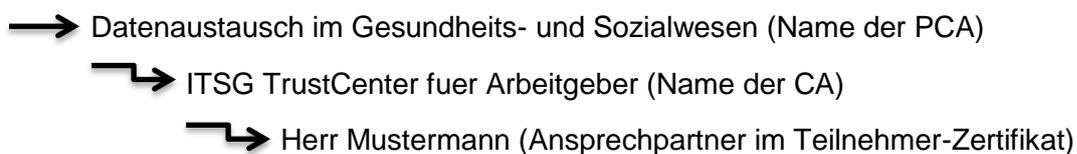


## Informationen mit Beispielen zur Verwendung der root Zertifikate

Ein Teilnehmer-Zertifikat für das Arbeitgeber- oder Leistungserbringerverfahren wird von einer Zertifizierungsstelle (CA) herausgegeben und veröffentlicht. Das Zertifikat einer Zertifizierungsstelle (CA) wird wiederum von einer übergeordneten Stammzertifizierungsstelle (PCA) zertifiziert und so wird der Zertifizierungspfad vom Teilnehmer-Zertifikat bis zum Wurzelzertifikat der PCA aufgelöst. Ohne die zugeordneten Zertifikate der PCA und der untergeordneten CA kann der Zertifizierungspfad des Teilnehmer-Zertifikats nicht vom System validiert werden. Bei der Überprüfung könnte eine Meldung angezeigt werden, dass die Integrität des Zertifikats nicht garantiert werden kann.

Beispiel eines Zertifizierungspfads:



Zur Validierung von Zertifikaten laden Sie bitte das entsprechende Wurzelzertifikat der PCA und das Zertifikat der untergeordneten CA herunter, welche das zu überprüfende Zertifikat im gleichen Gültigkeitszeitraum und mit entsprechendem Signaturhashalgorithmus ausgestellt haben. Im Zweifelsfall laden Sie alle CA-Zertifikate von einer übergeordneten PCA entsprechend für das Arbeitgeber- oder Leistungserbringerverfahren herunter.

### Beispiel 1:

Ihr SHA256-Zertifikat für das Arbeitgeberverfahren wurde im Januar 2016 erstellt. Laden Sie im gleichen Gültigkeitszeitraum (ab November 2014) mit entsprechendem SHA256-Signaturhashalgorithmus das Wurzelzertifikat der PCA mit der Seriennummer 32 und das CA-Zertifikat mit der Seriennummer 35 (Gültigkeitszeitraum 12.2015 bis 01.2021) herunter.

### Beispiel 2:

Ihr SHA256-Zertifikat für das Leistungserbringerverfahren wurde im Mai 2014 erstellt. Laden Sie im gleichen Gültigkeitszeitraum (ab November 2011) mit entsprechendem SHA256-Signaturhashalgorithmus das Wurzelzertifikat der PCA mit der Seriennummer 28 und das CA-Zertifikat mit der Seriennummer 2D (Gültigkeitszeitraum 12.2013 bis 01.2019) herunter.

Zum Importieren der heruntergeladenen root Zertifikate folgen Sie den Anweisungen für Ihr System oder im Handbuch Ihrer Verschlüsselungssoftware. Bei Fragen zu Ihrem System wenden Sie sich bitte an Ihren Systemadministrator. Bei Fragen zu Ihrer Verschlüsselungssoftware wenden Sie sich bitte an den Support des zuständigen Softwarehauses.