Certificats auto-signé

Certificat exportable

Crée un certificat exportable auto-signé dans le magasin personnel de l'utilisateur courant pour un usage de signature numérique.

```
$certname = "CertForVpn"
$cert= New-SelfSignedCertificate -Subject "CN=$certname" -CertStoreLocation
"Cert:\CurrentUser\My" -KeyExportPolicy Exportable -KeySpec Signature -
KeyLength 2048 -KeyAlgorithm RSA -HashAlgorithm SHA256
Export-Certificate -Cert $cert -FilePath "C:\temp\$certname.cer"
```

- Subject “CN=$certname” : définit le nom du sujet du certificat à “CN=CertForVpn”.
- CertStoreLocation “Cert:\CurrentUser\My” : le certificat est stocké dans le magasin personnel de l'utilisateur courant.
- KeyExportPolicy Exportable : la clé privée peut être exportée ultérieurement.
- KeySpec Signature : la clé est destinée à des signatures numériques.
- KeyLength 2048 : utilise une clé RSA de 2048 bits, ce qui est un bon compromis sécurité/performance.
- KeyAlgorithm RSA : l’algorithme de chiffrement est RSA.
- HashAlgorithm SHA256 : l’algorithme de hachage utilisé est SHA-256.
- Export-Certificate -Cert $cert -FilePath “C:\temp\$certname.cer” : Le certificat est exporté directement dans le répertoire C:\temp, en utilisant comme nom de fichier celui défini pour le sujet du certificat. Il est nécessaire de créer ce répertoire avant d'exécuter le script.

Créer un certificat root ca et un certificat client

Le script ci-dessous créé 2 certificats : un root ca et un client, utilisé pour configurer une authentification par certificat, par exemple dans une connexion VPN point-à-site (P2S)

1. Créé un certificat RootCa pour la clé public coté serveur
2. Créé le certificat utilisateur
3. Exporte le certificat au format X.509 binaire encodé DER
4. Converti au format X.509 encodé en base 64

```
$certnameca = "RootCa"
$certnamecl = "ClientP2S"

$cert = New-SelfSignedCertificate -Type Custom -KeySpec Signature -Subject
"CN=$certnameca" -KeyExportPolicy Exportable -HashAlgorithm sha256 -
KeyLength 2048 -CertStoreLocation "Cert:\CurrentUser\My" -KeyUsageProperty
Sign -KeyUsage CertSign
```

```
New-SelfSignedCertificate -Type Custom -DnsName $certnamecl -KeySpec
Signature -Subject "CN=$certnamecl" -KeyExportPolicy Exportable -
HashAlgorithm sha256 -KeyLength 2048 -CertStoreLocation
"Cert:\CurrentUser\My" -Signer $cert -TextExtension
@("2.5.29.37={text}1.3.6.1.5.5.7.3.2")

$DERCert    = "C:\temp\$certnameca.cer"
$Base64Cert = "C:\temp\Base64_$certnameca.cer"

Export-Certificate -Cert $cert -FilePath $DERCert

Start-Process -FilePath 'certutil.exe' -ArgumentList "-encode $DERCert
$Base64Cert" -WindowStyle Hidden
```

From:
https://www.adminsys.it/wiki/ - **Admin Sys**

Permanent link:
https://www.adminsys.it/wiki/scripts-powershell:certificats_auto-signe

Last update: **2026/04/26 00:15**