

Erneuern der Zertifikate in der ML 2

Einige der Zertifikate in der Musterlösung der Version 2.0 bis 2.5 laufen im September 2004 ab und müssen deshalb erneuert werden. Dies müssen Sie auch ausführen, wenn Sie eine Musterlösung der oben genannten Versionen durch Update auf den Versionsstand 2.6 bringen. Im Auslieferungszustand der Version 2.6 sind bereits erneuerte Zertifikate enthalten.

Übersicht über Zertifikate und Ablaufdatum

Einserver-Version

Zertifikatname	Ablaufdatum Trusted Root	Ablaufdatum Public Key
NetIdentity - GSERVER02	03.09.2012	03.09.2012
SSL CertificateDNS - GSERVER02	03.09.2012	03.09.2004 !!!
SSL CertificateIP - GSERVER02	03.09.2012	03.09.2004 !!!

In der Einserver-Version müssen also die beiden Zertifikate **SSL CertificateDNS** und **SSL CertificateIP** erneuert werden.

Zweiser-Server-Version

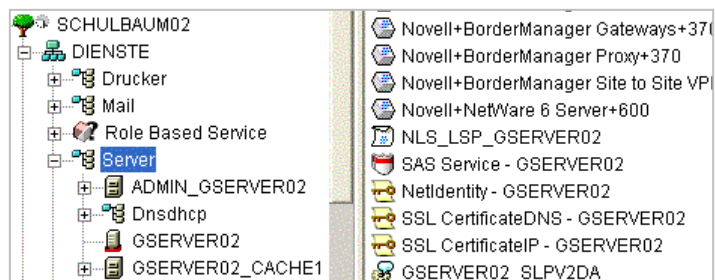
Zertifikatname	Ablaufdatum Trusted Root	Ablaufdatum Public Key
NAASKMO - KSERVER02	03.09.2012	15.12.2004 !!!
NetIdentity - GSERVER02	03.09.2012	03.09.2012
NetIdentity - KSERVER02	03.09.2012	03.09.2012
SSL CertificateDNS - GSERVER02	03.09.2012	03.09.2004 !!!
SSL CertificateDNS - KSERVER02	03.09.2012	16.12.2004 !!!
SSL CertificateIP - GSERVER02	03.09.2012	03.09.2004 !!!
SSL CertificateIP - KSERVER02	03.09.2012	16.12.2004 !!!

In der Zweiser-Server-Version müssen 5 Zertifikate erneuert werden:
NAASKMO, **SSL CertificateDNS – GSERVER02**, **SSL CertificateDNS – KSERVER02**, **SSL CertificateIP – GSERVER02** und **SSL CertificateIP – KSERVER02**.

Es müssen nun jeweils die alten Zertifikate gelöscht und neue Zertifikate mit demselben Namen erstellt werden. Dies geschieht mit ConsoleOne. Gehen Sie dabei schrittweise wie beschrieben vor.

1. Zertifikat löschen
2. Neues Zertifikat erstellen
3. Zertifikat überprüfen mit PKIDIAG

- Melden Sie sich als Admin an und starten Sie *ConsoleOne*. Klicken Sie auf die OU Server.Dienste, so dass Sie im rechten Fenster die Zertifikate sehen.



Achtung:

In manchen Umgebungen (Nici-Version) kommt es vor, dass beim Start von ConsoleOne oder beim Bearbeiten eines Benutzerobjekts die Fehlermeldung „Nici Fails to Set Current Tree Name“ erscheint. Es lassen sich dann auch keine Zertifikate bearbeiten bzw. erstellen.

Eine Abhilfe für dieses Problem ist auf www.support-netz.de unter dem Menüpunkt Novell > Aktualisierungen beschrieben.

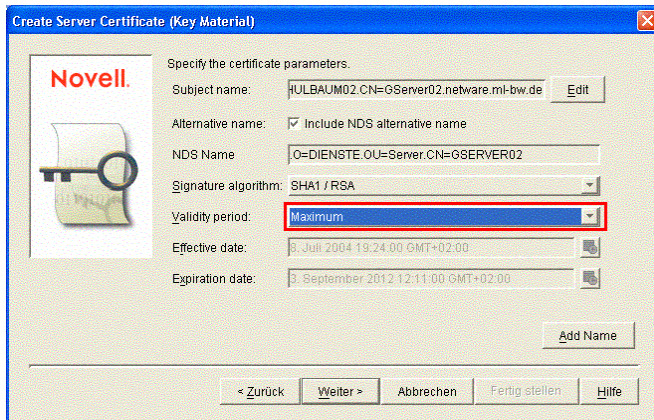
Beschreibung für SSL CertificateDNS – GSERVER02

1. Löschen Sie das Zertifikat-Objekt **SSL CertificateDNS – GSERVER02** mit ConsoleOne
2. Markieren Sie die OU Server
 - Erstellen Sie ein neues Objekt von der Klasse *NDSPKI:Key Material*



Wählen Sie bei Server den **GSERVER02** aus.
Tragen Sie bei Certificate name ein: **SSL CertificateDNS**
(Beachten Sie die Leerstelle zwischen SSL und CertificateDNS)
Wählen Sie bei Creation Method **Custom** aus.
Weiter.

- Wählen Sie im nächsten Dialog die Option **Organizational certificate authority**
- Im darauf folgenden Dialog sind folgende Einstellungen zu wählen:
2048 bits, SSL or TLS, Allow private key to be exported
- Kontrollieren Sie die folgenden Einstellungen:



Wählen Sie bei *Validity Period* die Option **Maximum**
Weiter

- Wählen Sie: **Your organization's certificate**
 - Fertigstellen
3. Neues Zertifikat prüfen mit PKIDIAG
 - Geben Sie an der Serverkonsole ein **SYS:NWMUSTERPKIDIAG2PKIDIAG** (möglicherweise in **SYS:NWMUSTERPKIDIAGPKIDIAG** bei älteren Versionen der ML. Ev. Download von Novell: <http://support.novell.com/servlet/filedownload/pub/pkidiag2.exe>) Führen Sie diesen Schritt in der Zweiserver-Version an beiden Servern aus.
 - Melden Sie sich als **Admin.Verwalter.Dienste** an.
 - Wählen Sie die Option **0 Begin Diagnostics now**
Wenn das neue Zertifikat fehlerfrei angelegt wurde, dann sollten Sie bei **Fixable problems found** und bei **Unfixable problems found** den Eintrag 0 vorfinden. Wenn nicht, dann haben Sie vermutlich den Zertifikatnamen nicht korrekt angegeben. Löschen Sie dann das neue Zertifikat wieder mit ConsoleOne und legen es wie beschrieben noch einmal an.

Beschreibung für SSL CertificateDNS – KSERVER02 (nur Zweiserver-Version)

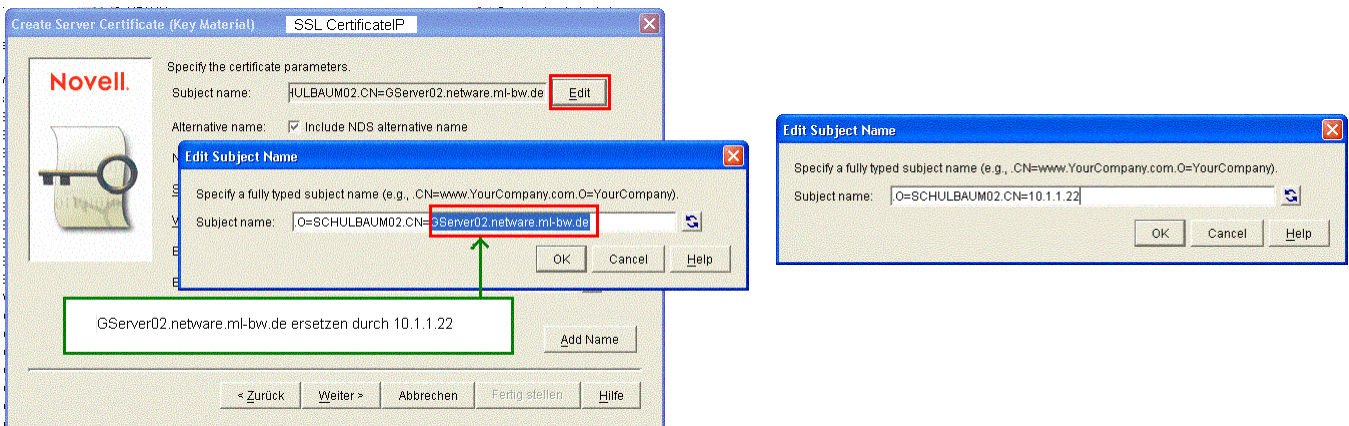
1. Löschen Sie das Zertifikat-Objekt **SSL CertificateDNS – KSERVER02** mit ConsoleOne
2. Markieren Sie die OU Server
 - Erstellen Sie ein neues Objekt von der Klasse *NDSPKI:Key Material*
Wählen Sie bei Server den **KSERVER02** aus.
Tragen Sie bei Certificate name ein: **SSL CertificateDNS**
 - Im weiteren gelten die selben Einstellungen wie beim **SSL CertificateDNS – GSERVER02**
3. Prüfen Sie das Zertifikat mit PKIDIAG

Beschreibung für NAASKMO – KSERVER02 (nur Zweiserver-Version)

1. Löschen Sie das Zertifikat-Objekt **NAASKMO – KSERVER02** mit ConsoleOne
2. Markieren Sie die OU Server
 - Erstellen Sie ein neues Objekt von der Klasse *NDSPKI:Key Material*
Wählen Sie bei Server den **KSERVER02** aus.
Tragen Sie bei Certificate name ein: **NAASKMO**
 - Im weiteren gelten die selben Einstellungen wie beim **SSL CertificateDNS – GSERVER02**
3. Prüfen Sie das Zertifikat mit PKIDIAG

Beschreibung für SSL CertificateIP – GSERVER02

1. Löschen Sie das Zertifikat-Objekt **SSL CertificateIP – GSERVER02** mit ConsoleOne
2. Markieren Sie die OU Server
 - Erstellen Sie ein neues Objekt von der Klasse *NDSPKI:Key Material*
Wählen Sie bei Server den **GSERVER02** aus.
Tragen Sie bei Certificate name ein: **SSL CertificateIP**
(Beachten Sie die Leerstelle zwischen SSL und CertificateIP)
 - Wählen Sie im nächsten Dialog die Option **Organizational certificate authority**
 - Im darauf folgenden Dialog sind folgende Einstellungen zu wählen:
2048 bits, SSL or TLS, Allow private key to be exported
 - Ändern Sie mit Edit den Subject name wie im folgenden Bild beschrieben:
(Die Domainbezeichnung muss durch die IP-Adresse ersetzt werden)



Wählen Sie bei *Validity Period* die Option **Maximum**
Weiter

- Wählen Sie: **Your organization's certificate**
 - Fertigstellen
3. Prüfen Sie das Zertifikat mit PKIDIAG

Beschreibung für SSL CertificateIP – KSERVER02 (nur Zweiserver-Version)

1. Löschen Sie das Zertifikat-Objekt **SSL CertificateIP – KSERVER02** mit ConsoleOne
2. Markieren Sie die OU Server
 - Erstellen Sie ein neues Objekt von der Klasse *NDSPKI:Key Material*
Wählen Sie bei Server den **KSERVER02** aus.
Tragen Sie bei Certificate name ein: **SSL CertificateIP**
 - Im weiteren gelten die selben Einstellungen wie beim **SSL CertificateIP – GSERVER02**,
verwenden Sie jedoch die IP-Adresse des KSERVER02 **10.1.1.21**
3. Prüfen Sie das Zertifikat mit PKIDIAG