



PKI DR18

Notre petite PKI... ne connaît pas la crise

Sommaire

Architecture v1

Architecture v2

Conclusion

Architecture v1

Besoin 1

Éliminer les certificats auto signés

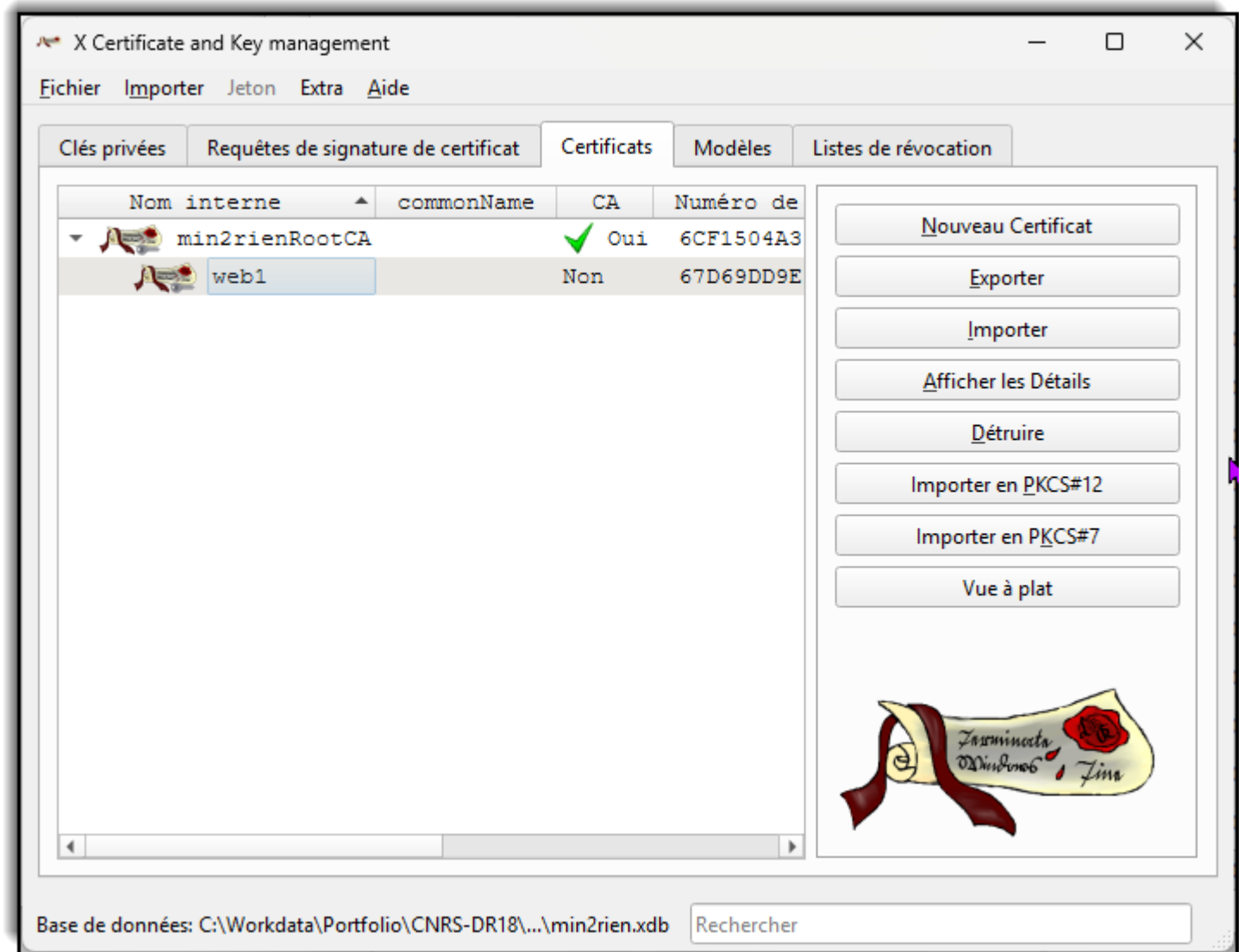
- Pourquoi
 - Permettre aux agents de respecter les recommandations de sécurité
 - Simplifier l'administration des postes
- Contrainte
 - Installation minimale
 - Utilisation simple



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

X Certificate and Key management

Créer un certificat x509

Source | **Sujet** | Extensions | Usage de la clé | Netscape | Avancé | Commentaire

Nom interne: **web2**

Distinguished name

countryName		organizationalUnitName	
stateOrProvinceName		commonName	web2
localityName		emailAddress	
organizationName			

Type	Contenu
------	---------

Clé privée: web2 (RSA:4096 bit) Inclure les clés utilisées **Générer une nouvelle clé**

OK Annuler Aide

X Certificate and Key management

Créer un certificat x509

Source | Sujet | Extensions | **Usage de la clé** | Netscape | Avancé | Commentaire

X509v3 Basic Constraints

Type: Entité Finale

Distance aux entités finales: Critical

Key identifier

- X509v3 Subject Key Identifier
- X509v3 Authority Key Identifier

Validité

Pas avant: 2026-05-01 00:00 GMT

Pas après: 2026-10-31 23:59 GMT

Intervalle de temps: **6** Mois

Minuit Heure locale Pas de date d'expiration précise

X509v3 Name Constraints

X509v3 Subject Alternative Name **DNS:copycn, DNS:web2.min2irn.fr**

X509v3 Issuer Alternative Name

X509v3 CRL Distribution Points

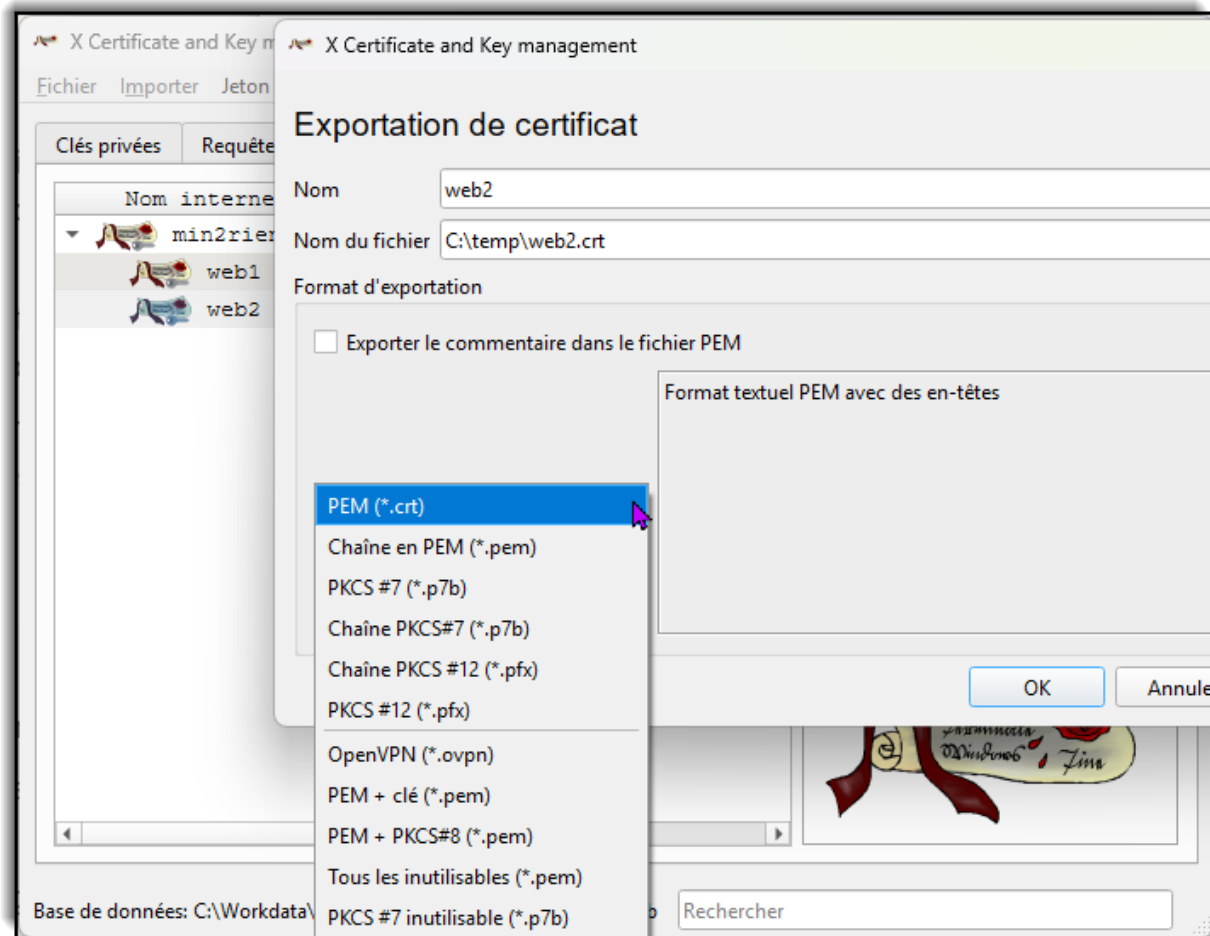
Authority Information Access

OSCP Must Staple

OK Annuler Aide

Démo XCA

Exporter un certificat



```
qqz3vMC++wSIJ51b716D2VgWQ6armq5PAHcbjqSvAoIBAQDhu55wudTwoFemPUqb
ZIEtHmBQY+705veB452tpwtNjFQQ9CgwBQJwD9YirnPN8M83VUX863sIkcgumf9n
RyAzT839bXHRgApwUD1VA1wT/93j+FHQGOaBDM15NCZuvRRn3MXY9pu6V1bHETcE
O/+A3Hng49V9x86D/h2FXqw3a1kiM77nZWkpV8F4KThpLuN9sVEP7cJOaGjFMmMD
+jYIJBmjro+8eOAB1SG304otmT67iCIUmUaM3WjIikDKU7T52W9KRx52eBuXURC8
RvTNHngM88343PpXqiT2I4FePSscy8xyEJ6S9or8uVg/socemrqQeaft+9RnN37N
CsiRAoIBAFFjld0xJQXfCme4XEKeGsoZCVZpdj21t65oz9+dBHRjfyCdsYcHfV4f
eGWeEcM5Rn7sy4o1c1Dx13sMUFTar1KuLdYI912/9C93oruevakq0ferYgG/2Y2W
fqs+65L1HuMYExs0d2SCNW5Gp320K7isOrzTOGTHbxfdjFrvMyYqB41evzSXyYX
V6RSX4xKZtuE+Z1c8g895d8TT1NGSVsVM+U3mmPHGNz1fa55eNd8ziwF0QXz1tu
y0v1m5ZRZtK7/fDG7/i5y1wtWwMXsciIf/KSS6k3IWIiS+wiHpVG7WfNaat9g2SF
Z5Mn7oScMcEK+MmQ/ZjSmmHalY3R6UkCggEADKwJW56m9kQtke4xqIV7eg+YuCGT
ZGAdCUOLMXZat4kjLoXyu3nI1CuYjPR8iqZZ2gsFamDs00M4i5oCYFkwL5FwWnOj
nN6S3YTXnAN2NCwGp2p1sLCAHtMSqPSq19bzMygkTulu5KNrgc9p14veVGtyAP3G
PCCHHCQnQ9bE6drhdsqfVSg1Ta2RqnJ5BaX7Z/wAP2Gv+TwC800Haf825UavBN5b
eMU1Yy2IU6oFaqx0mPzyAemKUMuHYGsw+NeifvOTBvmMvrm016M4YscvI/v8hcpV
me83rC3r5qjm+Y7wXBZVYq4Lav/cL1oMhfdFsz26dw+JCP00MFNzo11r1A==
-----END RSA PRIVATE KEY-----
-----BEGIN CERTIFICATE-----
MIIFWjCCA0KgAwIBAgIIGUsIcGpD7uUwDQYJKoZIhvcNAQELBQAwADAEFw0yNjA1
MDEwMDAwMDBaFw0yNjEwMzEyMzU5NTI1aMA8xDTALBgNVBAMTBhd1YjIwggIiMA0G
CSqGSIb3DQEBAQUAA4ICDwAwggIKAoICAQCcoBCXMqmgY1b/w8a0DzcFBVn6zJbPx
rU1dM34ac13ojICNRCgn3kMtQ1EzWJ4ZoQMf4kSVBfODbXhSYOL7AJpsCddDeH/S
Kn/szTfuumo1C6iUA+bjsUFJFDYd/BpoL3Ajb3MaF/8hQqzD89F3NDF7LOGZbfqx
kriixcCpgjmEBQ3F4Ln22YsCV9MAZBm2mV4bTGSpmYVfiwS4FRnhQc/a8fn2WpP7
83xKnThPIY12/u0ghibHOLLwJ17dAC0N7ofCzIwdzh9oUcDAVdzL6S0oBMhOyHu
eRPJHa5egPN5/xzEg6xnWv0z0eXM8ec3ttf6zV0J52LLDCNGXaptbeL6ggWwiaGw
003C5mzGQ91fII4c0REhH6cSYt2VdUI70D4RuompXguSA1XDTgqj2iej2z2r3V0S
9JJe8DK+CGdduCMW9EuIgwVh4Yr34t44TbpHbdjsMEKXDXmlcpnxIy+oxnGTAhd
zqWk3Jp+8hCKpPpgvodPZTSgj4HcGjAKNBw6TUsXJaTW1rJPYm6zMBBTSThfQq0
```

Une GPO

Distribution des racines sur l'ensemble du domaine AD.

Computer Configuration (Enabled)

Policies

Windows Settings

Security Settings

Public Key Policies/Trusted Root Certification Authorities

Certificates

Issued To	Issued By	Expiration Date	Intended Purposes
		21/01/2029 09:51:13	<All>
		07/03/2042 11:43:36	<All>
		08/11/2032 11:25:11	<All>
		01/10/2031 01:59:59	<All>
		20/04/2034 18:36:19	<All>

For additional information about individual settings, launch the Local Group Policy Object Editor.

Public Key Policies/Intermediate Certification Authority Certificates

Issued To	Issued By	Expiration Date	Intended Purposes
		12/11/2035 00:59:59	<All>

For additional information about individual settings, launch the Local Group Policy Object Editor.

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

DR18 Computer Properties

Superseded Templates Extensions Security Server

Subject Name Issuance Requirements

General Compatibility Request Handling Cryptography Key Attestation

Purpose: Signature and encryption

- Delete revoked or expired certificates (do not archive)
- Include symmetric algorithms allowed by the subject
- Archive subject's encryption private key

Authorize additional service accounts to access the private key

Key Permissions...

Allow private key to be exported

Renew with the same key

For automatic renewal of smart card certificates, use the existing key if a new key cannot be created

Do the following when the subject is enrolled and when the private key associated with this certificate is used:

- Enroll subject without requiring any user input
- Prompt the user during enrollment
- Prompt the user during enrollment and require user input when the private key is used

OK Cancel Apply Help

DR18 Computer Properties

Superseded Templates Extensions Security Server

Subject Name Issuance Requirements

General Compatibility Request Handling Cryptography Key Attestation

Template display name: DR18 Computer

Template name: DR18Computer

Validity period: 2 years

Renewal period: 3 months

Publish certificate in Active Directory

- Do not automatically reenroll if a duplicate certificate exists in Active Directory

OK Cancel Apply Help

DR18 Computer Properties

General Compatibility Request Handling Cryptography Key Attestation

Superseded Templates Extensions Security Server

Subject Name Issuance Requirements

Supply in the request

- Use subject information from existing certificates for autoenrollment renewal requests

Build from this Active Directory information

Select this option to enforce consistency among subject names and to simplify certificate administration.

Subject name format: None

- Include e-mail name in subject name

Include this information in alternate subject name:

- E-mail name
- DNS name
- User principal name (UPN)
- Service principal name (SPN)

OK Cancel Apply Help

AD CS

GPO d'enrôlement

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

Delegation

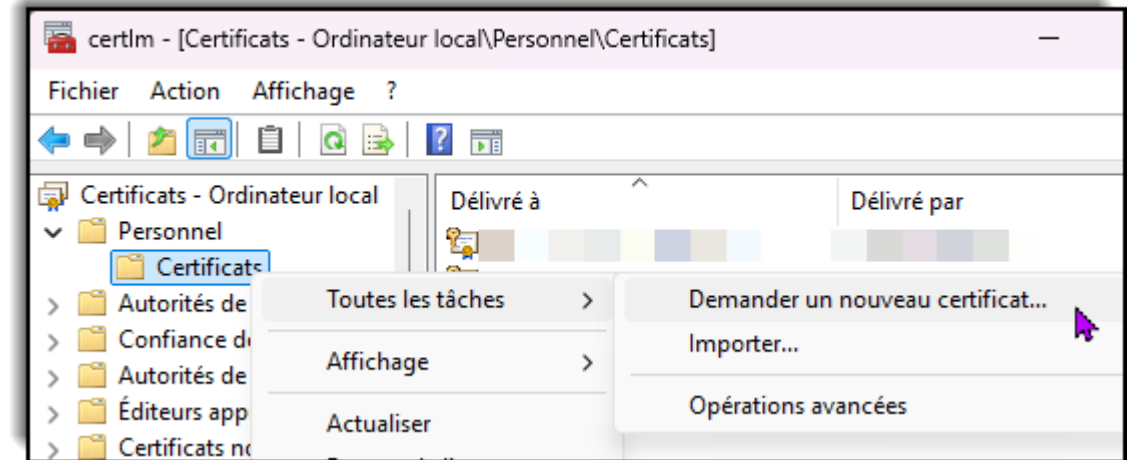
These groups and users have the specified permission for this GPO

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_po	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

Test AD DS

MMC Certificat ordinateur

- Présence du certificat
 - Personnel > Certificat
 - Si absent
 - GPRResult /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 :**

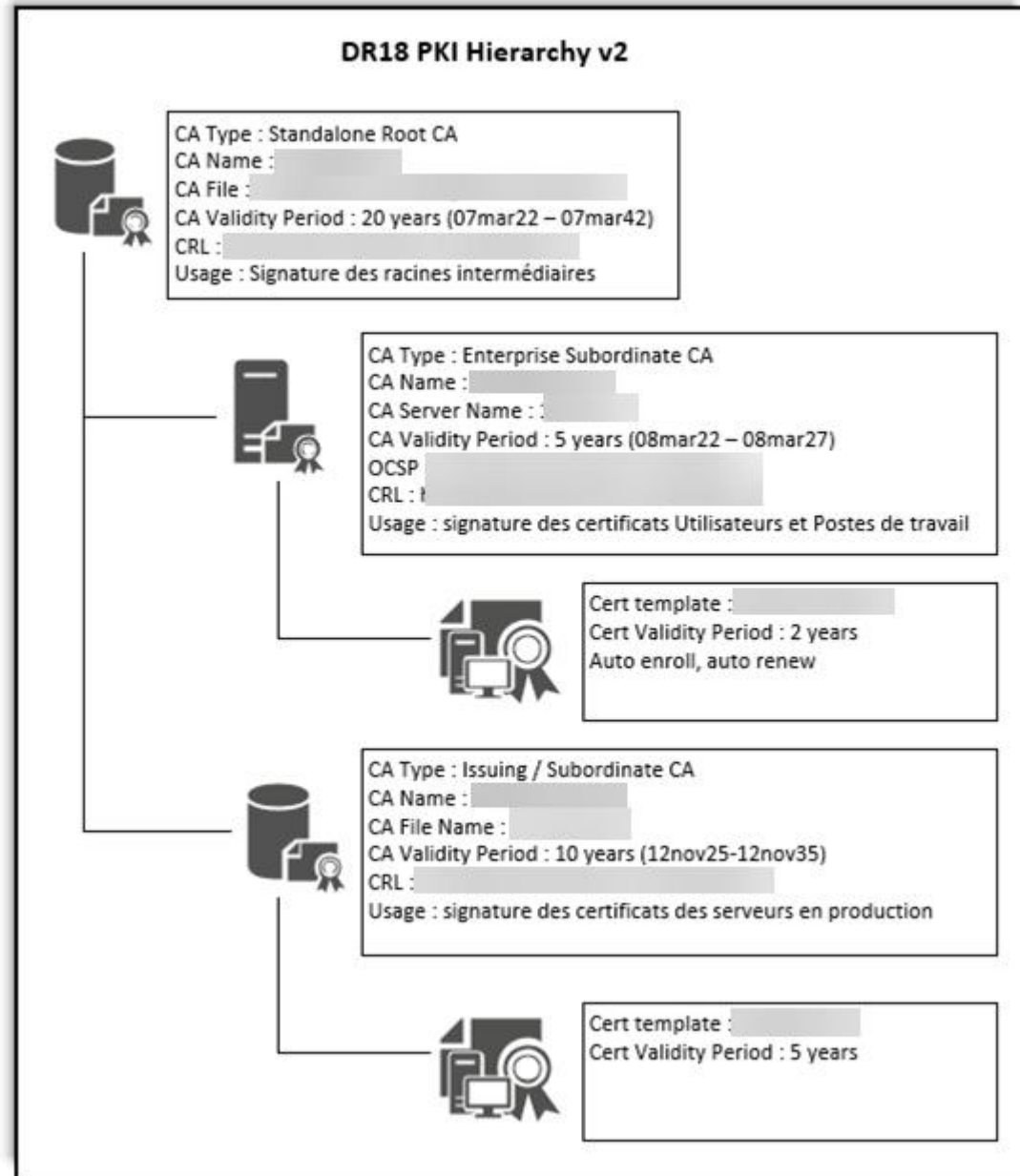
- > stocker les clés privées des AC racine hors ligne, idéalement dans un équipement sécurisé de type HSM (*Hardware Security Module*) ;
- > stocker les clés privées des AC intermédiaires en ligne dans un équipement sécurisé de type HSM ;
- > protéger les clés privées des certificats d'entité finale 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 connaît 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

The CNRS logo consists of the lowercase letters 'cnrs' in a dark blue, sans-serif font, centered within a white circle. The background of the slide is split: the left side is a solid yellow, and the right side is a blue field with a white halftone dot pattern. A curved white border separates the yellow and blue areas.

cnrs

**Merci pour votre
attention**

Des questions ?