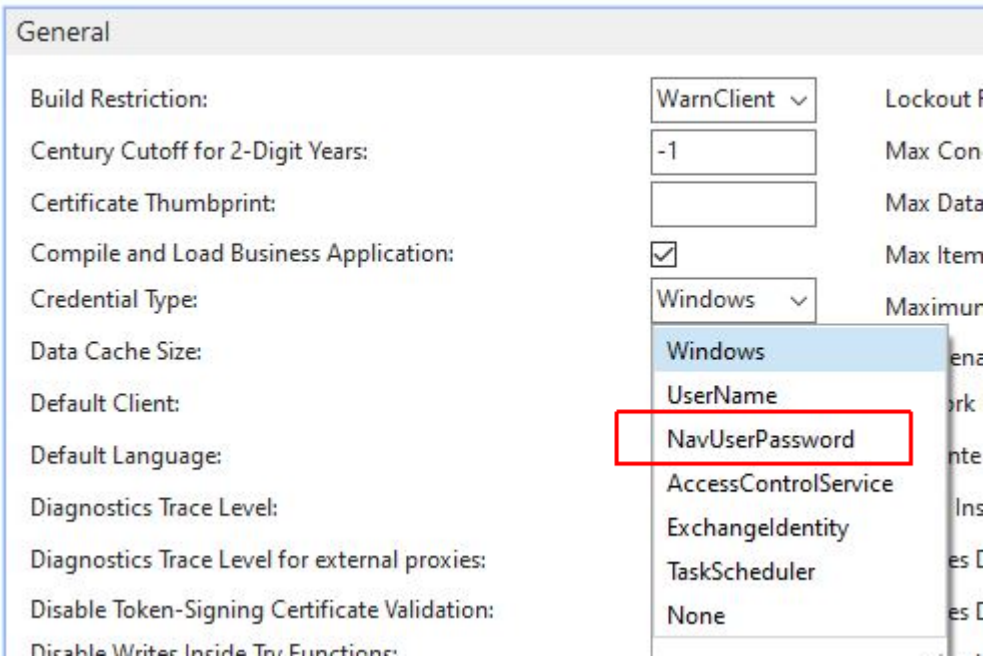
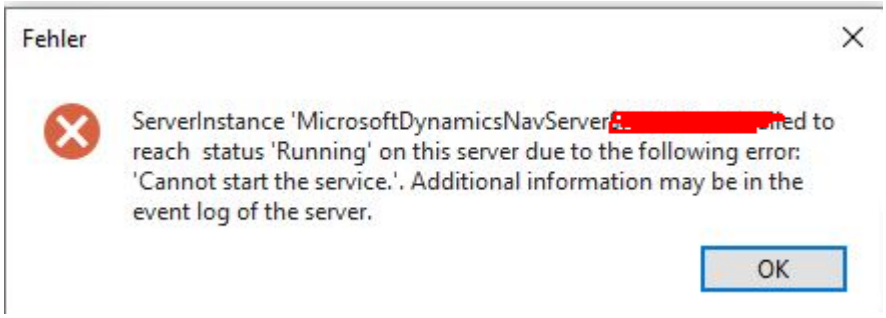
Der Navision / Business Central Webclient ist seit der 2018er Version erwachsen geworden! Und er wächst immer weiter. Es gibt seitdem kaum noch einen guten Grund den Windows Client einzusetzen. Seit Business Central 2019 (BC140) gibt es daher auch schon gar keinen WIndows-Client mehr. Einfach einen Browser öffnen, die URL Eingeben, und sofort mit Navision / Business Central arbeiten. Übrigens auch über Unternehmensgrenzen hinweg: Der Webclient ersetzt Fernzugriffe wie einen RDP (Remote Desktop Protocol) Client, Teamviewer, VNC und andere Remote-Zugriffstechniken gänzlich!

Dabei ist innerhalb einer Windows-Domäne die Anmeldeform über Windows noch immer die bequemste, und wird von Navision im Standard unterstützt. Einfach Navision / Business Central wie hier beschrieben installieren, und los geht es. Auch und gerade mit dem Webclient! Sollte der Browser nach Anmeldedaten fragen: Einfach die Windows Zugangsdaten eingeben, und fertig.

Was aber, wenn man den Client auch aus der Ferne, außerhalb eines VPN's, außerhalb einer Windows-Domäne nutzen will? Dann gibt es keine Windows-Zugangsdaten, die man eingeben könnte. Nichts einfacher als Das: Navision auf den Credential Type NavUserPassword umstellen, und… nix geht mehr!





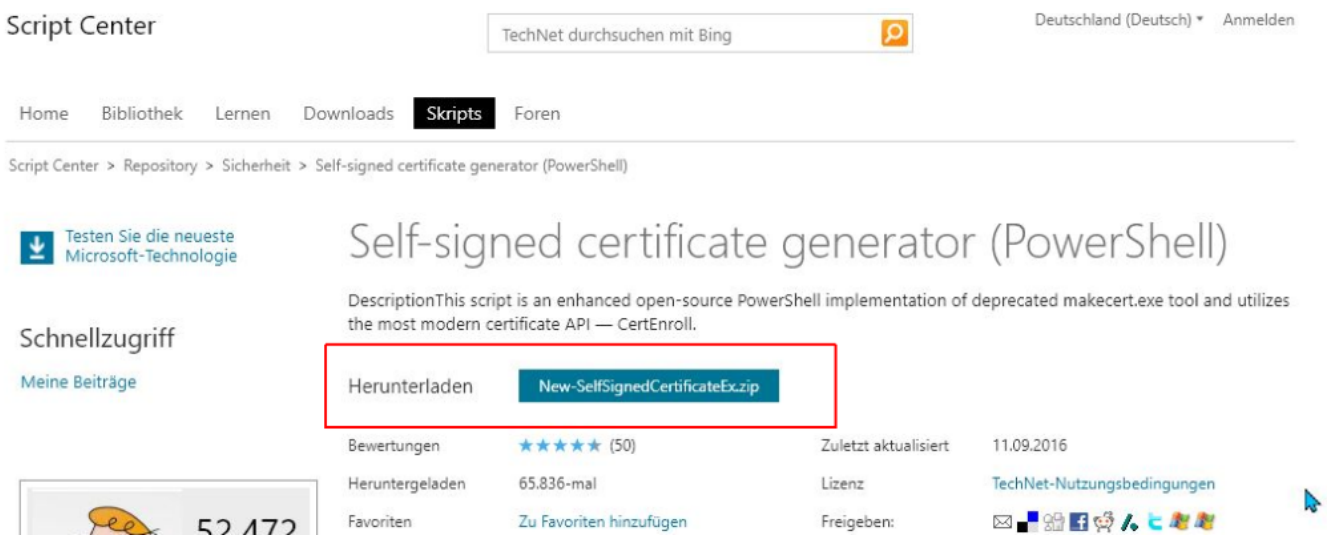
In der Ereignisanzeige findet man schnell die Lösung: Navision verlangt ab sofort ein Zertifikat! Die Ereignisanzeige meldet den Fehler:

Server instance: xxxx
Type: Microsoft.Dynamics.Nav.Types.NavConfigurationException
SuppressMessage: False
ContainsPersonalOrRestrictedInformation: False
DiagnosticsSuppress: False
MessageWithoutPrivateInformation: **Zertifikat mit dem Fingerabdruck wurde weder im Speicher CurrentUser noch im Speicher LocalMachine gefunden.**
Microsoft.Dynamics.Nav.Types.CertificateHelper.FindCertificateFromThumbprint(String certificateThumbprint)

Microsoft will hier den Benutzer vor sich selber schützen, und authentifiziert in dieser Konstellation nur noch über ein Zertifikat. Egal ob man diese zusätzliche Sicherheitsstufe will oder braucht. Also gut: Ärmel hoch, und los geht es. Seit 2018 auch, dank neuer Powershell Scripte, sehr einfach. Der Hexentanz mit makecert.exe **ist nicht mehr nötig**!

Hinweis: Sie können auch jedes andere zur Verfügung stehende Zertifikat benutzen, überspringen Sie dann bitte einfach die Punkte zum neu erstellen eines selbstsignierten Zertifikates. Ansonsten führen Sie die folgenden Schritte am einfachsten auf dem Navision / Business Central Datenbankserver aus.

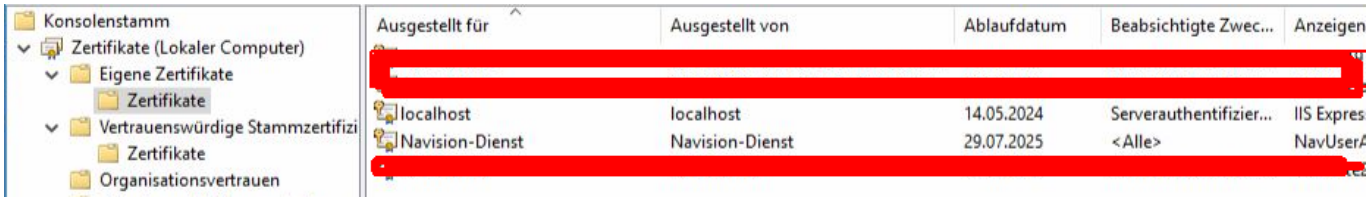
Vorbereitung: Sie benötigen das Powershell Script New-SelfSignedCertificateEx, welches Sie hier finden:



laden und entpacken Sie diese Datei z.B. nach c:\Temp. Ich habe das Script mal hier beigefügt, empfehle aber natürlich den Download direkt von Microsoft.

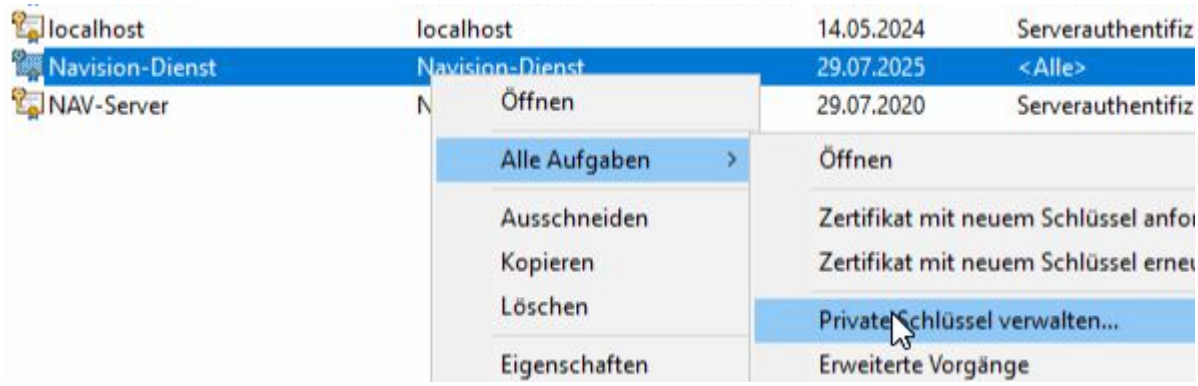
1. Starten Sie die Powershell im Administratormodus
2. wechseln Sie in c:\temp (oder wo Sie das Script gespeichert haben)
   (Tipp: Sie können bei den meisten Befehlen nur die Anfangsbuchstaben tippen, und dann mit der TAB-Taste vervollständigen)
   Set-ExecutionPolicy RemoteSigned
   Bestätigen Sie die Rückfrage mit J
3. *Import-Module .\New-SelfSignedCertificateEx.ps1*
4. *New-SelfSignedCertificateEx -Subject „CN=Navision-Dienst“ -IsCA $True -Exportable -StoreLocation LocalMachine -FriendlyName „NavUserAndPassword“ -NotAfter $([datetime]::now.AddYears(5))*

Natürlich können sie die Platzhalter für die Zertifikatsbezeichnung und das Password beliebig ändern.
„Navision-Dienst“ bezeichnet dabei den Servernamen! Am Ende dieser Anleitung finden Sie eine Möglichkeit, diese Bezeichnung über die Konfigurationsdateien zu ändern.
Empfehlung: Tragen Sie hier gleich die richtige DnsIdentiy ein! (Computername bei dem Installieren von Navision / Business Central).
Die Shell nach dem Aufruf nicht schließen, Sie brauchen noch den Thumprint.
Dieser Befehl erzeugt ein neues Zertifikat im Zertifikatspeicher:

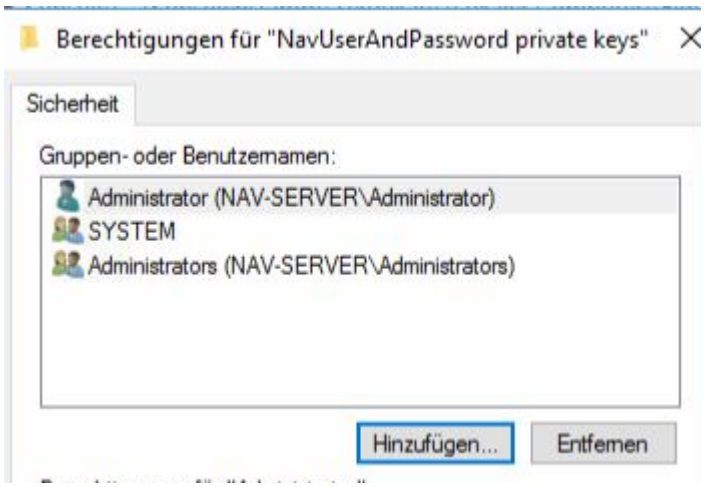


Anzeige eines neuen Zertifikats im Zertifikatspeicher für die Navision / Business Central Credentials NavUserAndPassword

Öffnen Sie eine mmc für die Zertifikate (mmc.exe, Datei/SnapIn Hinzufügen, Zertifikat, Computer Account/Local Computer).
Markieren Sie das neu erzeugte Zertifikat, rechte Maustauste, Alle Aufgaben, Private Schlüssel verwalten

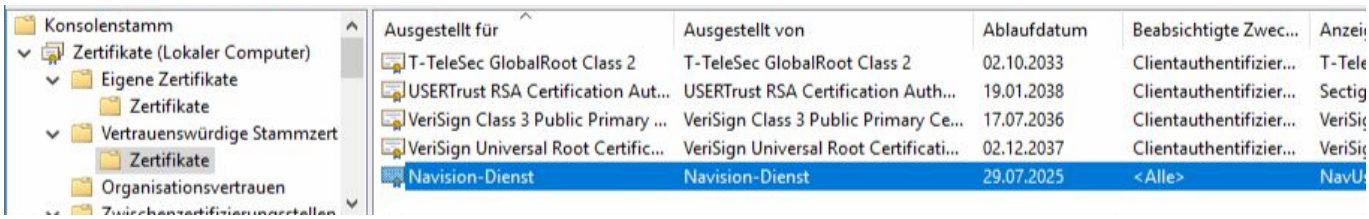


Fügen Sie das Dienstekonto des Navision-Diensteservers hinzu (oft Administrator oder Network/Netzwerkdienste)



kopieren Sie das Zertifikat bitte auch noch in den Ordner Vertrauenswürdige

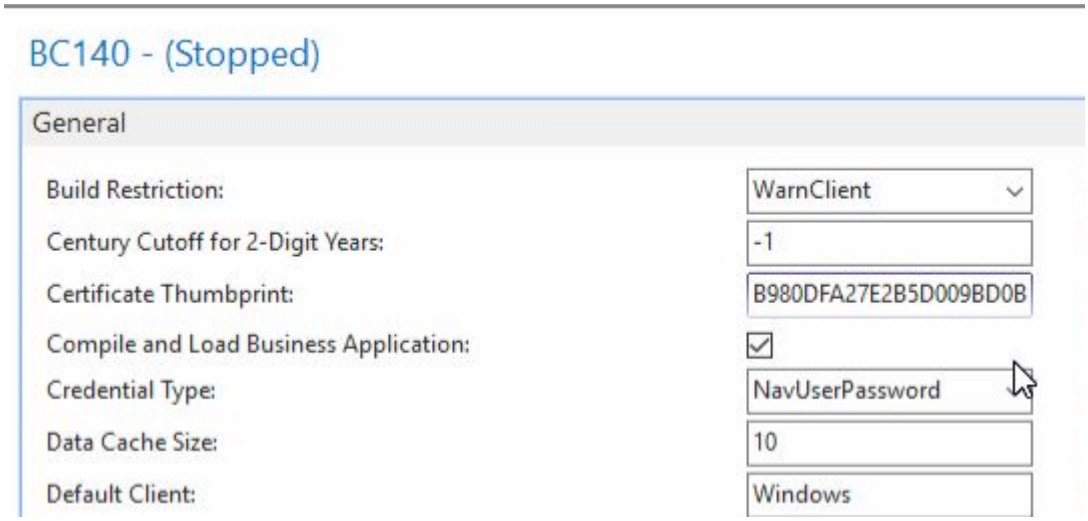
Stammzertifikate/Zertifikate (Rechte Maustaste/Kopieren, Zielordner -> Einfügen)



Sie können die Zertifikatsverwaltung nun schließen.

Kopieren Sie nun den Thumbprint aus der Konsole. Dies ist zuverlässiger als das Kopieren aus der Zertifikatsverwaltung.

Fügen Sie diesen „Fingerabdruck“ (wörtlich: Daumenabdruck) nun in der Navision-Dienstekonfiguration unter Certificate Tumbprint ein:



Im Zertifikat wurde der Rechnername hinterlegt („Navision-Dienst“). Sollte dies abweichen, so können Sie dies alternativ auch in der ändern:

Fehler bei der Identitätsprüfung für eine ausgehende Nachricht. Die erwartete DNS-Identität des Remoteendpunkts war „**nav-server**„, aber der Remoteendpunkt hat den DNS-Anspruch „**Navision-Dienst**“ bereitgestellt. Wenn es sich hierbei um einen rechtmäßigen Remoteendpunkt handelt, können Sie das Problem beheben, indem Sie ausdrücklich die DNS-Identität „Navision-Dienst“ als die Identity-Eigenschaft von EndpointAddress angeben, wenn Sie einen Kanalproxy erstellen.

Dies wird in der web.config (bis Nav 2017) bzw. NavSettings.JSON in z.B. im Ordner C:\inetpub\wwwroot\Instanzen-Name zu finden, z.B. C:\inetpub\wwwroot\BC140 oder ClientUserSettings.config in z.B. C:\Users\AppData\Roaming\Microsoft\Microsoft Dynamics NAV\100 geändert:

```
"//DnsIdentity":  "The DNS or subject name from the server
certificate.",
                        "DnsIdentity":  "NAV-Server",
```

Ändern Sie den Eintrag in Dns Identity von „NAV-Server“ (in diesem Beispiel) auf „Navision-Dienst“: Empfehlung: Erstellen sie das Zertifikat direkt mit dem passenden DNS-Eintrag!