ICA 13 mit Storefront und Zertifikaten nutzen

Dieses HowTo beschreibt, wie Sie mittels Rangee Linux eine Verbindung zu einem Citrix Storefront Server herstellen können. Hierzu muss ein überprüfbares Zertifikat einer Zertifizierungsstelle vorhanden sein. Sollten Sie kein Zertifikat einer offiziellen Zertifizierungsstelle besitzen, können Sie sich auch eine eigene Zertifizierungsstelle einrichten.

benötigte Softwaremodule
ICA 13 7.00 Build 030
Firmware 7.00

Inhaltsverzeichnis

1. Vorbereitung

Bitte achten Sie darauf dass die Uhrzeit des Cients mit der der Zertifizierungsstelle übereinstimmt, am Besten verwenden Sie einen Zeitserver.

2. Einrichten einer Zertifizierungsstelle auf einem Windows Server 2008R2

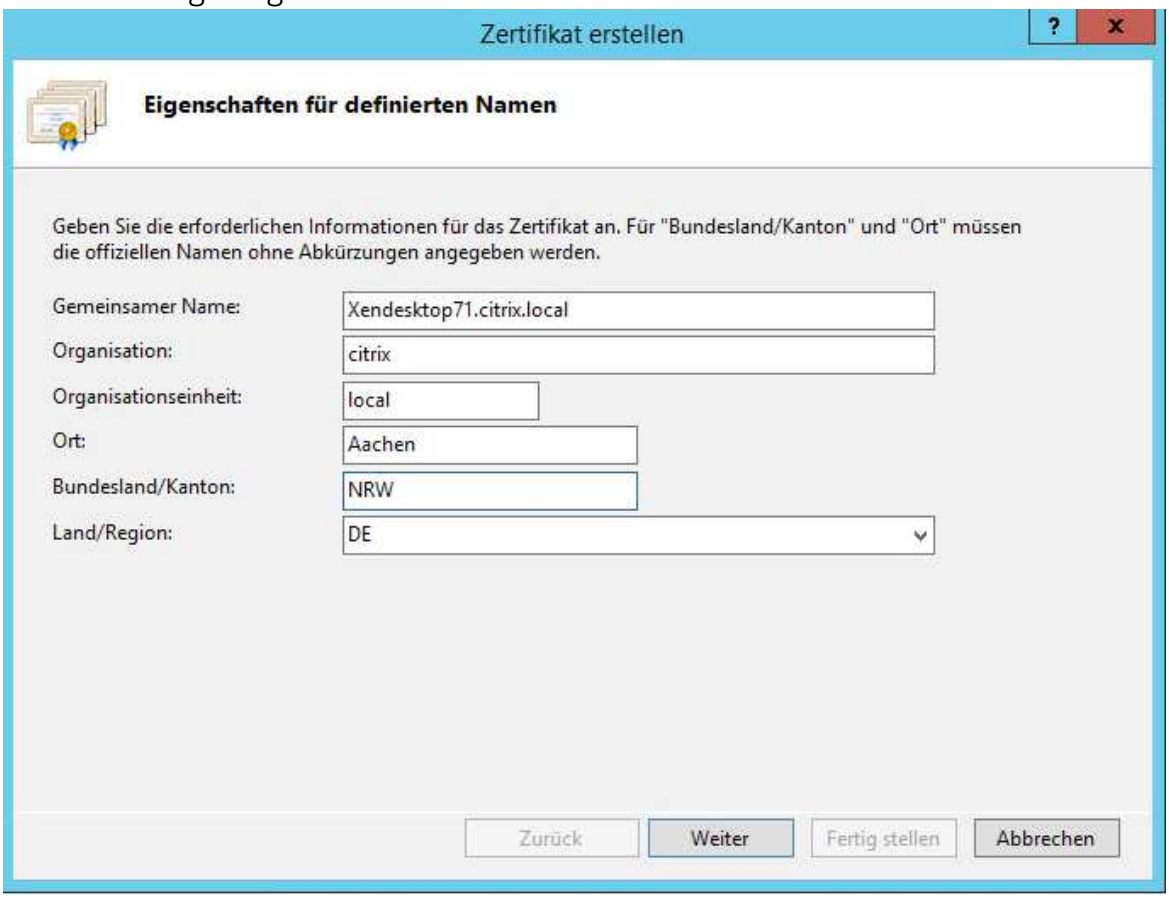
1. Öffnen Sie den Servermanager
2. Wählen Sie „Rolle hinzufügen“
3. Rolle „Active Directory-Zertifikatdienste“ wählen
4. Wählen Sie die Rollendienste:
    a. Zertifizierungsstelle
    b. Zertifizierungsstellen-Webregistrierung
5. Installationstyp „Unternehmen“
6. Zertifizierungsstellentyp „Stammzertifizierungsstelle“
7. „Neuen privaten Schlüssel erstellen“
8. Kryptographie kann auf Standard belassen werden
9. Allgemeiner Name dieser Zertifizierungsstelle: „CITRIX-CA“, kann nach Belieben vergeben werden
10. Die restlichen Einstellungen können auf Standard belassen werden

3. Erstellung eines Domänenzertifikats für den Storefront Server

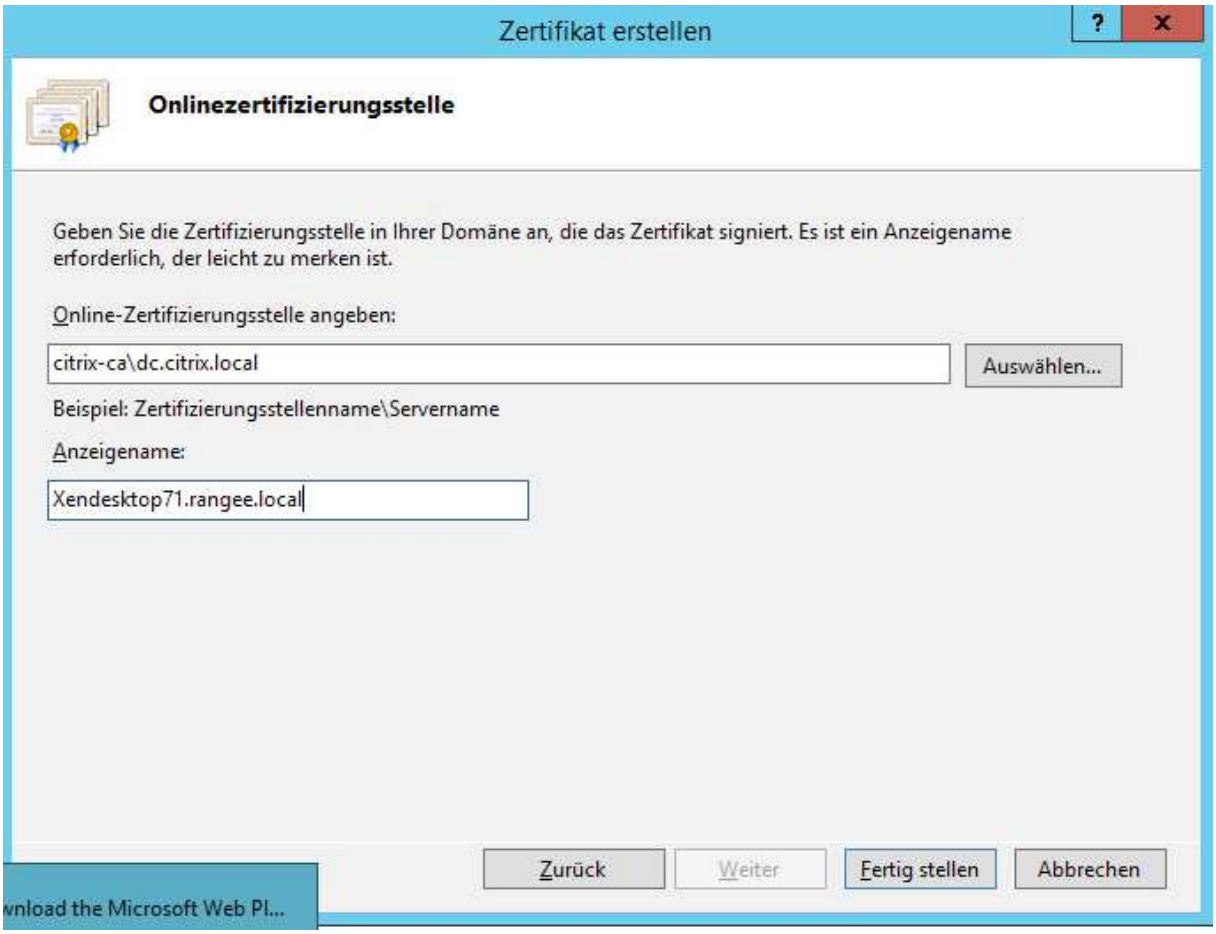
Falls Sie ein von einer offiziellen Stelle signiertes Zertifikat haben, müssen Sie dieses für die Storebrowse Verbindung verwenden – andernfalls müssen Sie sich wie folgt ein Domänenzertifikat erstellen.

1. Öffnen Sie den Internetinformationsdienste (IIS)-Manager
2. Wählen Sie Ihren Strorefront Server aus
3. Öffnen Sie „Serverzertifikate“
4. Wählen Sie „Domänenzertifikat erstellen…“ (rechts oben)

5. Tragen Sie als „Gemeinsamer Name“ den FQDN des Storefront-Server ein, z.B.: „Xendesktop71.citrix.local“, die restlichen Werte können nach Belieben eingetragen werden.



6. Tragen Sie unter Online-Zertifizierungsstelle die auf Sie zutreffenden Daten im Format „Zertifizierungstellenname\Servername“ ein (siehe 1.9), z.B.:



7. Wählen Sie anschließend „Fertig stellen“

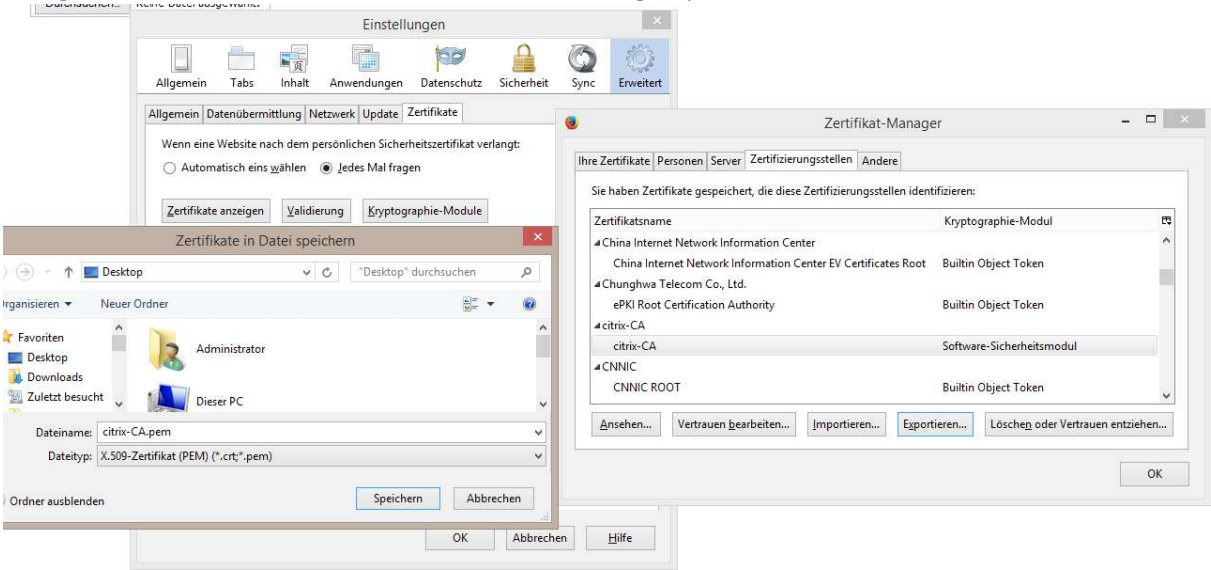
3. Einbinden des Zertifikats auf die Storebrowse Webseite

1. Wählen Sie im IIS-Manager Ihre Storebrowse Website mit einem Rechtsklick an
2. Wählen Sie „Bindungen bearbeiten…“
3. Wählen Sie den Typ „https“ aus und klicken Sie anschließend auf „Bearbeiten…“
4. Wählen Sie als „SSL-Zertifikat“ das von Ihnen in Schritt 2 erstellte oder das bereits von einer offiziellen Stelle signierte Zertifikat
5. Bestätigen Sie die noch offenen Menüs mit „OK“ und starten Sie anschließend die Webseite neu

4. Erstellung eines Zertifizierungsstellenzertifikats im Format *.pem oder *.crt

Um die folgenden Schritte durchführen zu können, benötigen Sie einen Firefox Browser – da dieser in der Lage ist die Zertifikate recht einfach im benötigten Format zu exportieren. Falls Ihnen bereits das Zertifizierungststellenzertifikat im *.pem oder *.crt Format vorliegt, können Sie diesen Schritt überspringen.

1. Öffnen Sie im Firefox die Webseite Ihres Zertifizierungsanbieters bei Domänenzertifikaten ist dies „%FQDN der Zertifizierungsstelle%/certsrv“. Z.B.: http://dc.citrix.local/certsrv/
2. Wählen Sie dort „Download eines Zertifizierungsstellenzertifikats, einer Zertifikatkette oder einer Sperrliste“
3. Wählen Sie „Zertifizierungsstellenzertifikat installieren“
4. Wählen Sie „Dieser CA vetrauen, um Websites zu identifizieren“
5. Betätigen Sie F10 um die Optionsleiste einzublenden
6. Wählen Sie anschließend „Extras“ -> “Einstellungen“ -> “Erweitert“ -> „Zertifikate“ -> „Zertifikate anzeigen“
7. Wählen Sie nun unter „Zertifizierungsstellen“ Ihr soeben importiertes Zertifikat aus und klicken Sie anschließend auf „Exportieren“
8. Vergeben Sie einen Namen mit der Endung *.pem oder *.crt



5. Importieren des Zertifikats am ThinClient

1. Öffnen Sie das Webinterface des ThinClient (https://IP-Adresse)
2. Wählen Sie unter „Werkzeuge“ (unten links) die Option „Zertifikat“
3. Drücken Sie anschließend „Zertifikat installieren“ und wählen Sie Ihr in Schritt 4 exportiertes *.pem Zertifikat aus
4. Drücken Sie abschließend auf „Installieren“ (unten rechts)
5. Anschließend können Sie eine Storefront Verbindung herstellen

6. Möglich Fehlerquellen

1. Verwenden Sie in der ThinClient Konfiguration ausschließlich den FQDN des Storefront Servers – die IP Adresse kann mittels eines selbst erstellen Zertifikats nicht überprüft werden - eine Verbindung schlägt fehl.
2. Stellen Sie sicher, dass der FQDN über den TC auflösbar ist. Über „Werkzeuge“ -> „Ping“ können Sie dies überprüfen.
3. Stellen Sie sicher dass Sie das Zertifizierungsstellenzertifikat am ThinClient im Format *.crt oder *.pem importiert haben (Schritt 4 und 5).
   Das hier beschriebene Vorgehen funktioniert nicht mit dem Zertifikat des Storefront Server.
4. Überprüfen Sie Datum- und Uhrzeiteinstellungen am ThinClient. Zu stark abweichende Uhrzeiten kann die Überprüfung des Zertifikates fehlschlagen lassen.
   Z.B.: Datum am ThinClient 12.02.2012 + Zertifikat gültig ab 26.01.2014 = Überprüfung ergibt ungültiges Zertifikat.