PKI DR18

Notre petite PKI… ne connait pas la crise

Sommaire

Architecture v1

Besoin 1

Eliminer les certificats auto signés

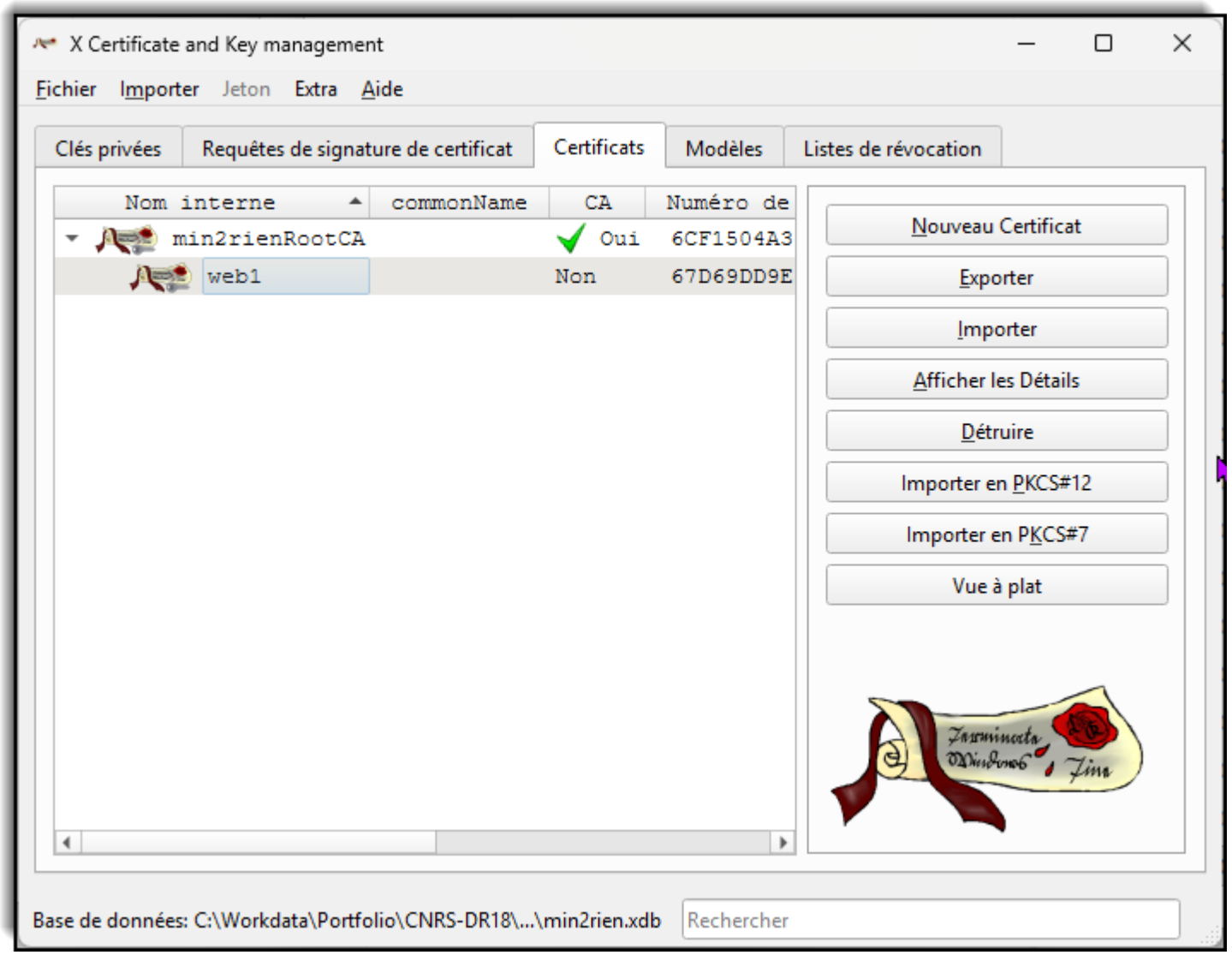
- Pourquoi
  - Permettre aux agents de respecter les recommandations de sécurité
  - Simplifier l’administration des postes

- Contrainte
  - Installation minimale
  - Utilisation simple

Solution 1

XCA - https://hohnstaedt.de/xca

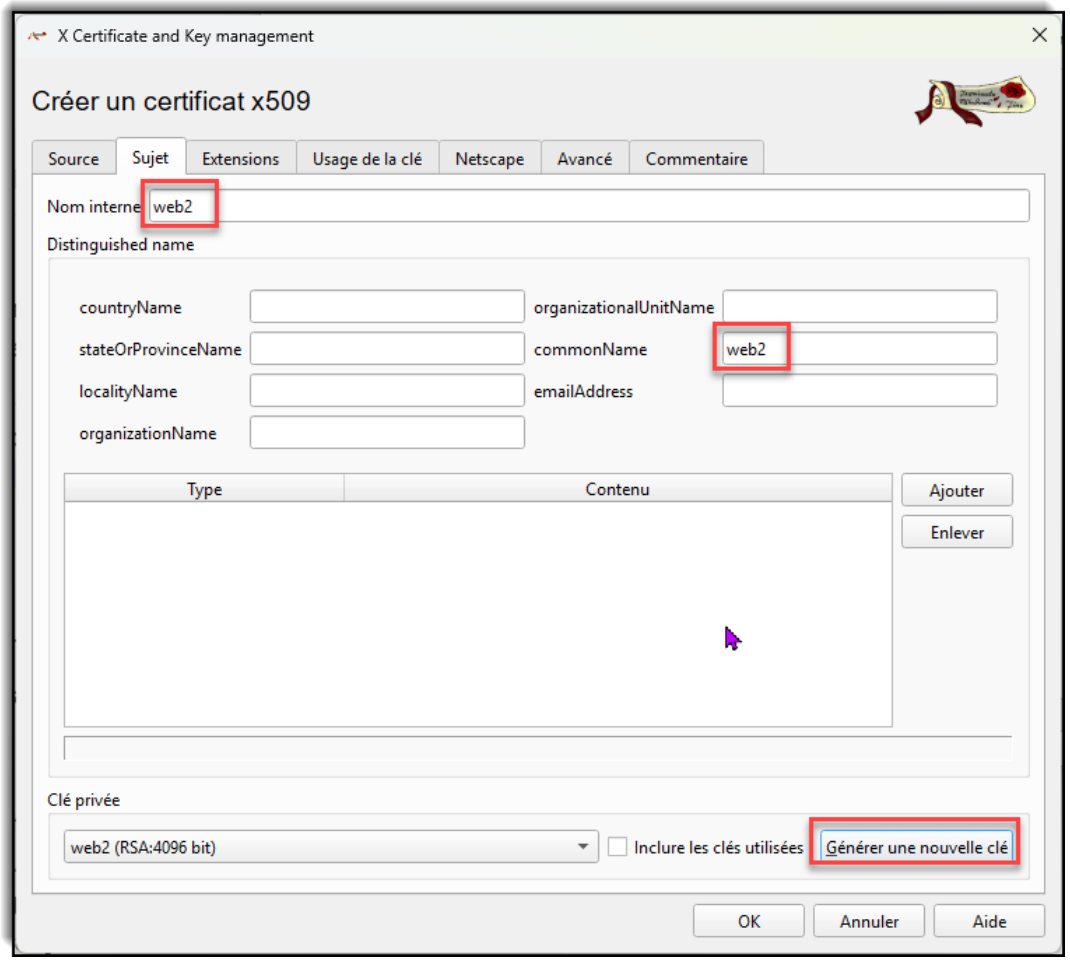
- Une application
  - Windows,
  - Mac,
  - Linux
- Un CLI
- FOSS
  - OpenSSL
  - QT
  - SQL lite

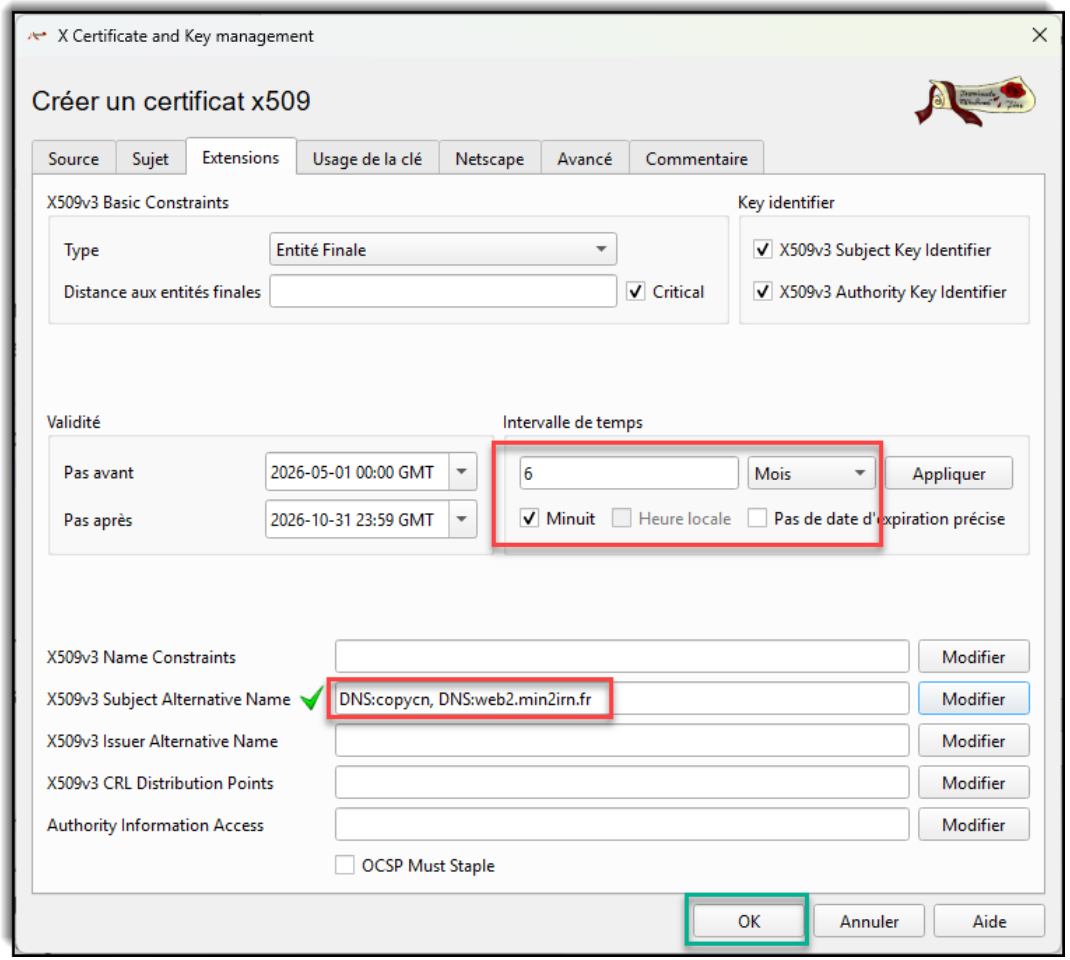


https://www.arsouyes.org/articles/2019/38_PKI_avec_XCA/

Démo XCA

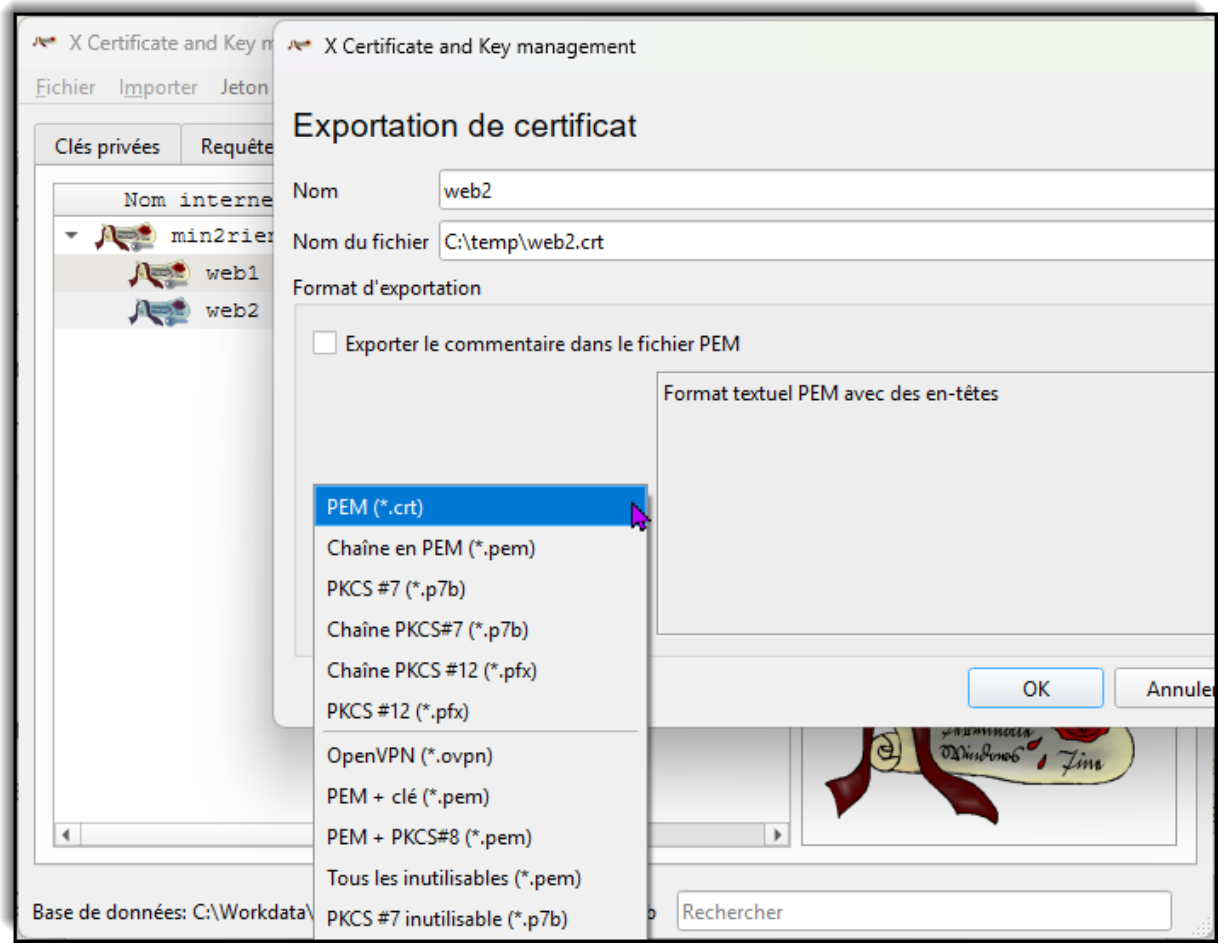
Créer un certificat





Démo XCA

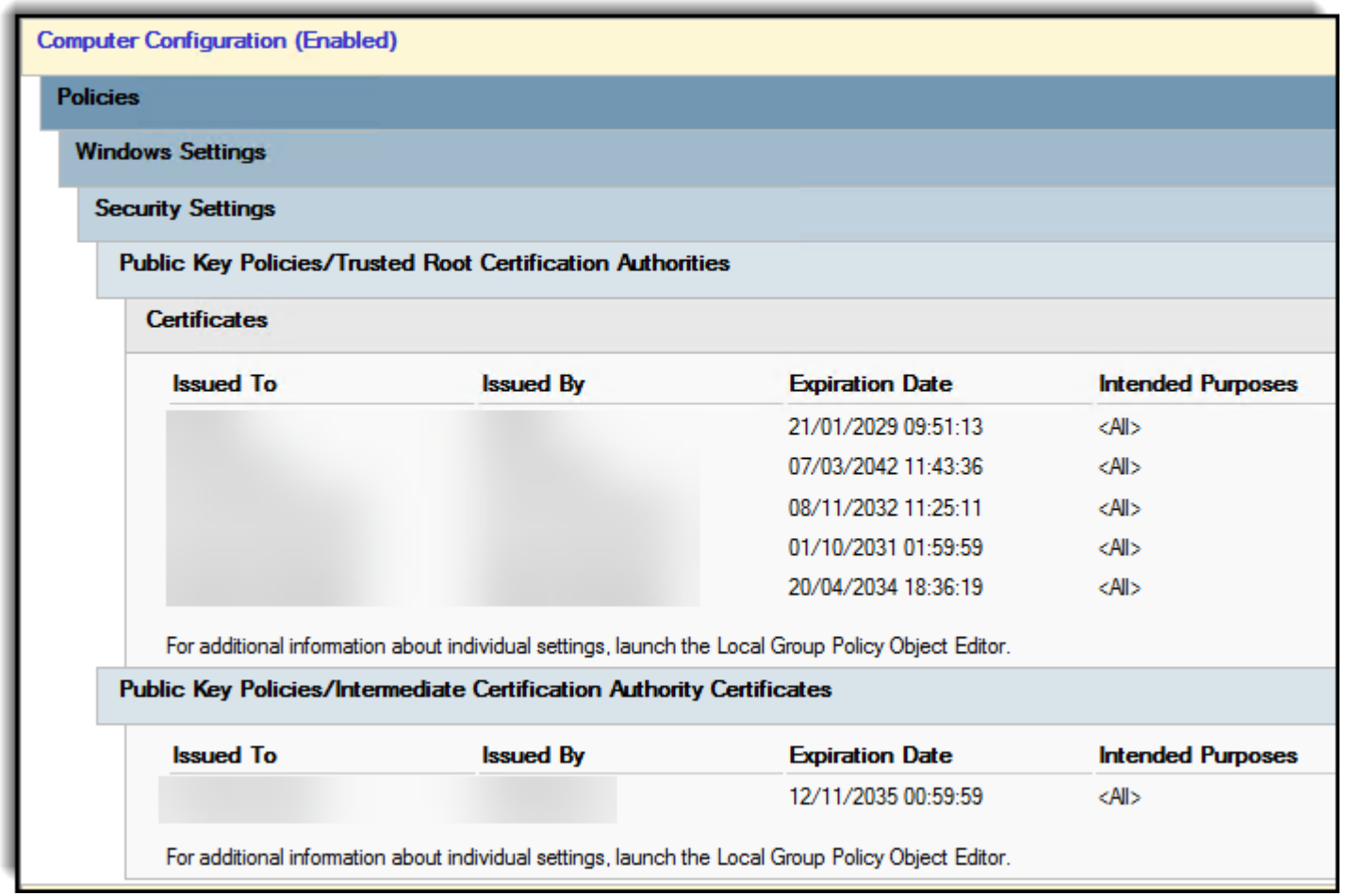
Exporter un certificat




```
qzq3vMC++wSIJ5lb7l6D2VgWQ6armq5PAHcbjqSvAoIBAQDhu55wudTwoFemPUqb
ZIEtHmBQY+705veB452tpwtNjFQQ9CgwBQJwD9YirnPN8M83VUX863sIkcgumf9n
RyAzt839bXHRgApwUD1VAlwT/93j+FHQGOaBDM15NCZuvRRn3MXY9pu6V1bHETcE
O/+A3Hng49V9x86D/h2FXqw3a1kiM77nZWkpV8F4KTHpLuN9sVEP7cJOaGjFMmMD
+jYIJBMjro+8eOABlSG304otmT67iCIUmUaM3WjIIkDKU7T52W9KRx52eBuXURC8
RvTNHngM88343PpXqiT2I4FePSscy8xyEJ6S9or8uVg/socemrqQeaft+9RnN37N
CsiRAoIBAFFjld0xJQXfCme4XEKeGsoZCVZpdj21t65oz9+dBHRjfyCdsYcHfV4f
eGWeEcM5Rn7sy4olc1Dx13sMUfTar1KuLdYI912/9C93oruevakqOferYgG/2Y2W
fqs+65LlHuMYExXs0d2SCNW5Gp32OK7isOrzTOGTHbxfdjFrvMYyqB41evzSXYyX
V6RSX4xKZtuE+Zlc8g895d8TT1NGSVssVM+U3mmPHGNzlfa55eNd8ziwfOQXzltu
yOv1m5ZRZtK7/fDG7/i5y1wtWwMXsciIf/KSS6k3IWIiS+wiHpVG7WfNaat9g2SF
Z5Mn7oScMcEK+MmQ/ZjSmmHaly3R6UkCggEADKwJW56m9kQtke4xqIV7eg+YuCGT
ZGAdCUOLMXZat4kjLoXyu3nIlCuYjPR8iqZZ2gsFamDsO0M4i5oCYFkwL5FwWnOj
nN6S3YTXnAN2NCwGp2p1sLCAHtMSqPSql9bzMygkTulu5KNrgc9pl4veVGtyAP3G
PCCHHCQnQ9bE6drhdsqfVSglTa2RqnJ5BaX7Z/wAP2Gv+TwC8O0Haf82SUavBN5b
eMU1Yy2IU6oFaqx0mPzyAemKUmuHYGsw+NeifvOTBvmMvrmO16M4YscvI/v8hcpV
me83rC3r5qjm+Y7wXBZVYq4Lav/cLloMhfdFsz26dw+JCP0OMFNzo11rlA==
-----END RSA PRIVATE KEY-----
-----BEGIN CERTIFICATE-----
MIIFWjCCA0KgAwIBAgIIGUsIcGpD7uUwDQYJKoZIhvcNAQELBQAwADAeFw0yNjA1
MDEwMDAwMDBaFw0yNjEwMzEyMzU5NTlaMA8xDTALBgNVBAMTBHdlYjIwggIiMA0G
CSqGSIb3DQEBAQUAA4ICDwAwggIKAoICAQCoBCXMqmgy1b/w8a0DzcFBVn6zJbPx
rU1dM34acl3ojICNRCgn3kMtQ1EzWJ4ZoQMf4kSVBfODbXhSYOL7AJpsCddDeH/S
Kn/szTfuumolC6iUA+bjsUFJFDYd/BpoL3Ajb3MaF/8hQqzD89F3NDF7LOGZbfqx
kriixcCpgjmEBQ3F4Ln22YsCV9MAZBm2mV4bTGSpmYVfiwS4FRnhQc/a8fN2WwP7
83xKnThPIY12/u0ghibHOLLWdJ17dAC0N7ofCzIwdzh9oUcDAVdzL6S0oBMhOyHu
eRPJHa5egPN5/xzEg6xnWv0zOeXM8ec3ttF6zV0J52LLDCNGXaptbeL6ggWwiaGw
003C5mzGQ91fII4cOREhH6cSYt2VdUI7OD4RuompxguSAlXDTgqj2iej2z2r3V0S
9JeE8Dk+CGdduCMW9EuIgWGVh4Yr34t44TbpHbdjsMEKXdXmLcpnxIy+oxnGTAhd
zqWk3Jp+8hCKpPpgvodPZTSgj4HcGjAkNKBw6TUsXJaTWlrJPYm6zMbBTSThfQq0
```

Une GPO

Distribution des racines sur l'ensemble du domaine AD.



Besoin 2

Authentification 802.1x

- Pourquoi
  - Authentification des postes pour l’accès au réseau (802.1x)

- Contrainte
  - Automatisation de :
    - La génération des certificats
    - L’installation des certificats
    - Le renouvellement des certificats

Solution 2

AD CS

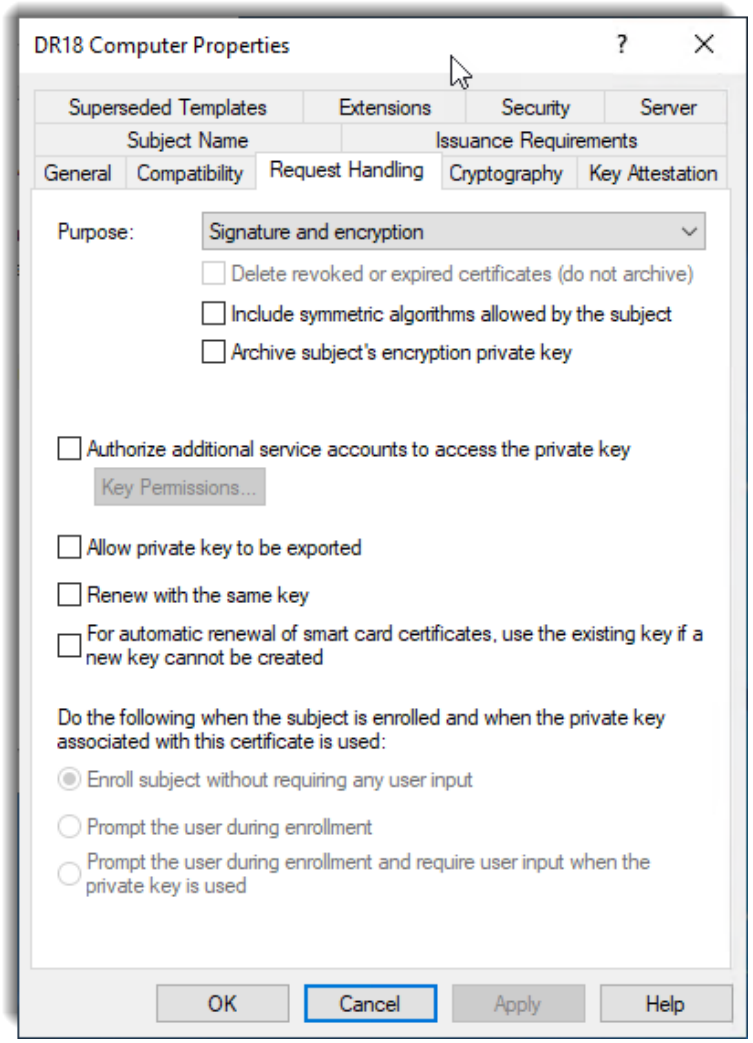
- Evidence
  - Environnement AD DS
  - GPO
- Architecture de référence
  - 1 serveur CA Racine (éteint)
  - 1 serveur CA intermédiaire
- Automatisation
  - Template AD CS
  - GPO
- Pas de self service (petit potam)

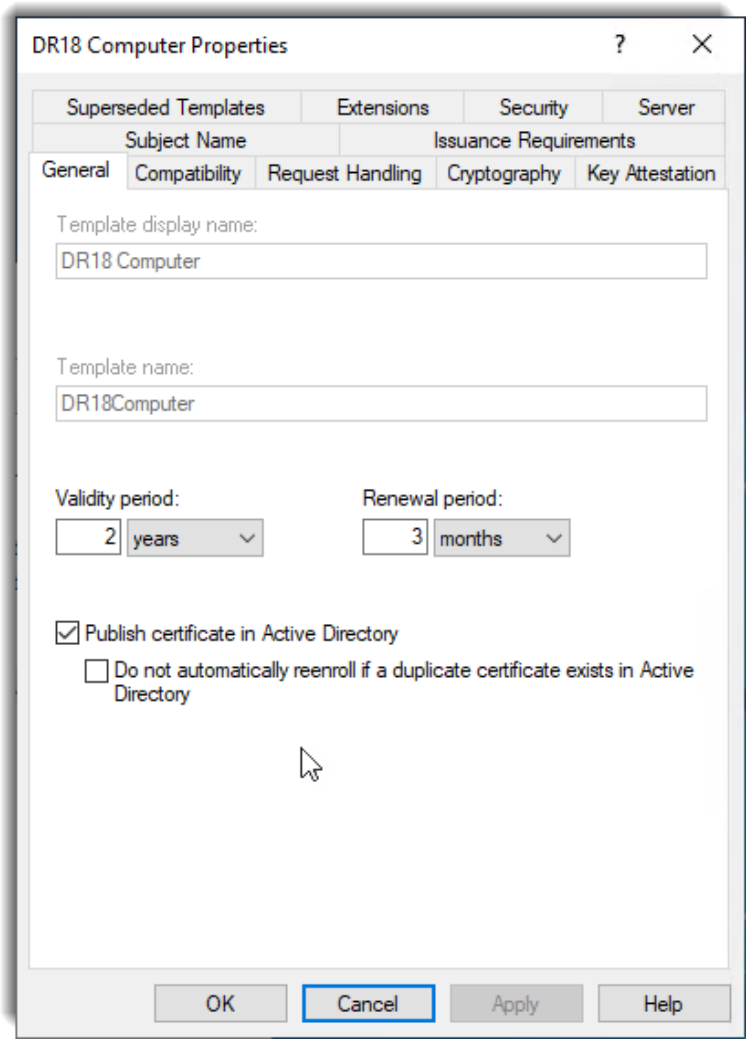
Quelques guides

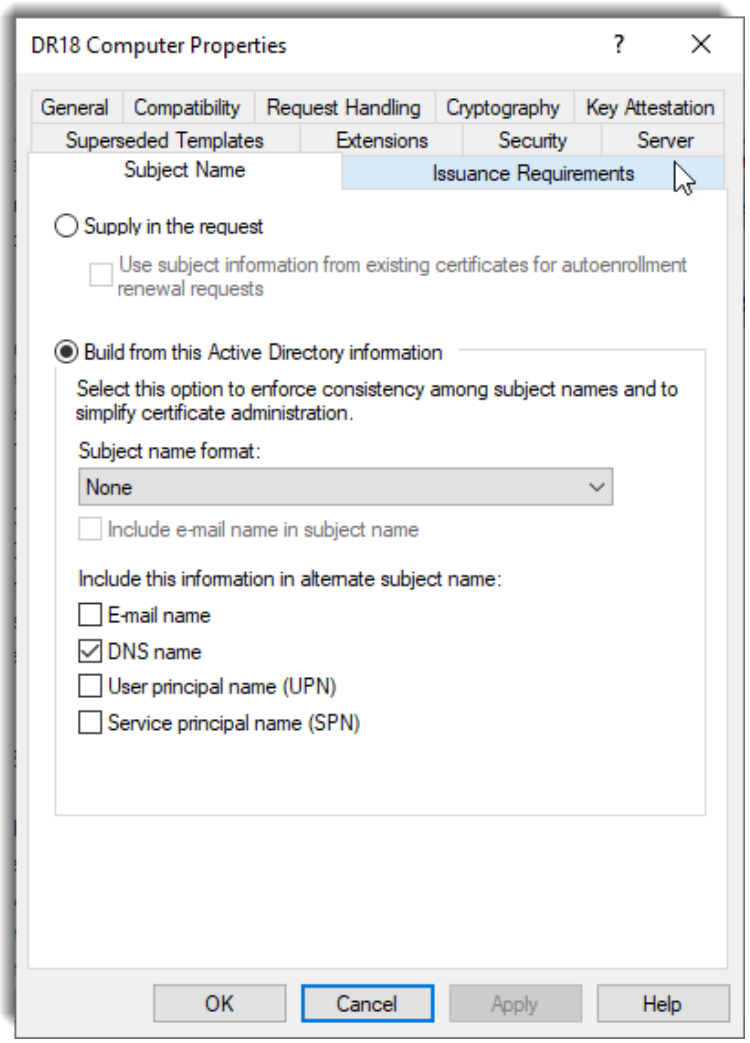
- https://mjcb.ca/publications/practical-guide-to-pki-with-windows-server-second-edition/
- https://github.com/cfloquetprojects/homelab/wiki/Deploying-Offline-Root-CA-in-Windows-Server-2019
- https://www.it-connect.fr/cours/ad-cs-autorite-de-certification-windows-server/

AD CS

Le template







AD CS

GPO d’enrôlement

Delegation

These groups and users have the specified permission for this GPO

Name	Allowed Permissions	Inherited
\Administrateurs de l'entreprise	Edit settings, delete, modify security	No
\Admins du domaine	Edit settings, delete, modify security	No
\ggc_	Read (from Security Filtering)	No
\gr_p	Read (from Security Filtering)	No
\Ordinateurs du domaine	Read (from Security Filtering)	No
NT AUTHORITY\ENTERPRISE DOMAIN CONTROLLERS	Read	No
NT AUTHORITY\SYSTEM	Edit settings, delete, modify security	No

Computer Configuration (Enabled)

Policies

Windows Settings

Security Settings

Public Key Policies/Certificate Services Client - Auto-Enrollment Settings

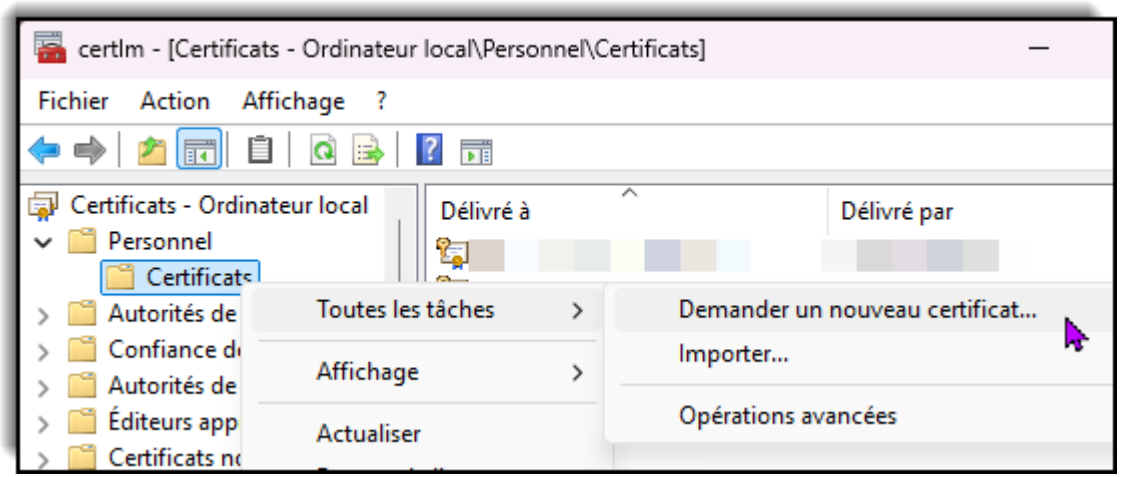
Policy	Setting
Automatic certificate management	Enabled

Option	Setting
Enroll new certificates, renew expired certificates, process pending certificate requests and remove revoked certificates	Enabled
Update and manage certificates that use certificate templates from Active Directory	Enabled

Test AD DS

MMC Certificat ordinateur

- Présence du certificat
  - Personnel > Certificat
  - Si absent
    - GPResult /z /scope computer



- Test de la délivrance
  - Personnel > Certificat
  - Demander un certificat
  - Sélection du modèle

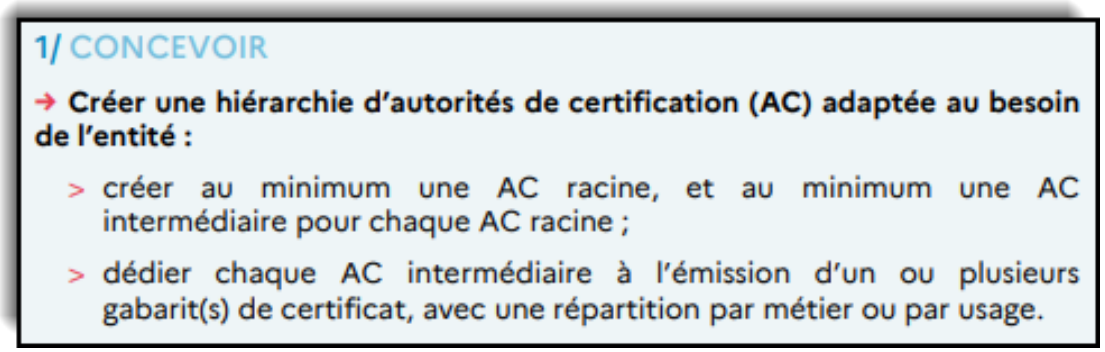
Architecture v2

Tout va bien… mais !

- Nous avons 2 CA racines
- CA racine AD CS rarement maintenu
  - VM éteinte
  - Oubli des MAJ
- Le SSI à toutes les clés

Publication ANSSI

- Août 2025



1/ CONCEVOIR

→ **Créer une hiérarchie d'autorités de certification (AC) adaptée au besoin de l'entité :**

> créer au minimum une AC racine, et au minimum une AC intermédiaire pour chaque AC racine ;

> dédier chaque AC intermédiaire à l'émission d'un ou plusieurs gabarit(s) de certificat, avec une répartition par métier ou par usage.

→ **Protéger les clés privées des certificats :**

> stocker les clés privées des AC racine hors ligne, idéalement dans un équipement sécurisé de type HSM (*Hardware Security Module*) ;

> stocker les clés privées des AC intermédiaires en ligne dans un équipement sécurisé de type HSM ;

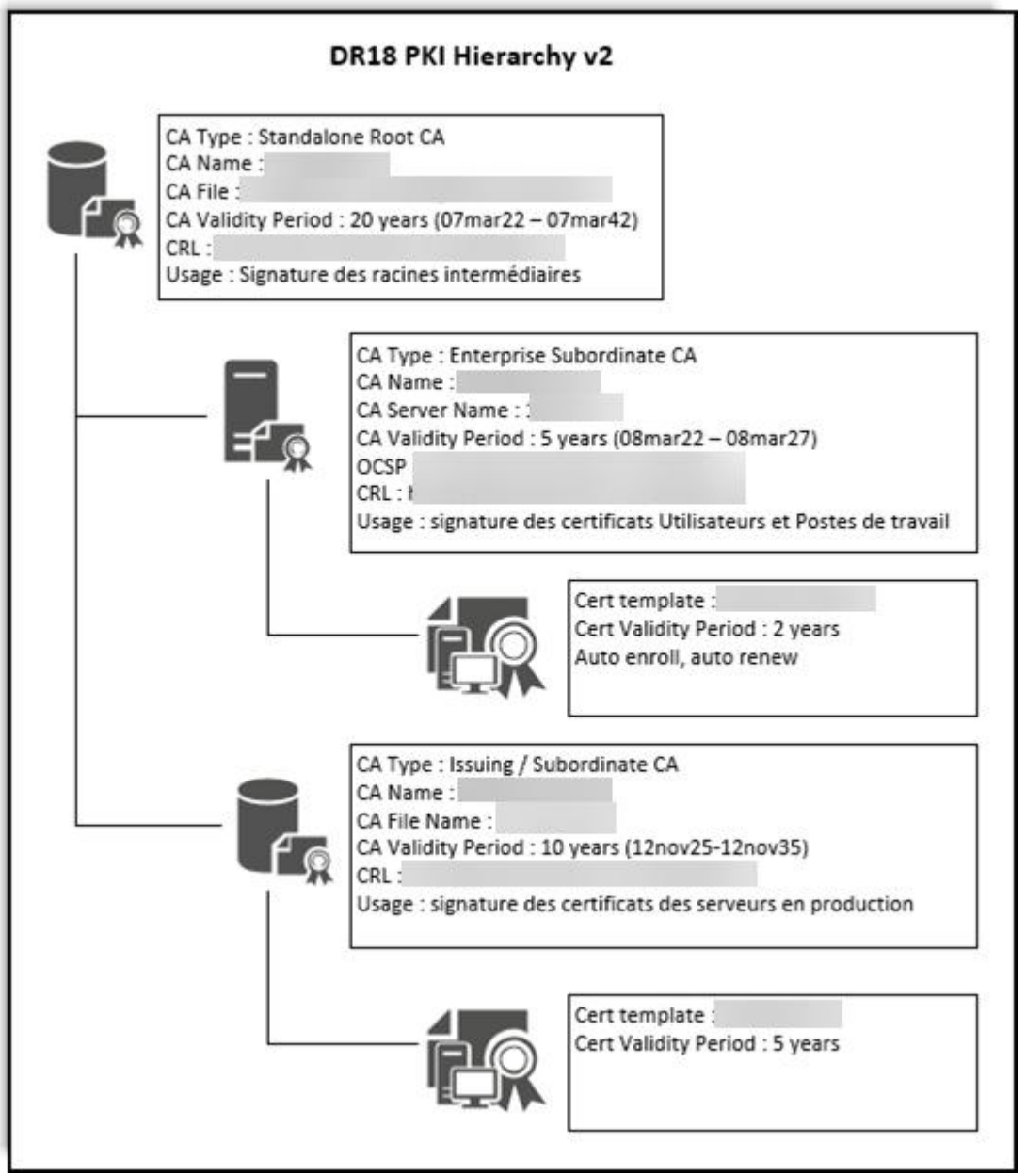
> protéger les clés privées des certificats d'entité finale par du contrôle d'accès et, idéalement, par du chiffrement. Ajouter une protection matérielle lorsque le niveau de sensibilité des clés le nécessite.

→ **Séquestrer hors ligne une copie des clés privées des certificats dédiés au chiffrement.**

https://messervices.cyber.gouv.fr/guides/infrastructure-de-gestion-de-cles-igc

Hiérarchie

- 1 CA racine XCA
- 2 CA intermédiaires
  - AD CS pour les postes
  - XCA pour les serveurs



RootCA

- Reprise sous XCA de la racine AD CS
  - Opération très simple
- Partage des responsabilités
  - Stockage de l’application et des données
    - XCA + BdD
    - Export PKCS #12
  - Mots de passe
    - Imprimé au coffre de la direction
- Cérémonial de signature

https://4sysops.com/archives/use-openssl-based-software-xca-as-offline-root-certificate-authority-for-ad-certificate-services/

SubCA Server

- Nouvelle base
- Signé par la CA Racine

- L’ancienne PKI n’a pas été supprimée

A ce jour

Notre PKI ne connait pas la crise

- Automatisation AD CS
  - Renouvellement automatique des certificats ordinateur
  - Ajout de la délivrance des certificats utilisateurs (VPN IPSec)
- Amélioration à traiter
  - Alerte pour le renouvellement des certificats XCA
  - Nettoyage périodique des certificats AD CS

Merci pour votre attention

Des questions ?