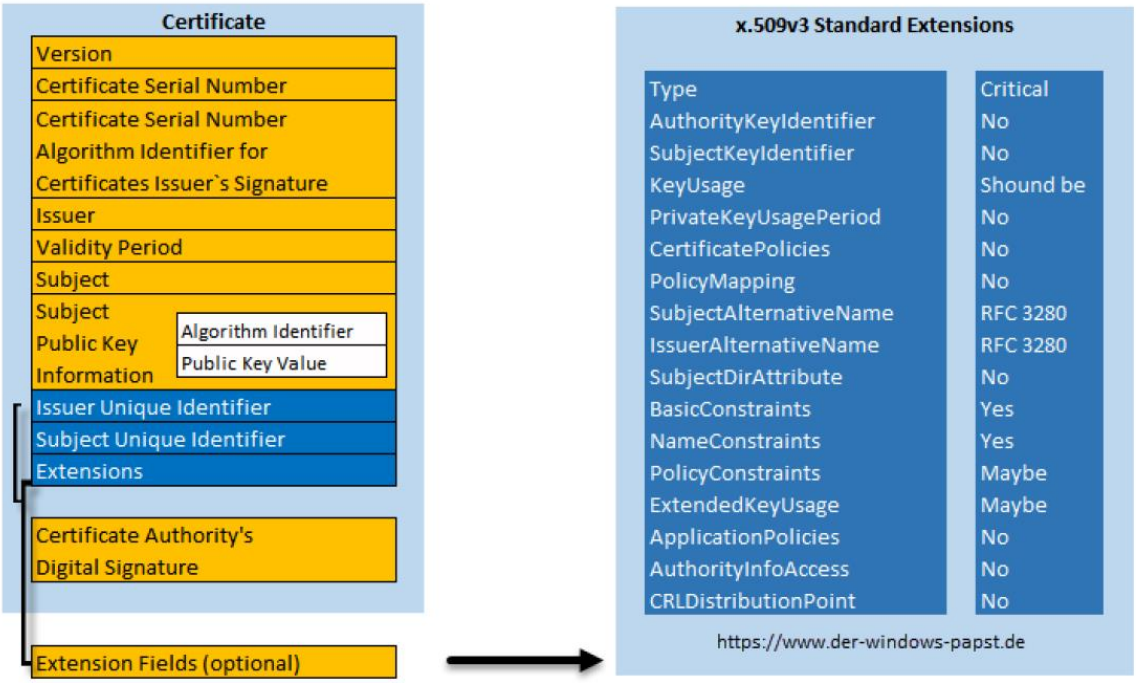
New-SelfSignedCertificate Parameter Eigenschaften

In meinem letzten Dokument bin ich mehr auf die grundlegenden Eigenschaften eines Zertifikats eingegangen und habe diese erklärt.

https://der-windows-papst.de/2019/07/06/eigenschaften-eines-x-509-v3-zertifikats/



Heute möchte ich mehr auf den Powershell-Befehl „New-SelfSignedCertificate" eingehen.

Mit New-SelfSignedCertificate erstellen wir Zertifikate. Zertifikate besitzen Eigenschaften (Attribute) und diese Eigenschaften geben wir beim Erstellen als Parameter mit an. Und was bedeuten diese Attribute überhaupt?

Subject:

Name des Zertifikats im X500 Format

Provider:

bestimmt den Kryptografieanbieter

KeyAlgorithm:

bestimmt den Algorithmus für den öffentlichen Schlüssel. KSP unterstützt CNG, ECDH.

KeyLength:

bestimmt die Schlüssellänge des Zertfikats. Ein muss wenn der Algorithmus nicht RSA ist.

KeyUsage:

beschränkt den öffentlichen Schlüssel in seiner Wirksamkeit. DigitalSignature, KeyEncipherment,DataEncipherment usw.

New-SelfSignedCertificate Parameter Eigenschaften

KeySpec:

bestimmt die Verwendungsart des öffentlichen Schlüssels. Signature oder Exchange (default).

HashAlgorithm:

gibt die Hash-Funktion an mit dem das Zertifikat signiert wurde. Der Hash-Algorithmus greift nicht in die Verschlüsselung oder Authentifizierung ein. Der Hash-Algorithmus erzeugt einen Fingerabdruck (HASH). Dieser Fingerabdruck bestätigt, dass die Informationen zwischen Server und Client nicht manipuliert oder beschädigt wurden. Webbrowser, E-Mail-Clients und Server benötigen diesen Hash zum Entschlüsseln (Prüfsumme) und zur Bestätigung der Integrität.

SignatureAlgorithm:

gibt den Algorithmus an mit dem das Zertifikat signiert wurde. Mit diesem Algorithmus werden auch weitere Inhalte über den privaten Schlüssel signiert.

KeyExportPolicy:

bestimmt ob der Private Schlüssel exportiert werden darf

KeyFriendlyName:

bestimmt den Anzeigename des Zertifkats

DnsName:

bestimmt weitere Subjectnames (SAN) oder IPs.

NotAfter:

bestimmt die maximale Gültig des Zertifikats

NotBefor:

bestimmt ab wann das Zertifikat gültig wird

CertStoreLocation:

bestimmt den Ablageort des Zertifikats. AuthRoot, Root, CertificateAuthority, My etc.

Der Befehl zum Erstellen eines Zertifikats kann z.B. so aussehen:

```
$cert = New-SelfSignedCertificate -Subject "CN=www.der-windows-papst.de" `
-CertStoreLocation "Cert:\LocalMachine\My" `
-HashAlgorithm "SHA256" `
-KeyAlgorithm "RSA" `
-KeyLength "2048" `
-KeyUsage "KeyEncipherment","DigitalSignature" `
-KeySpec "KeyExchange" `
-KeyExportPolicy "Exportable" `
-Provider "Microsoft RSA SChannel Cryptographic Provider" `
-KeyFriendlyName "WebService" `
-DnsName "der-windows-papst.de","www.der-windows-papst.de" `
-NotAfter (Get-Date).AddYears(5)
```

Weitere Informationen zu Vorlagen und deren Einsatzzweck

https://der-windows-papst.de/2019/01/06/zertifikatvorlage-und-einsatzzweck/