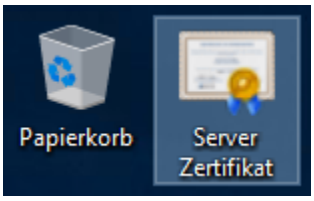
Windows: Einem Server-Zertifikat vertrauen

Für den Zugriff auf Remote Desktop Services (und viele andere Dienste) müssen Client-Computer dem jeweiligen Remote-Computer vertrauen.
Im Falle eines selbst-signierten Zertifikats ist es notwendig, diesem auf dem Client-Computer das Vertrauen auszusprechen, indem es in die Sammlung der *vertrauenswürdigen Stammzertifizierungsstellen* aufgenommen wird.

Das Zertifikat muß als Datei an den/die Client-Computer übermittelt werden:

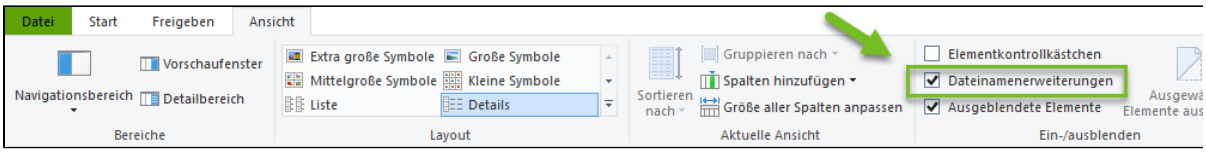


Schritt-für-Schritt-Anleitung

1

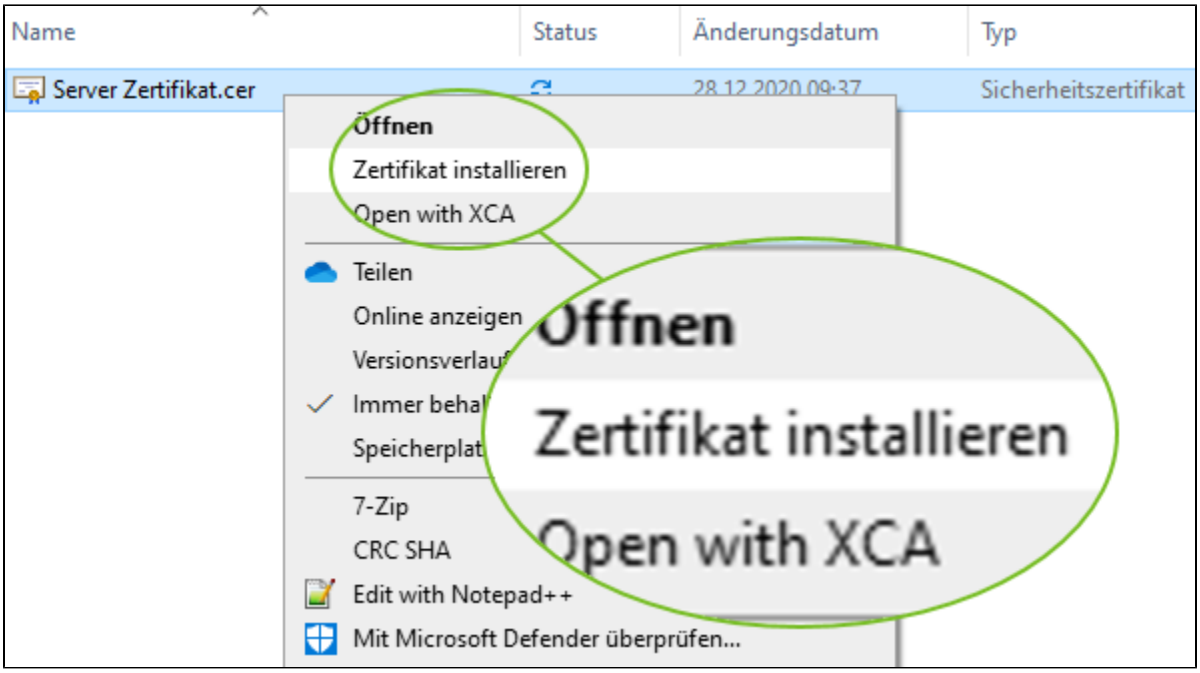
Die Zertifikatedatei muß die Endung .cer besitzen. Benennen Sie die Datei bitte um, wenn sie eine andere Endung haben sollte (Taste F2 oder rechte Maustaste > *Umbenennen*).

Falls Dateiendungen nicht sichtbar sind, aktivieren Sie bitte *Dateinamenerweiterungen* auf dem Reiter *Ansicht* in der Kopfzeile des Windows-Explorers:



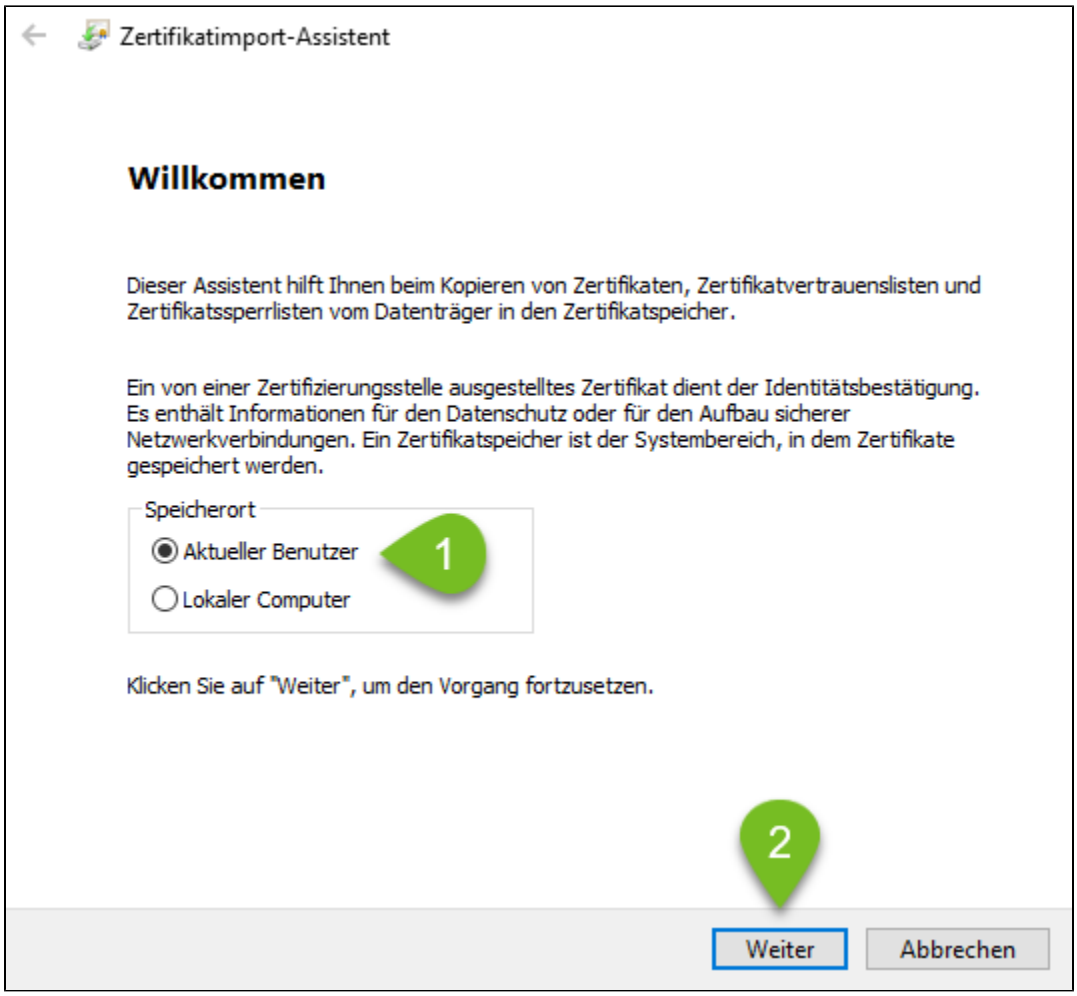
2

Klicken Sie mit der rechten Maustaste auf die Zertifikatsdatei und wählen *Zertifikat installieren*.



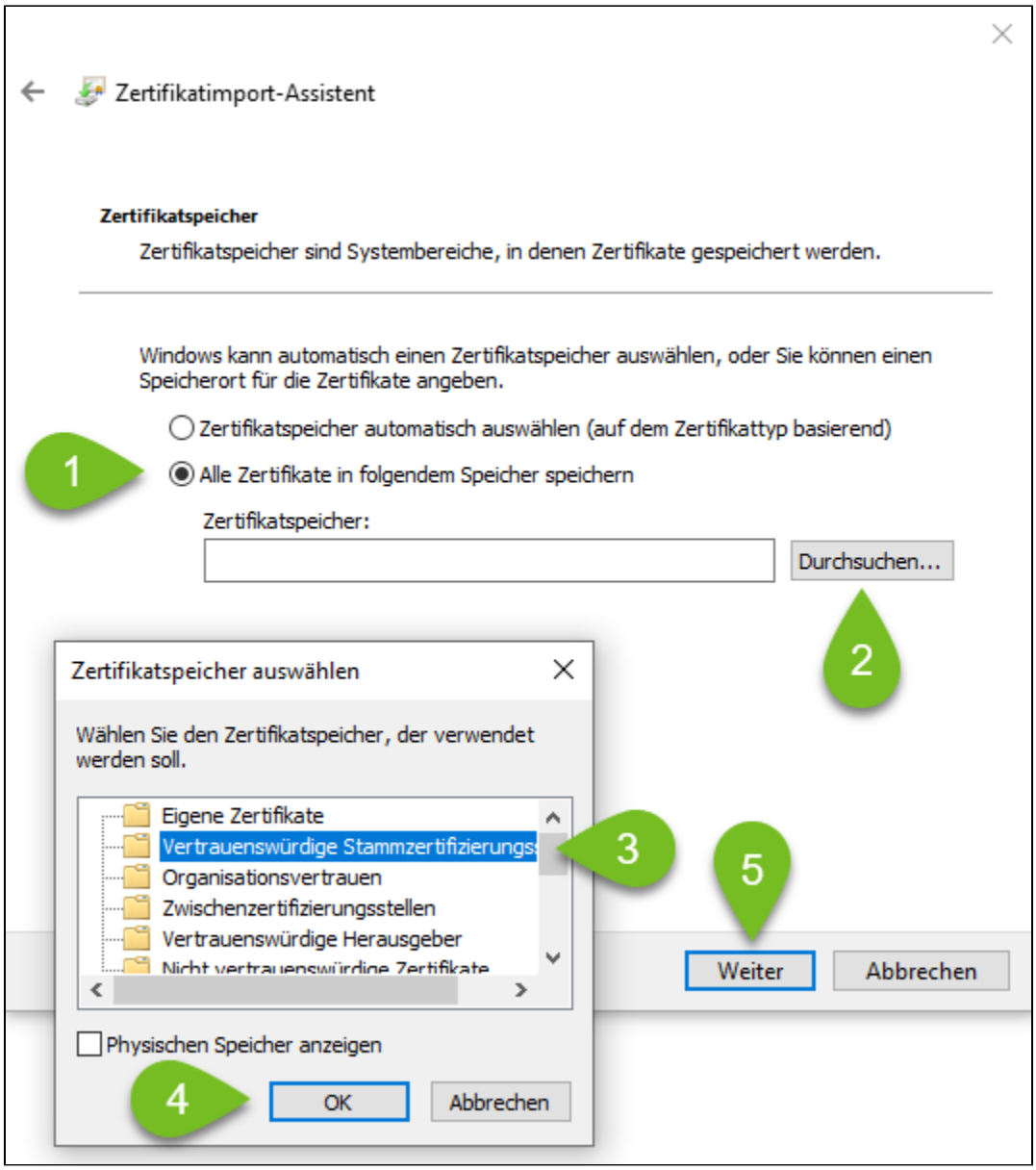
3

Wählen Sie im Zertifikatimport-Assistenten als Speicherort *Aktueller Benutzer* und klicken Sie anschließend auf *Weiter*.



4

Wählen Sie *Alle Zertifikate im folgenden Speicher speichern* aus und klicken auf *Durchsuchen*. Wählen Sie als Zertifikatsspeicher *Vertr auenswürdige Stammzertifizierungsstellen*, klicken auf *OK* und anschließend auf *Weiter*.



5

Klicken Sie auf *Fertig stellen* und bestätigen Sie, dass Sie das Zertifikat installieren möchten mit *Ja*.

Verwandte Artikel

- Windows: Einem Server-Zertifikat vertrauen
- Office 365: Aktivierung von Office 365 ProPlus auf einem Terminalserver
- Terminalserver: TAPI-Line-Zuordnung in Cluster-Umgebungen