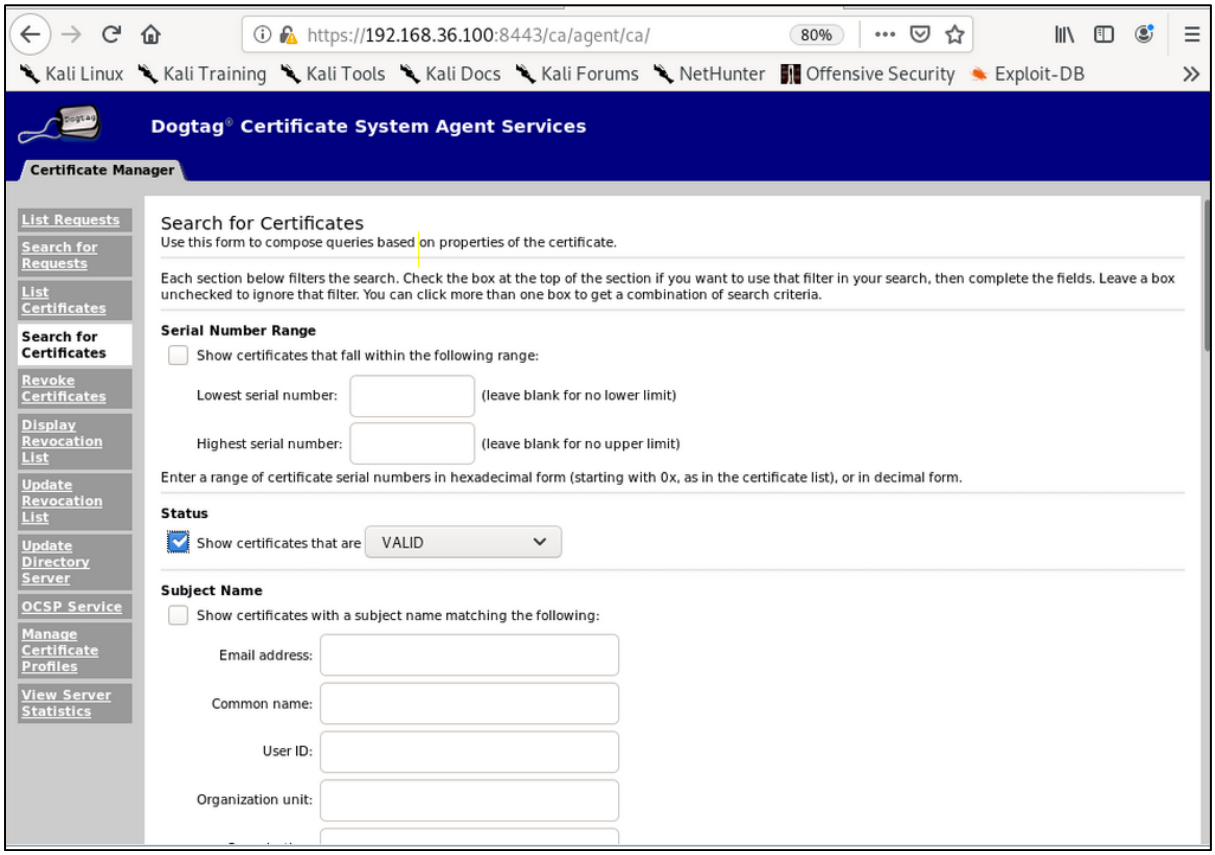
- **CRL entries: 0 certificates revoked**



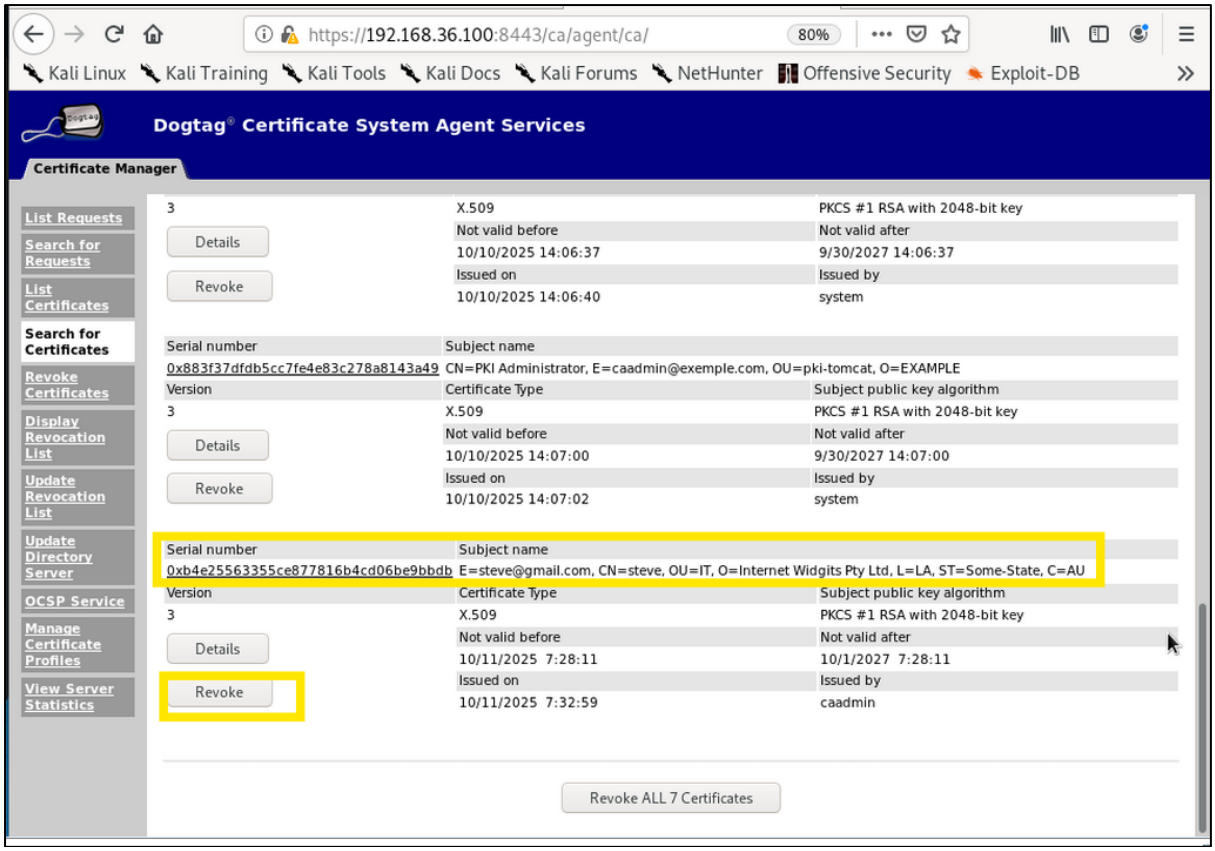
Revocation Steps:

- Access "**Agent Services**" → "**Search for Certificates**"

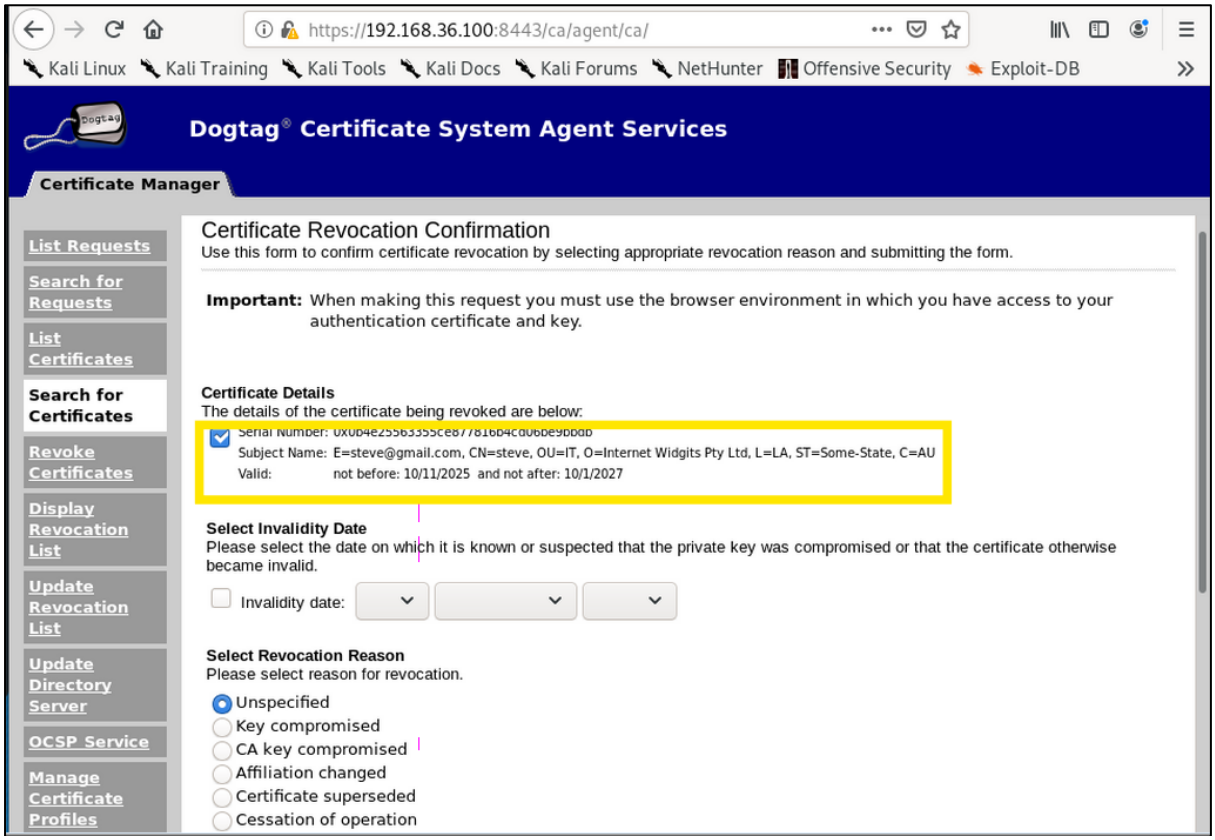




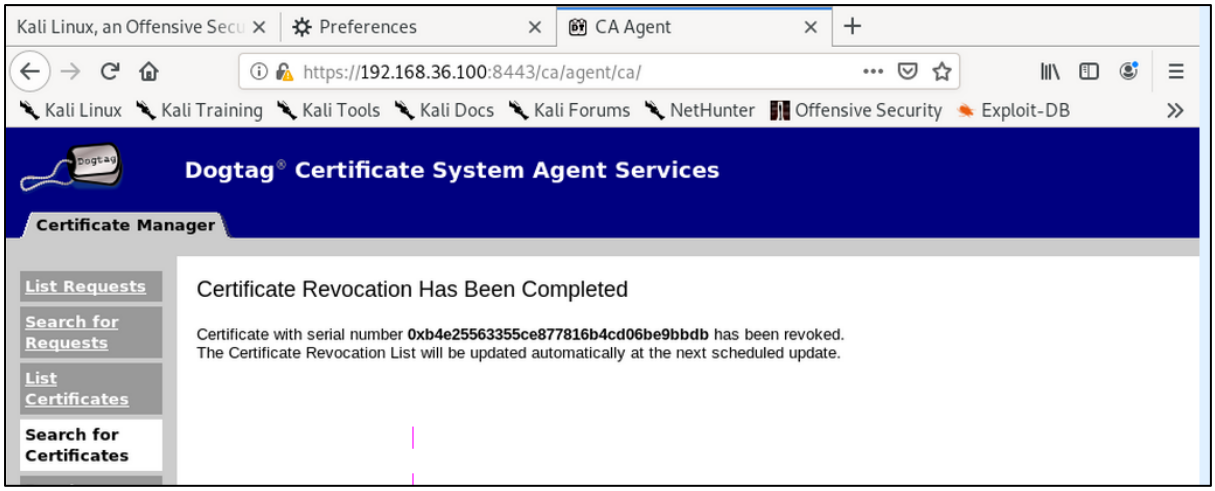
- Select target certificate from active certificates list



- **Choose revocation reason (e.g., "Unspecified")**

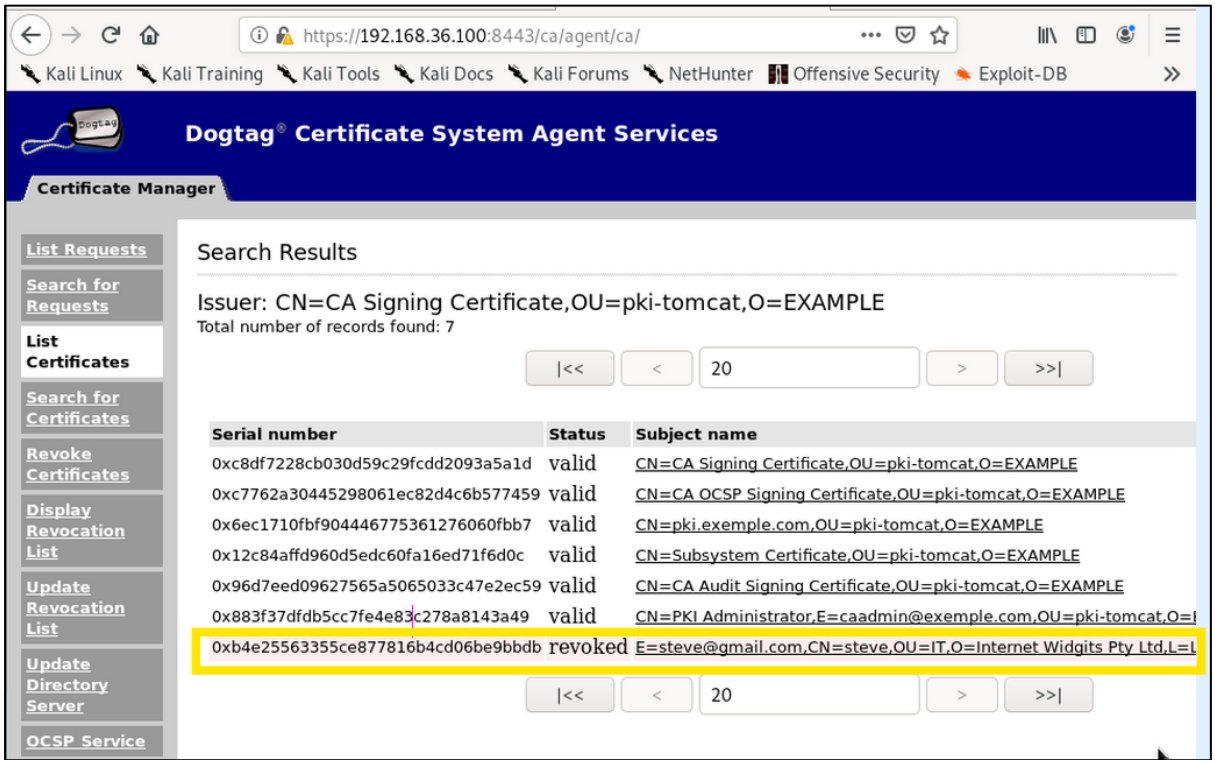


- Certificate immediately is added in revocation list

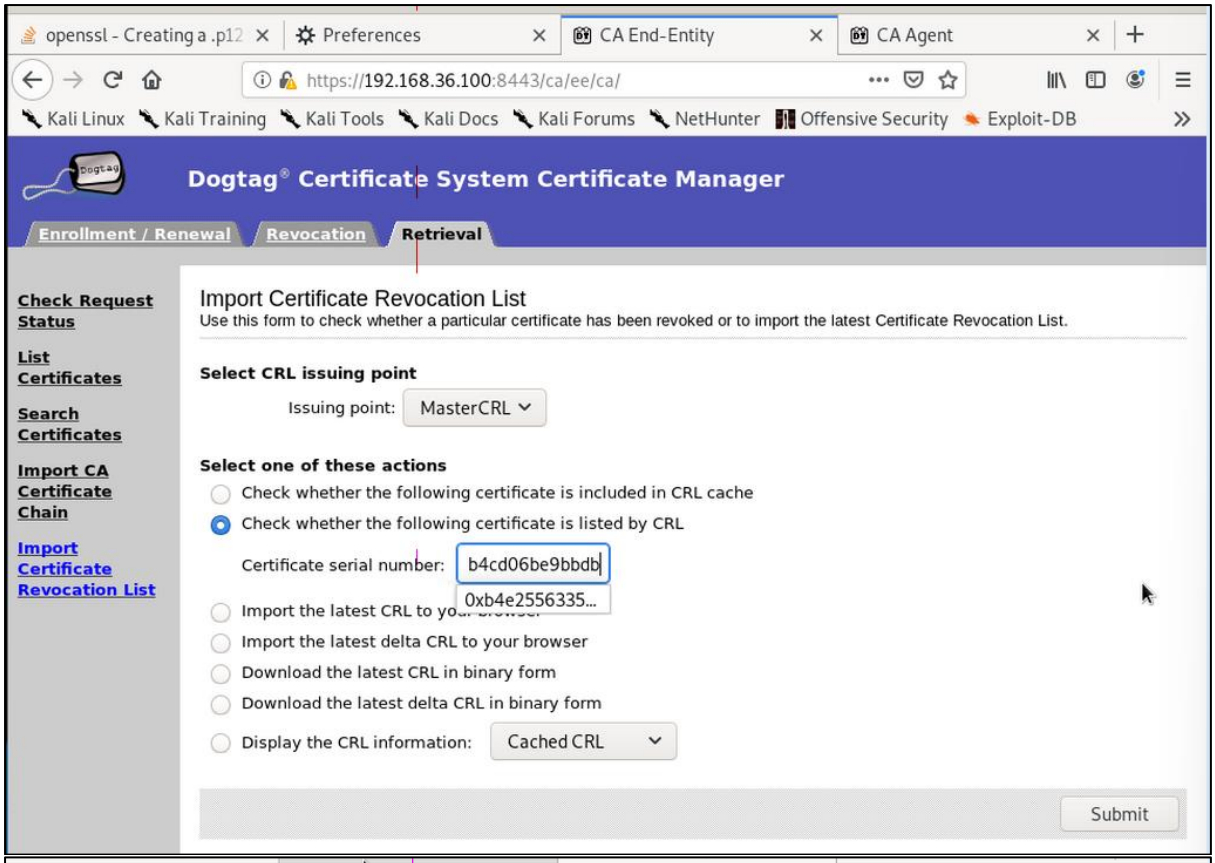


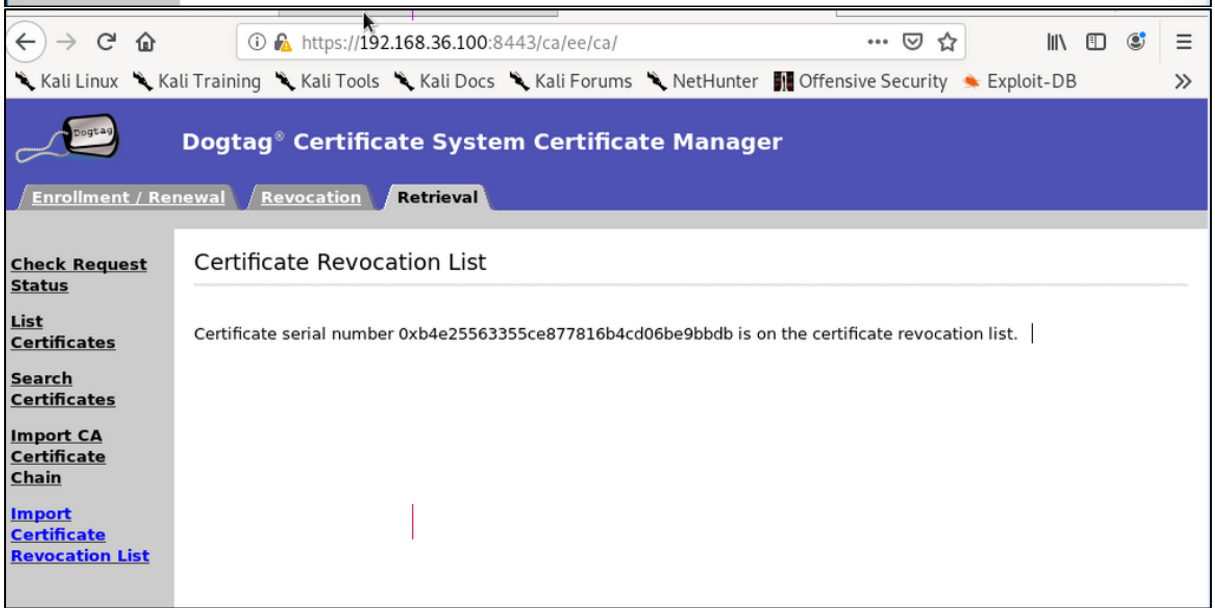
Post-Revocation Verification:

- Status changes to "Revoked" in certificate database



- **In SSL End user services:**





Certificate Revocation List (CRL) Management

CRL Monitoring:

Navigate to: " Agent Services " → "Display Revocation List" in left menu

You'll see current CRL information:

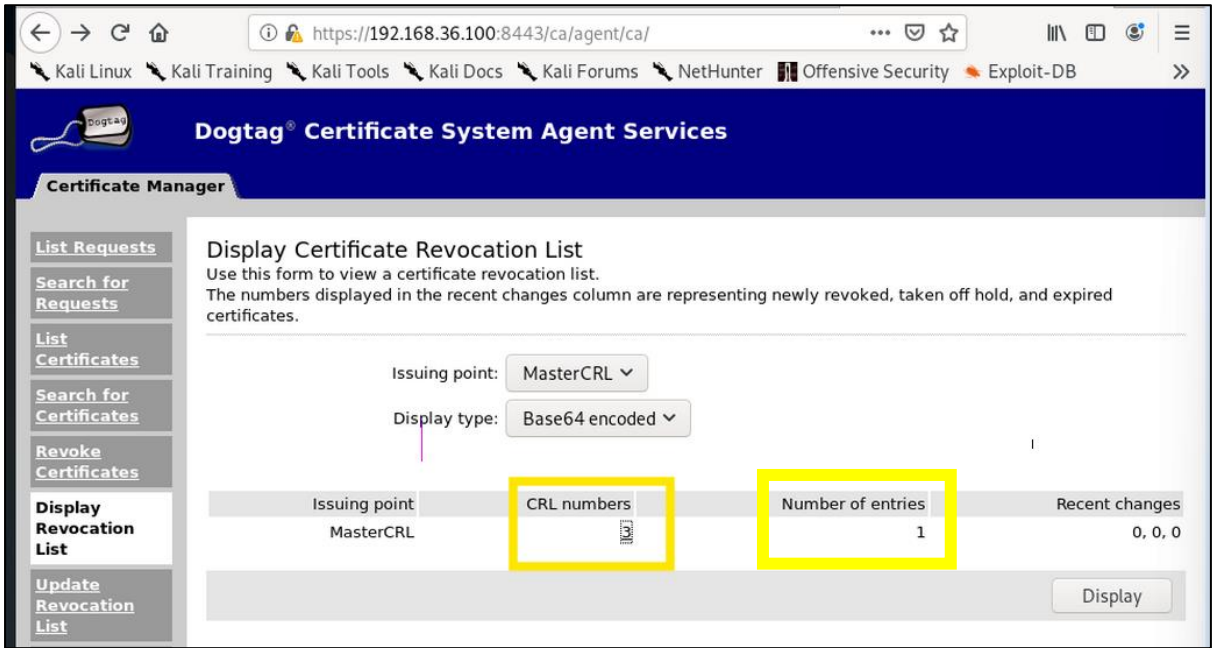
- CRL Number
- Issuing point
- Recent updates

Number of Entries = Nombre de certificats révoqués

- C'est le contenu de la CRL
- Combien de certificats sont actuellement révoqués
- Statique entre les mises à jour CRL

CRL Number = Numéro d'opération

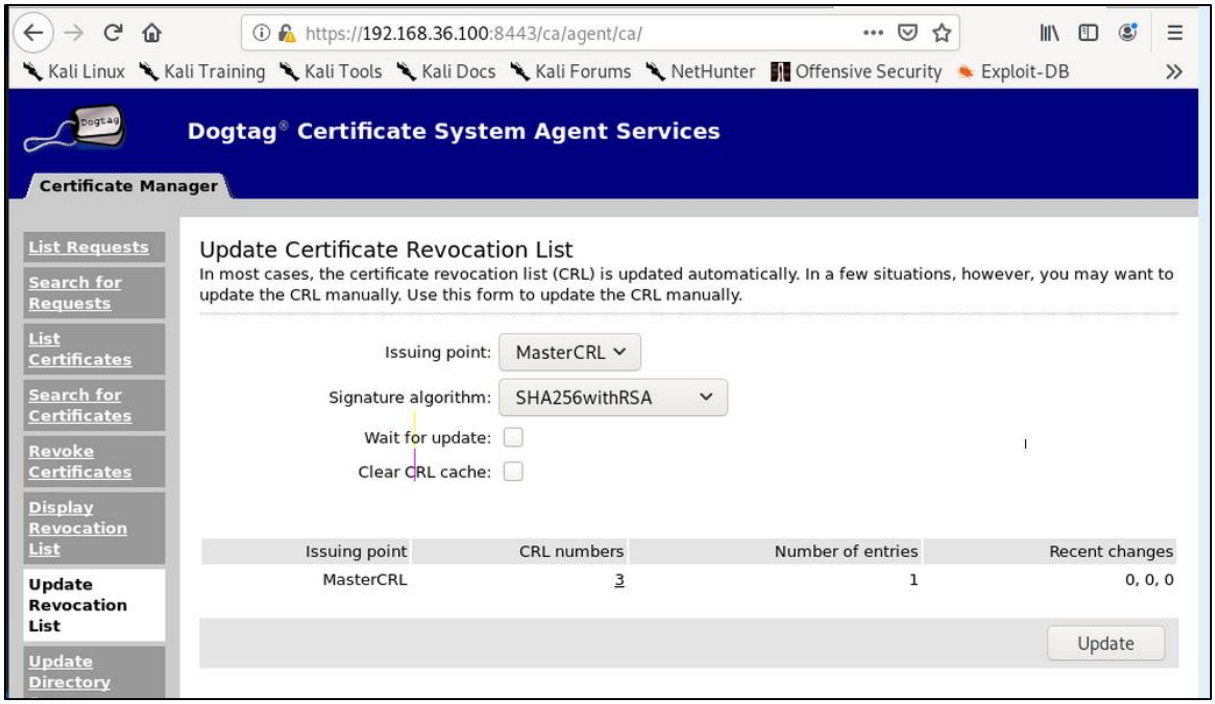
- C'est le versionnement de la CRL
- Combien de fois la CRL a été générée
- S'incrémente à chaque nouvelle génération



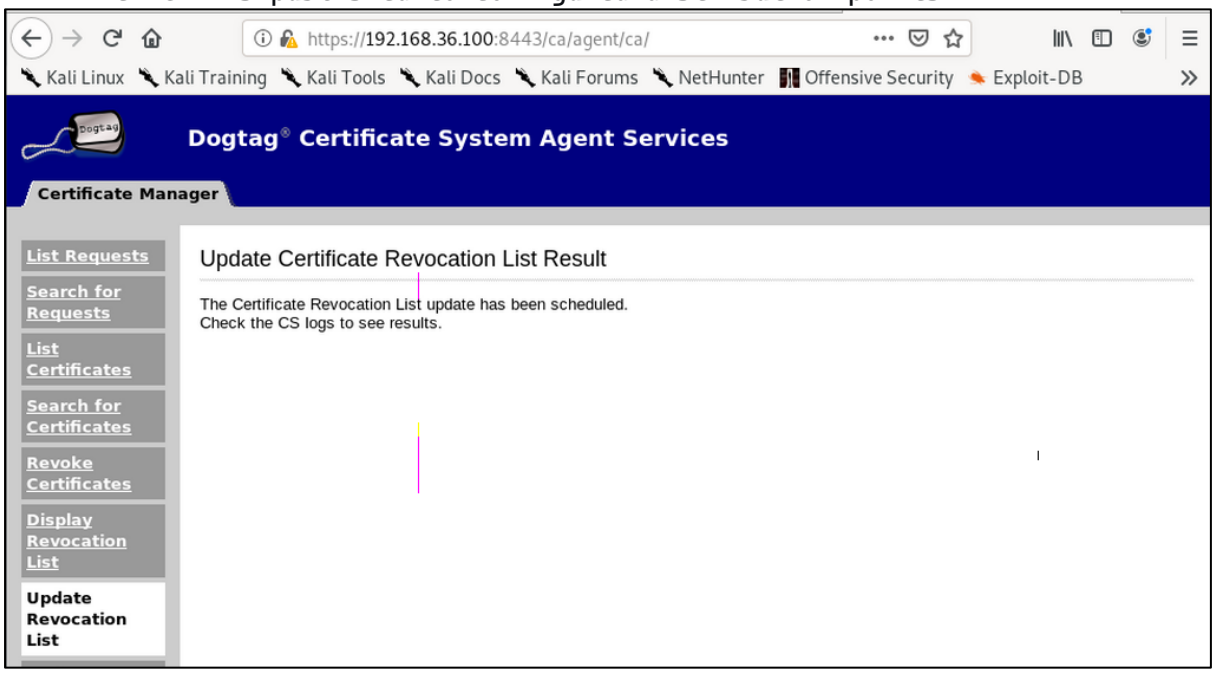
After revoking a certificate, it is automatically added to the CRL, but a manual CRL update can also be performed.

Manual CRL Update

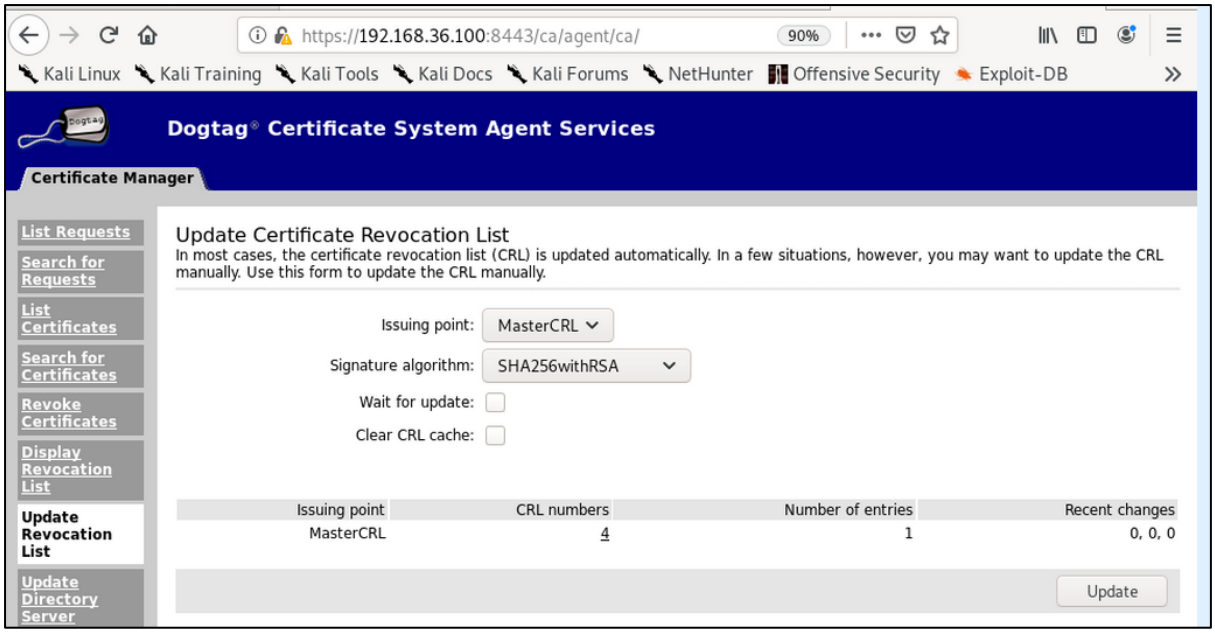
- Click "Update Revocation List" to generate new CRL immediately
- Confirm the update



- New CRL is published to configured distribution points



- **The increase of the CRL Number from 3 to 4 confirms that the CRL update operation was successfully triggered and executed after the certificate revocation.**



Ressources :

- GitHub - dogtagpki/pki: The Dogtag Certificate System is an enterprise-class Certificate Authority (CA) which supports all aspects of certificate lifecycle management, including key archival, OCSP and smartcard management.
- Quick Start · dogtagpki/pki Wiki · GitHub
- Install Dogtag Certificate System and deploy the subsystem - HSM Integration Guides
- Configuring Dog Tag (PKI) Certificate Authority on Fedora ~ Peter Manton :: Tech Notes
- How to use Dogtag PKI to setup Certificate Authority Server in Linux
- CA User Guide · dogtagpki/pki Wiki · GitHub
- Administration Guide · dogtagpki/pki Wiki · GitHub