iQ.Suite KeyManager

Verwendung und Konfiguration von DigiCert S/MIME-Zertifikaten

Dokumentversion 3.2

Stand: 19.03.2024

Inhalt

1 Einführung

Um öffentliche S/MIME-Zertifikate von DigiCert auch über iQ.Suite KeyManager verwenden zu können, müssen Sie zunächst ein **DigiCert ONE**-Konto besitzen und über den Trust Lifecycle Manager ein **CertCentral**-Konto konfiguriert haben. Diese Konten müssen über oder mit DigiCert angelegt werden. [1]

Wenn diese Schritte erfolgreich angelegt, durchlaufen und über DigiCert validiert sind, können Sie das Client-Zertifikat im iQ.Suite KeyManager Konnektor angeben und verwenden.

Zusammenspiel „KeyManager – DigiCert One – CertCentral“

iQ.Suite KeyManager (KMS) fordert ein Zertifikat bei DigiCert ONE an, DigiCert ONE leitet die Anforderung an CertCentral weiter.

[1] https://docs.digicert.com/en/trust-lifecycle-manager/how-to-guides/issue-public-s-mime-certificates-from-certcentral-using-the-gbs-iq-suite-keymanager-software.html

2 Konto in DigiCert ONE

DigiCert ONE (DC1) ist die PKI-Lösung und Verwaltungsplattform der DigiCert. Ein Teil davon ist der Trust LifeCycle Manager (TLM), zu dem sich iQ.Suite KeyManager verbindet.

Falls Ihre Organisation über kein Konto verfügt, beachten Sie folgende Hinweise:

- Für ehemalige **QuoVadis-Kunden** muss das Konto manuell von Ihrem DigiCert Account Manager angelegt werden.

  Ihr DigiCert Account Manager wird Sie nach Kontaktdaten (Technical, Administrative und Admin) fragen. Wenn Ihnen kein DigiCert Account Manager bekannt ist, kontaktieren Sie bitte den DigiCert Support.

- Wenn Sie ein **neuer Kunde** sind, gehen Sie wie folgt vor:

  1. Unter https://digicert.com wählen Sie „Contact us“.
  2. Teilen Sie mit, dass Sie Zugriff auf den **Trust LifeCycle Manager** sowie das Template **Public S/MIME Secure Email using CMP (via CertCentral)** benötigen, um Zertifikate per iQ.Suite KeyManager zu beantragen.
  3. Sie werden dann von einem Account Manager kontaktiert, mit dem Sie Ihre Bestellung besprechen können und der Ihr Konto erstellt.

Das Konto benötigt eine Multi-Faktor-Authentifizierung mithilfe einer Authenticator App.

Nachdem das Konto erstellt ist, prüfen Sie die Konfiguration.
Das Unternehmenskonto (Organisation), Benutzer, Business Unit, Seat Assignment sollten eingerichtet sein, bevor mit der Konfiguration in iQ.Suite KeyManager begonnen wird.

3 Konto in CertCentral

Auf **CertCentral** werden die Zertifikate beantragt. Dieses Konto wird in einem späteren Schritt mit dem DigiCert ONE-Konto verbunden.

Sie können das Konto auf einer dieser Webseiten selbstständig anfordern:

- EU-Konten:
  https://certcentral.digicert.eu/account/login.php
- US-Konten (für US und Kanada):
  https://login.digicert.com/account/login.php

Die Erstellung dieses Kontos hängt *nicht* von dem DigiCert ONE-Konto ab. Beide Konten können gleichtzeitig erstellt werden.

Das Konto benötigt eine Multi-Faktor-Authentifizierung und die Authenticator App.

Nachdem das Konto erstellt wurde, gehen Sie wie folgt vor:

1. Erstellen und validieren Sie die Organisation (Menü **Zertifikate > Organisationen**).

   Die Validierung erfolgt manuell durch DigiCert und kann mehrere Tage in Anspruch nehmen. Bei Rückfragen senden Sie eine E-Mail an standard.validation.de@digicert.com.

2. Erstellen und validieren Sie die E-Mail-Domänen (Menü **Zertifikate > Domänen**).

   Die Validierung kann vollautomatisch z.B. über DNS oder E-Mail erfolgen.

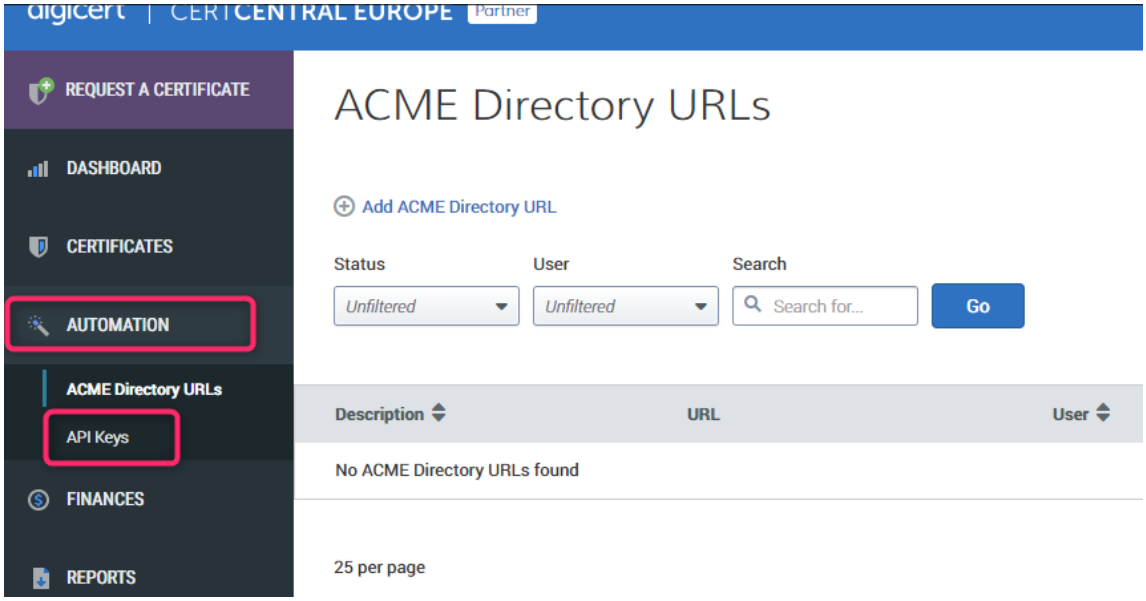
4 Konfiguration der Schnittstelle

4.1 CertCentral

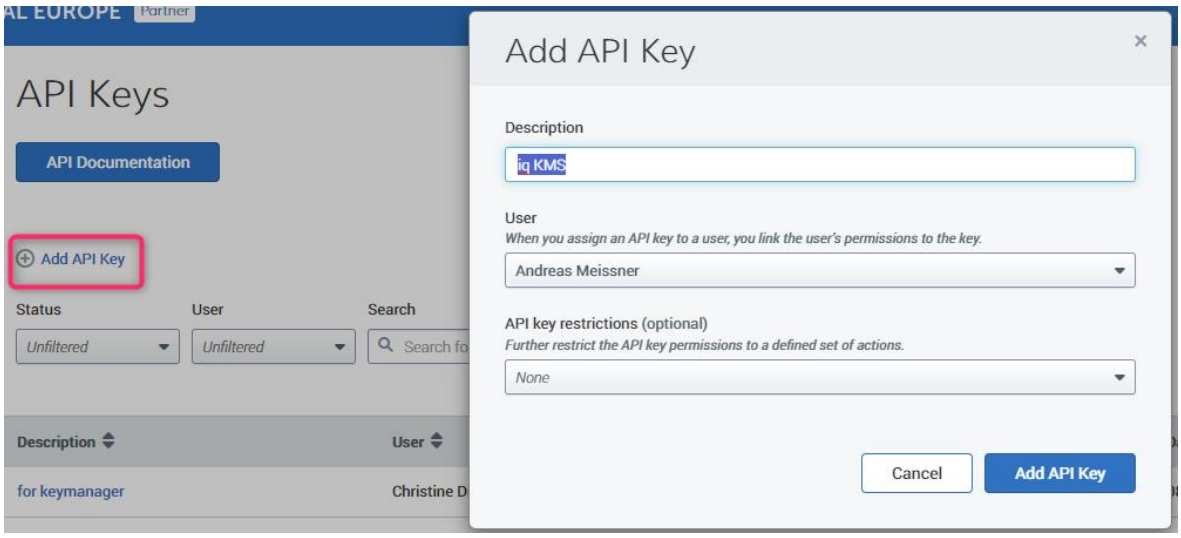
Melden Sie sich an CertCentral an:
https://certcentral.digicert.eu/account/login.php?lang=de

Erstellen Sie dann in CertCentral einen **API-Schlüssel ohne Beschränkungen**:

1. Klicken Sie auf **Automation > API Keys**: (URL: https://certcentral.digicert.eu/secure/automation/api-keys/):

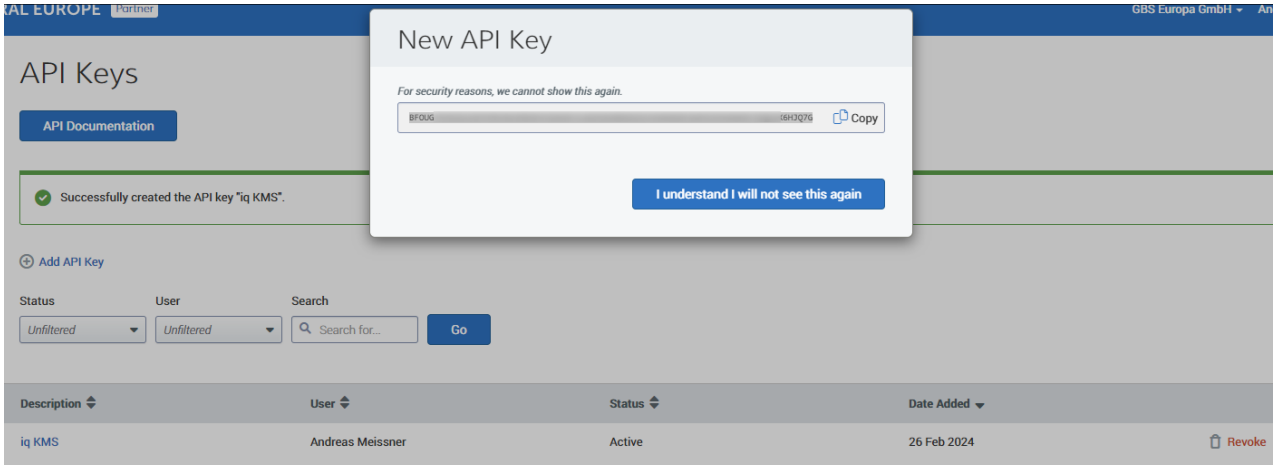


2. Klicken Sie auf **Add API Key** und tragen Sie bei **Description** den gewünschten Namen ein:



3. **Wichtig:**
   Der so erzeugte Schlüssel wird nach Hinzufügen nicht mehr vollständig angezeigt.

   Aus o.g. Grund kopieren Sie den Schlüssel vorher in die Zwischenablage und speichern Sie ihn an einer sicheren Stelle. Weitere Einträge kommen im späteren Verlauf ebenfalls noch hier hinzu.

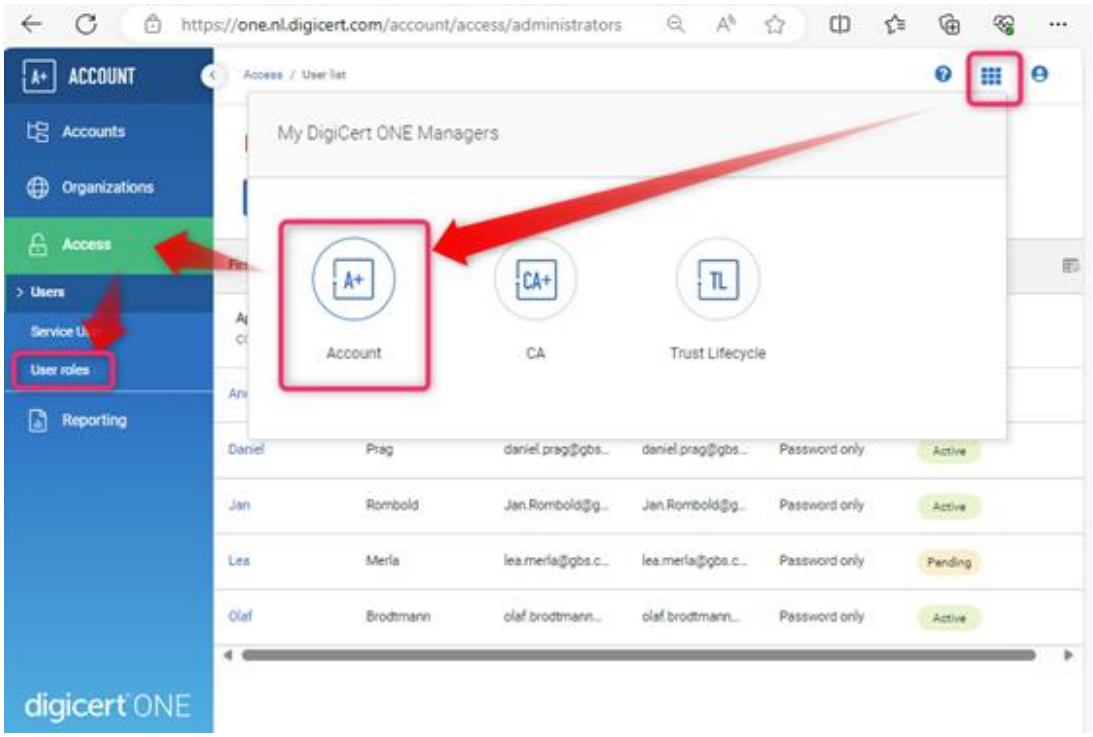


4.2 DigiCert ONE

Melden Sie sich an DigiCert ONE an:
https://one.nl.digicert.com

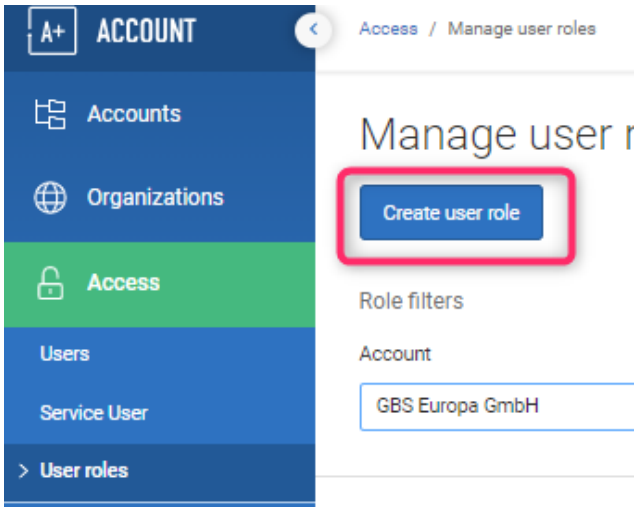
In DigiCert ONE gehen Sie wie folgt vor:

1. Öffnen Sie über das Symbol (oben rechts) den **Account Manager** und gehen dann über **Account > Access > User roles**:

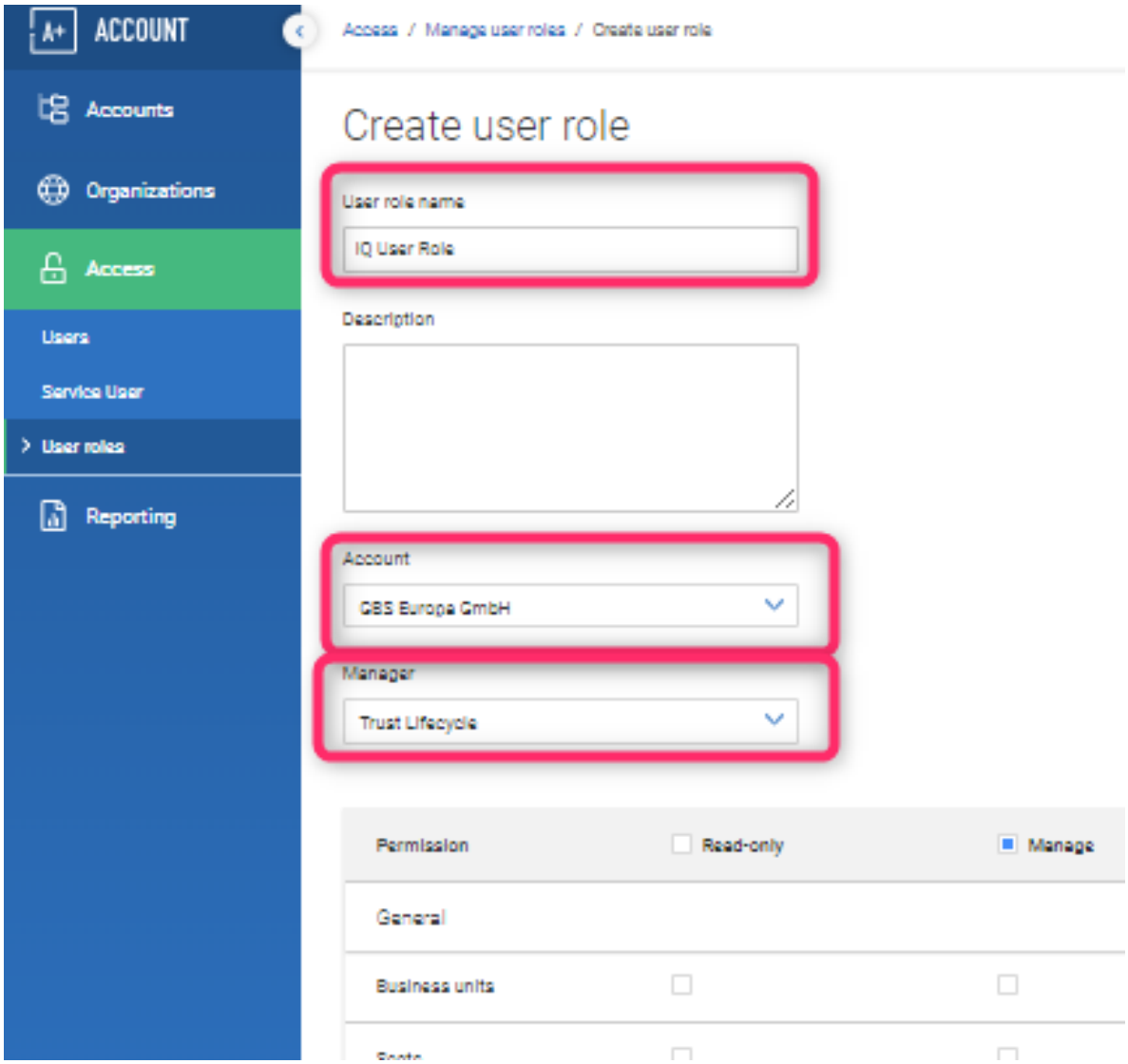


URL: https://one.nl.digicert.com/account/access/manage-user-roles

2. Um eine neue **Rolle** für den Service-Benutzer zu erstellen, klicken Sie im Bereich **Access > User roles** auf den Button **Create user role**:

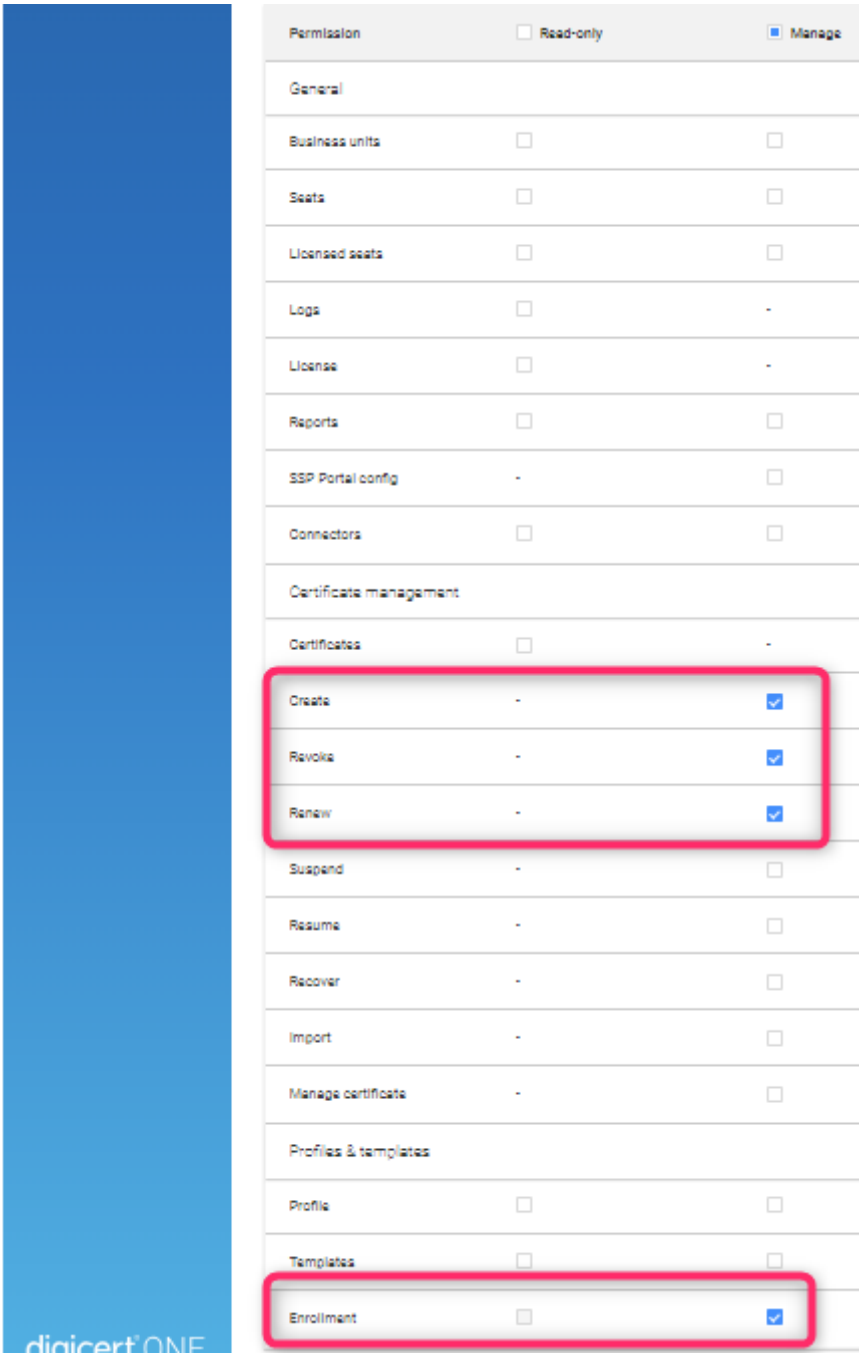


Folgender Dialog öffnet sich:

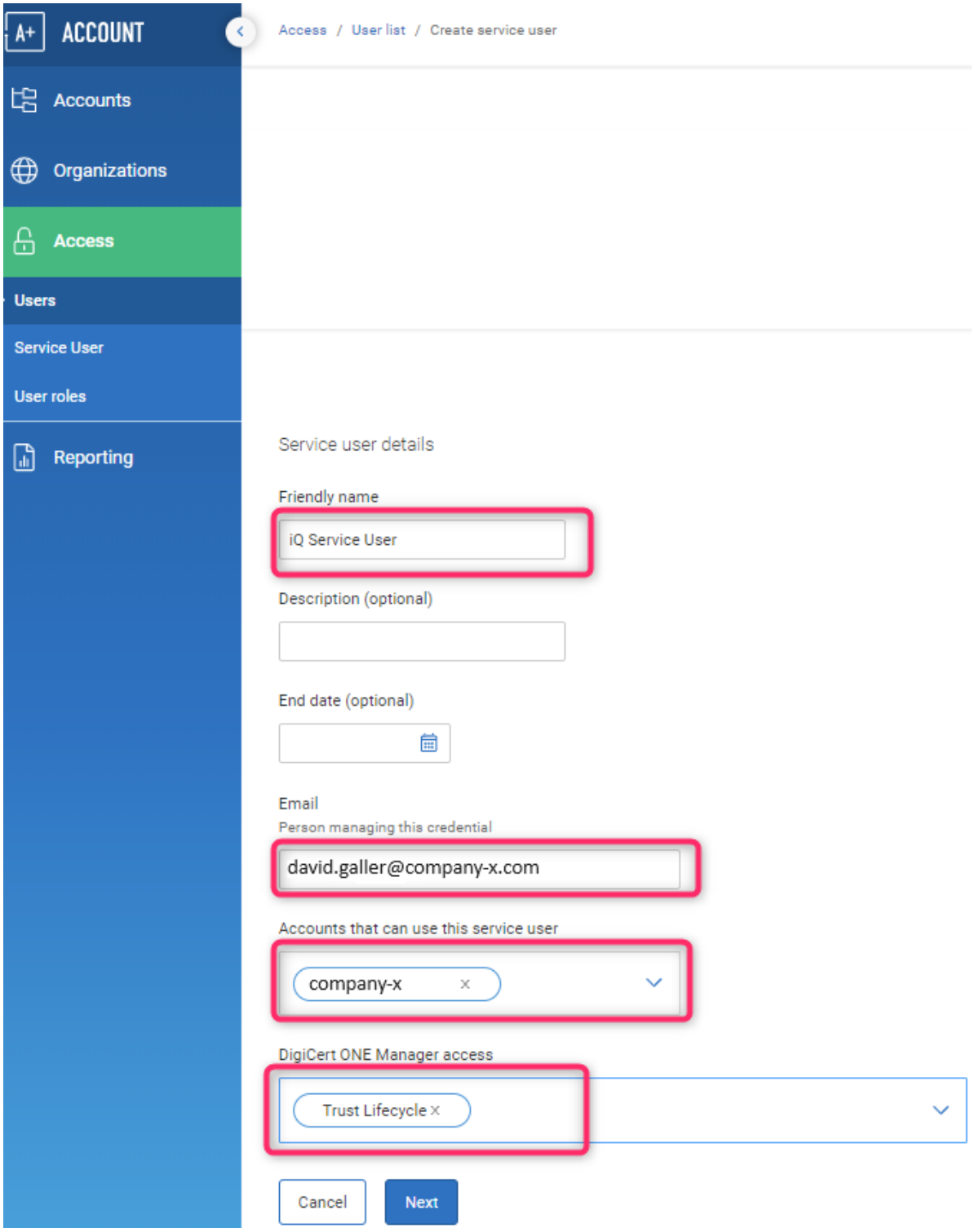


- Tragen Sie Bei **User role name** einen beliebigen **Namen** für die Benutzerrolle ein, z.B. „iQ User Role“.
- Wählen Sie bei **Account** Ihr angelegtes Konto aus.
- Wählen Sie bei **Manager** ‚Trust Lifecycle‘ aus.

3. In der Tabelle unter dem Feld „Manager“ aktivieren Sie in der Spalte **Manage** folgende **Berechtigungen**:
   - ☐ Create (notwendig)
   - ☐ Revoke (empfohlen)
   - ☐ Renew (empfohlen)
   - ☐ Enrollment (notwendig)

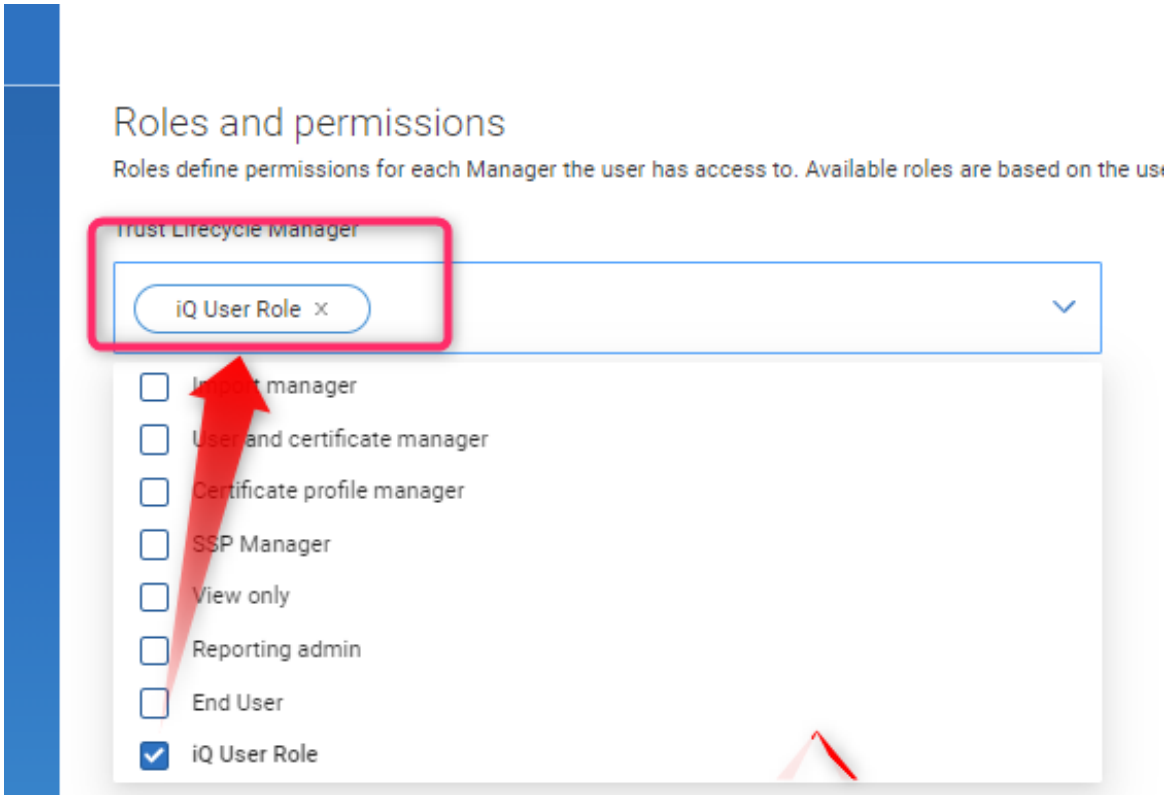


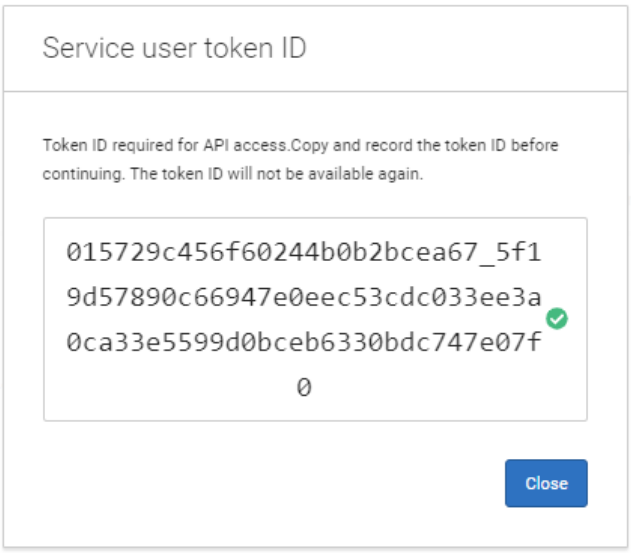
4. Erstellen Sie unter **Access > Service User** einen Service-Benutzer wie folgt:



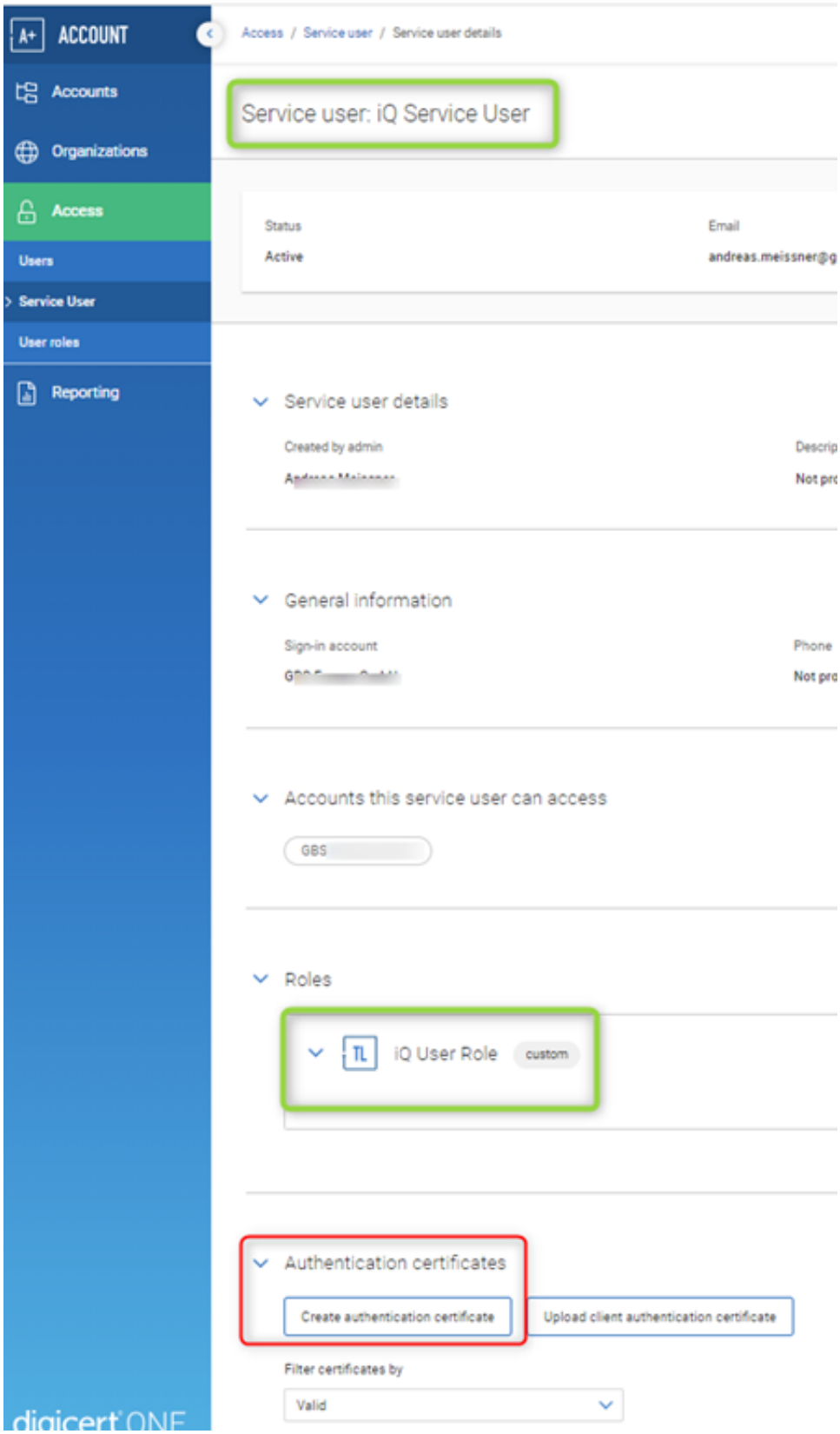
URL: https://one.nl.digicert.com/account/access/service-user

5. Klicken Sie auf **Next** und weisen Sie dem neu erstellten Service-Benutzer die zuvor erstellte **Rolle** zu:

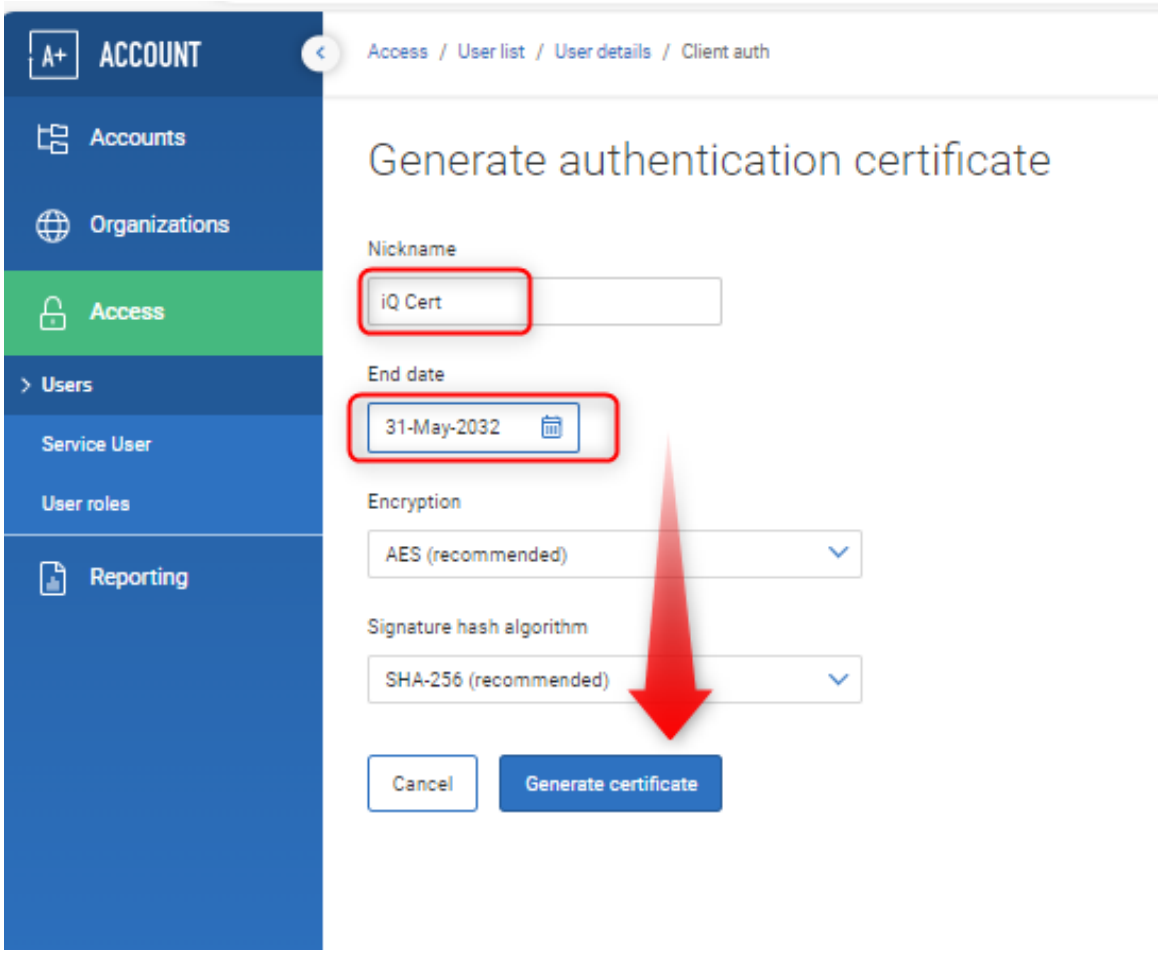




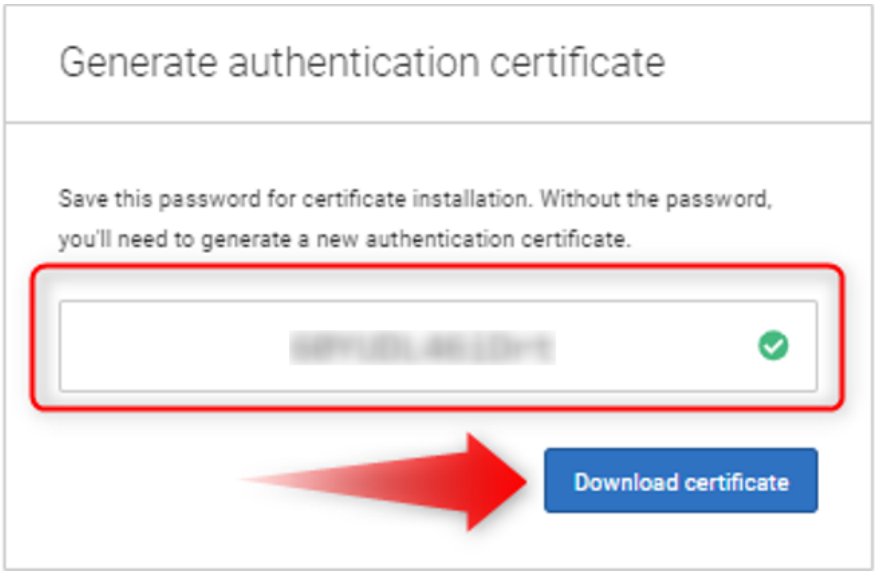
6. Klicken Sie unter **Access > Service user > Service user details > Authentication certificates** auf **Create authentication certificate**, um ein Authentifizierungszertifikat zu erstellen.



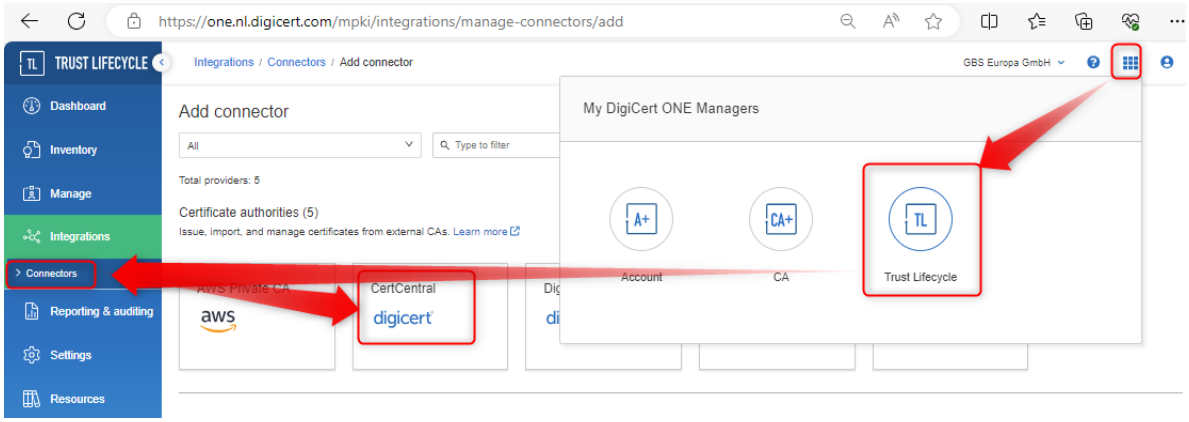
7. Tragen Sie einen **Nickname** ein und wählen Sie ein **EndDate**, an dem das Zertifikat ablaufen soll. Klicken Sie dann auf **Generate certificate**:



8. Speichern Sie das **Passwort** und laden Sie das Zertifikat herunter, das später in iQ.Suite KeyManager bei dem Konnektor als **Client-Zertifikat** verwendet wird:

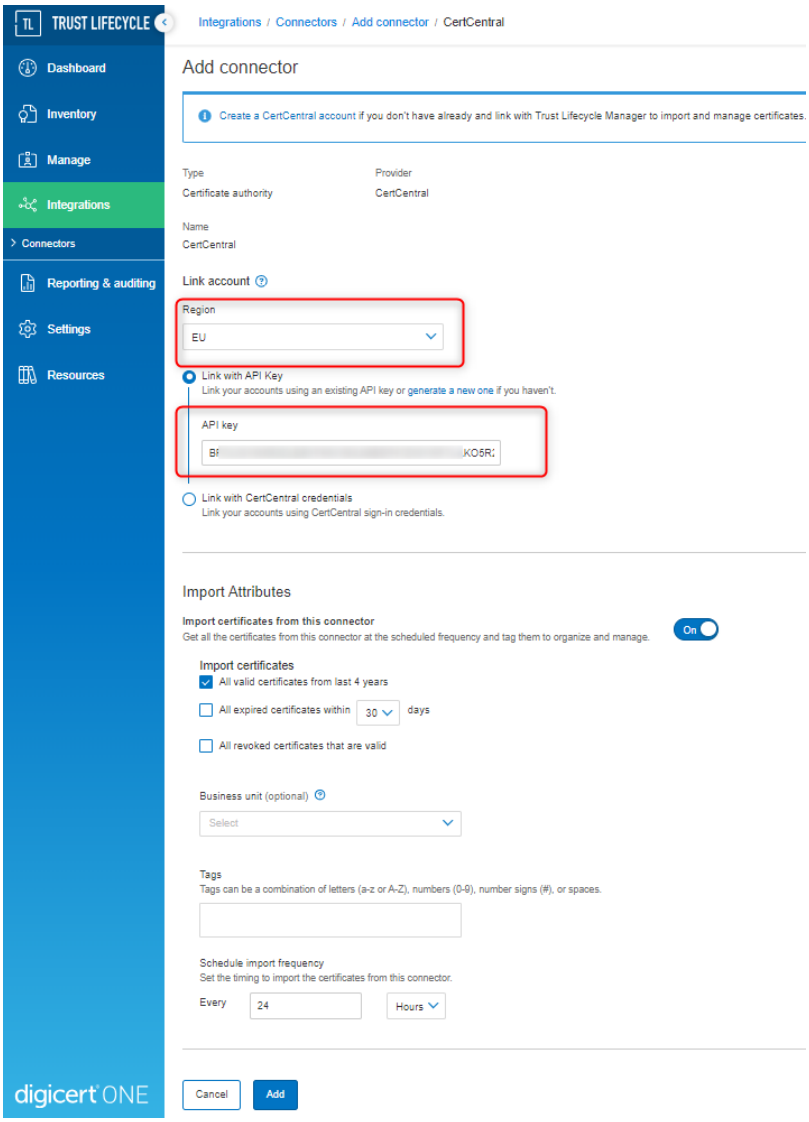


9. Öffnen Sie über das Symbol (oben rechts) den **Trust Lifecycle Manager** und erstellen Sie einen **CertCentral Connector** (Menü **Integration > Connectors > CertCentral**):



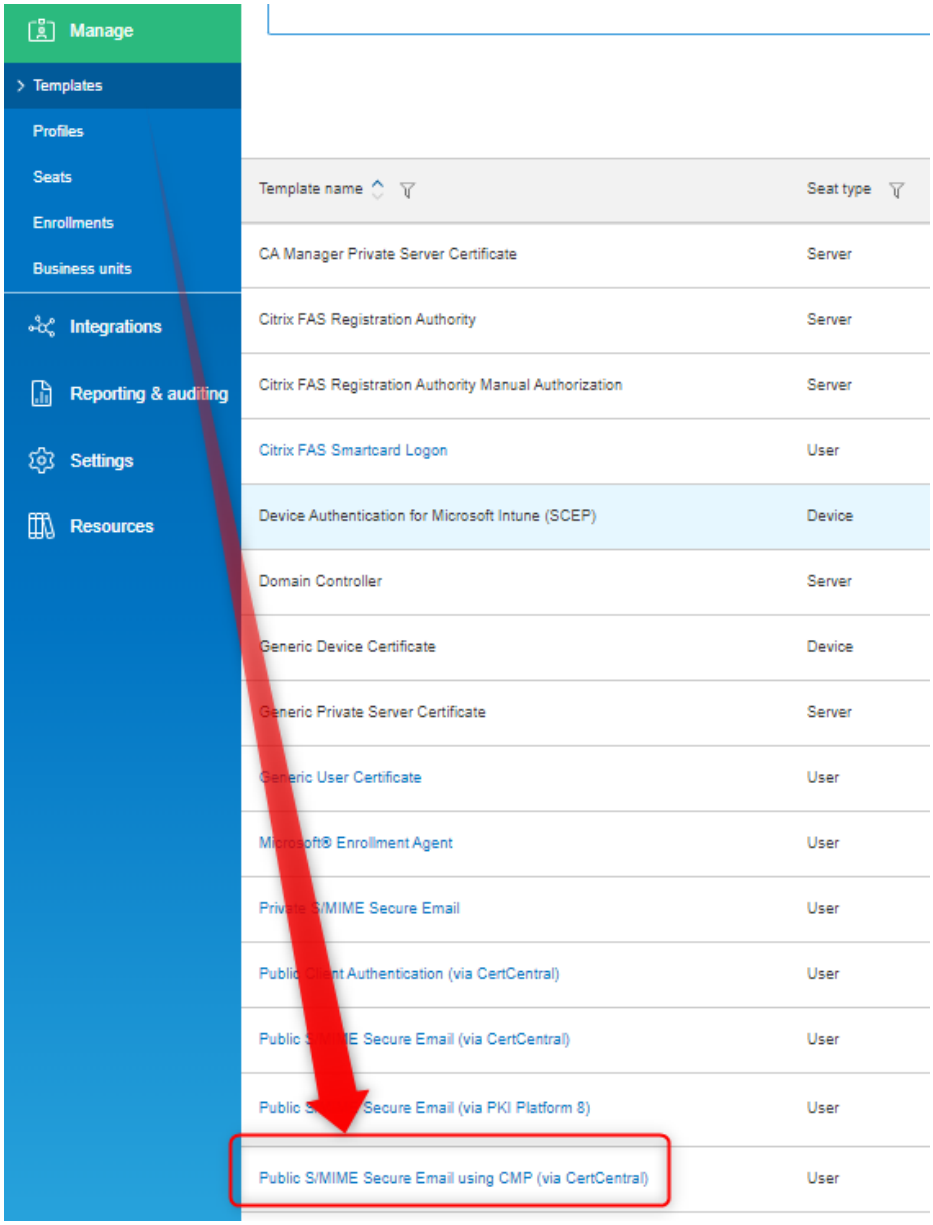
URL: https://one.nl.digicert.com/mpki/integrations/manage-connectors

10. Im Dialog **Add connector** nehmen Sie folgende Einstellungen vor:

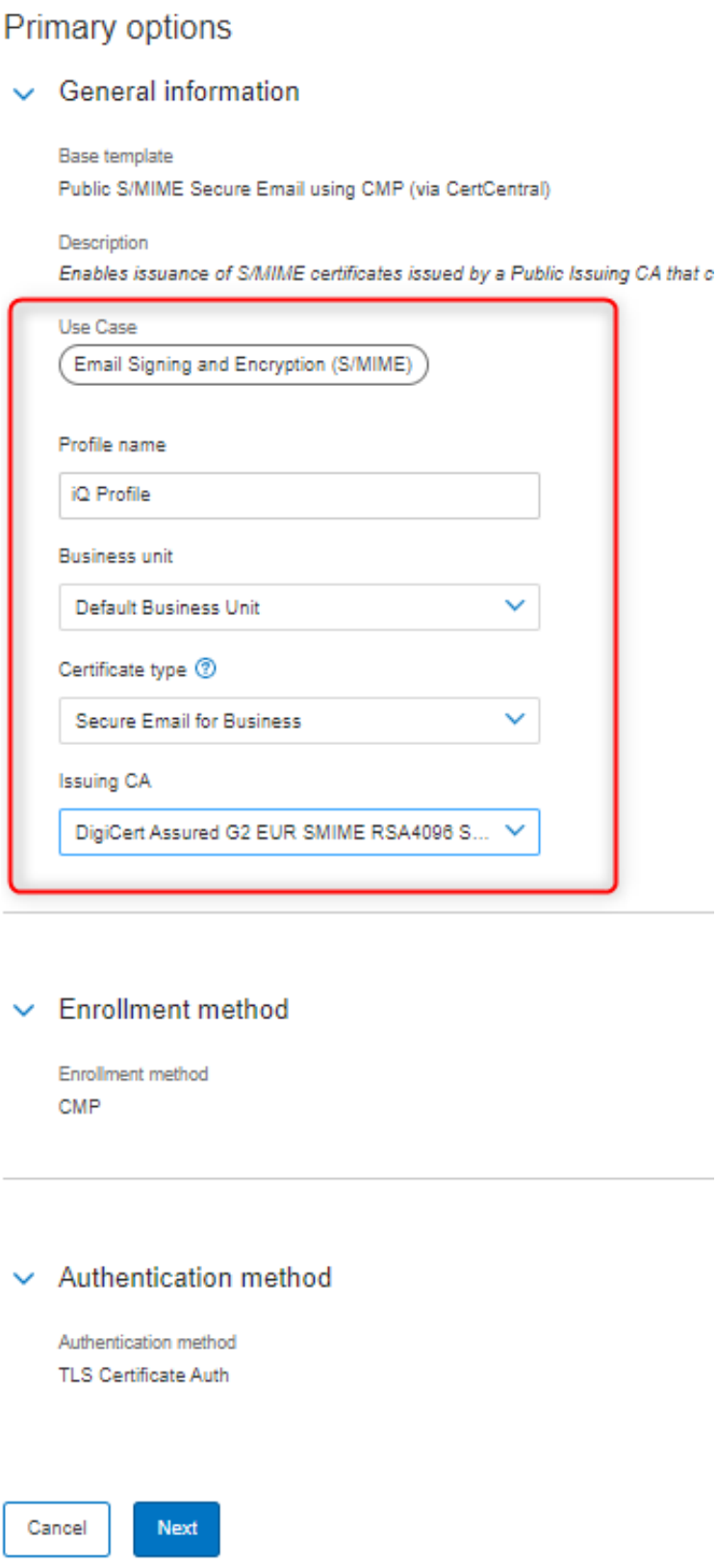


- Wählen Sie bei Region den passenden Wert aus:
  - **US** oder **EU**
    Dies hängt davon ab, ob Sie ein CertCentral US-Konto oder ein CertCentral EU-Konto erstellt haben. Wenn Sie dies nicht beachten, ist der API Key ungültig.
- Tragen Sie bei **API Key** den in CertCentral erstellten API-Schlüssel ein.

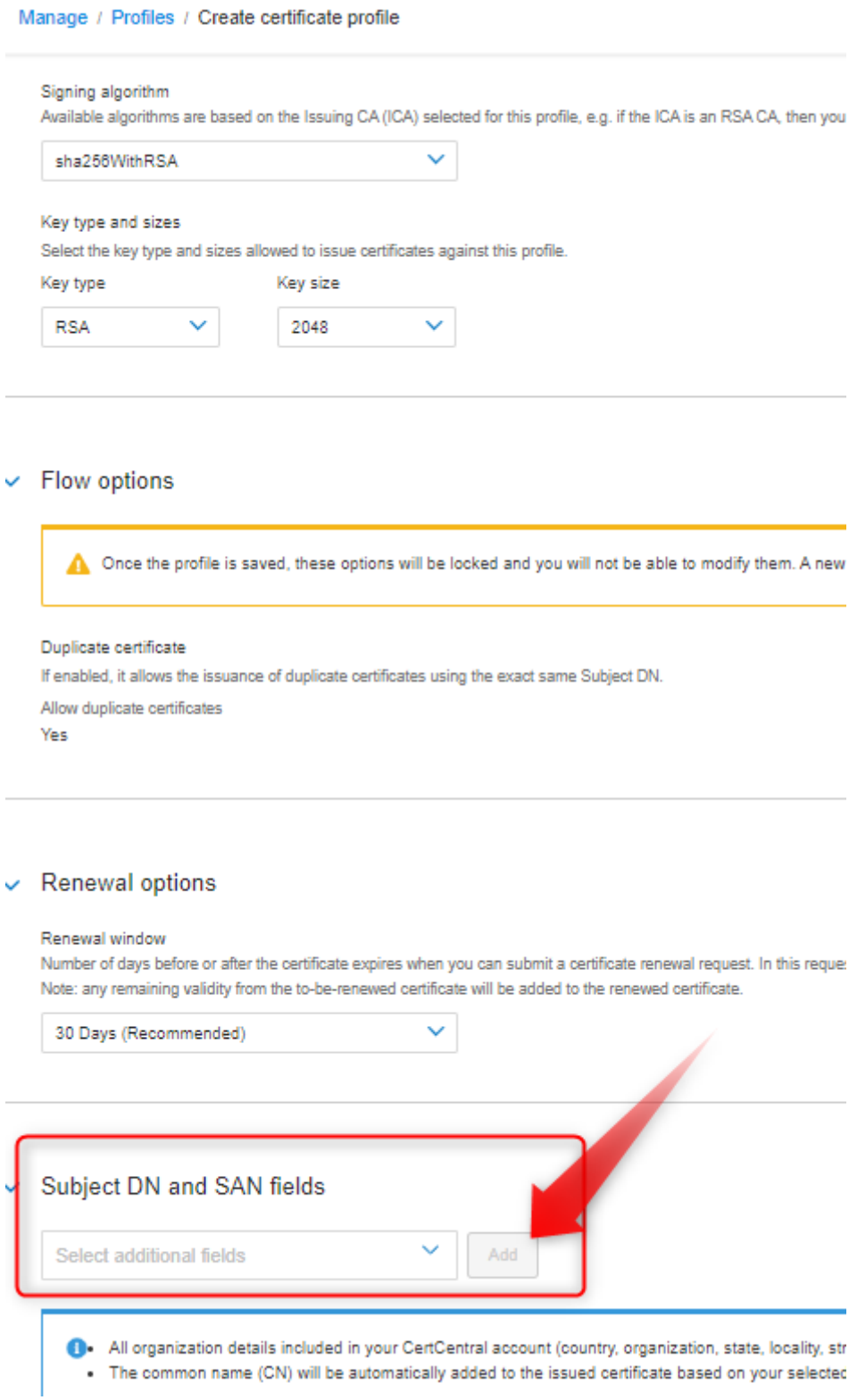
11. Erstellen Sie ein **Zertifikatsprofil** (Menü **Profiles > Templates**):
    https://one.nl.digicert.com/mpki/manage/templates
12. Klicken Sie Sie unter **Manage > Templates** auf das Template **Public S/MIME Secure Email using CMP (via CertCentral)**:



13. Wählen Sie bei **Certificate type** den Zertifikatstyp ‚Secure Email for Business' und bei **Issuing CA** das Root-Zertifikat von DigiCert aus:

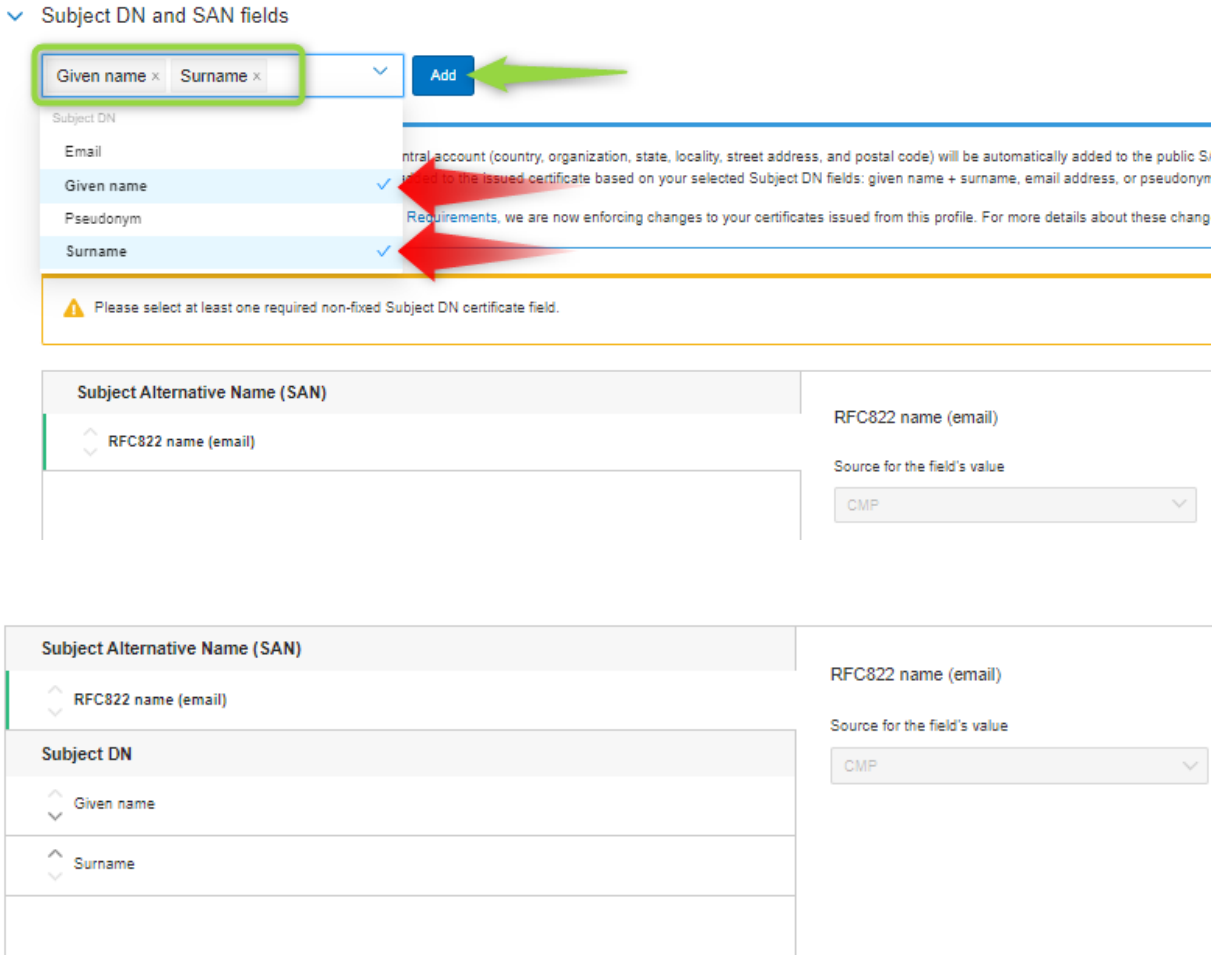


14. Öffnen Sie **Manage > Profiles > Create certificate profile** und klicken Sie dort im Feld **Subject DN and SAN fields** auf **Add**:

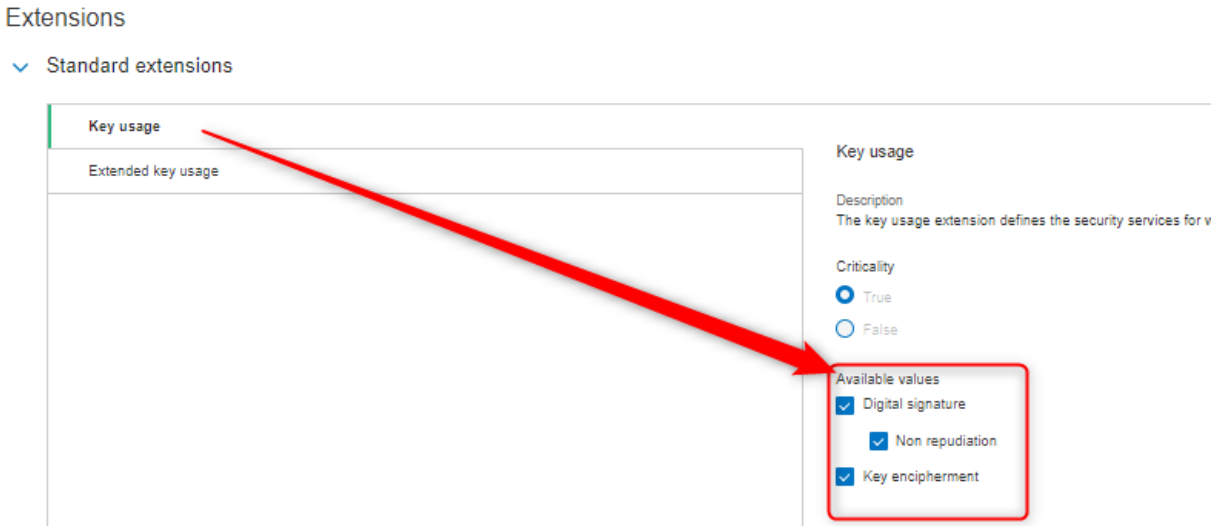


- Bei den SAN-Feldern ist **RFC822 name (email)** notwendig. Außerdem müssen Sie für **Subject DN** den Vornamen und Nachnahmen gleichzeitig auswählen und hinzufügen.

  Wichtig:
  Bei iQ.Suite KeyManager ≤ 8.0.9 muss zusätzlich **E-Mail-Adresse** hinzugefügt werden.
  Ab KeyManager 8.0.10 darf die E-Mail-Adresse *nicht* hinzugefügt werden.

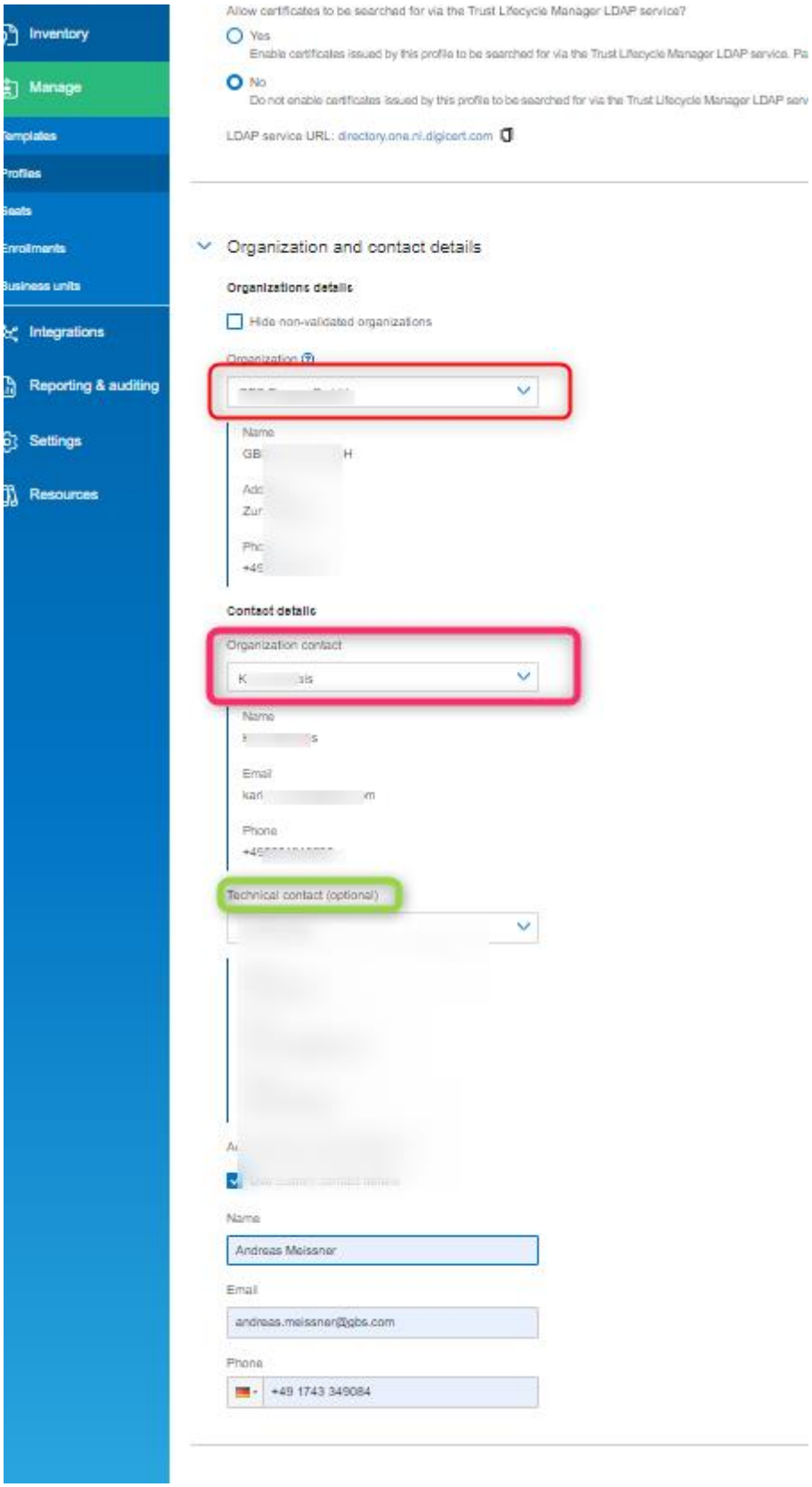


15. Bei **Standard Extensions** aktivieren Sie folgende Checkboxes:
    - ☐ Digital signature
    - ☐ Non repudiation
    - ☐ Key encipherment

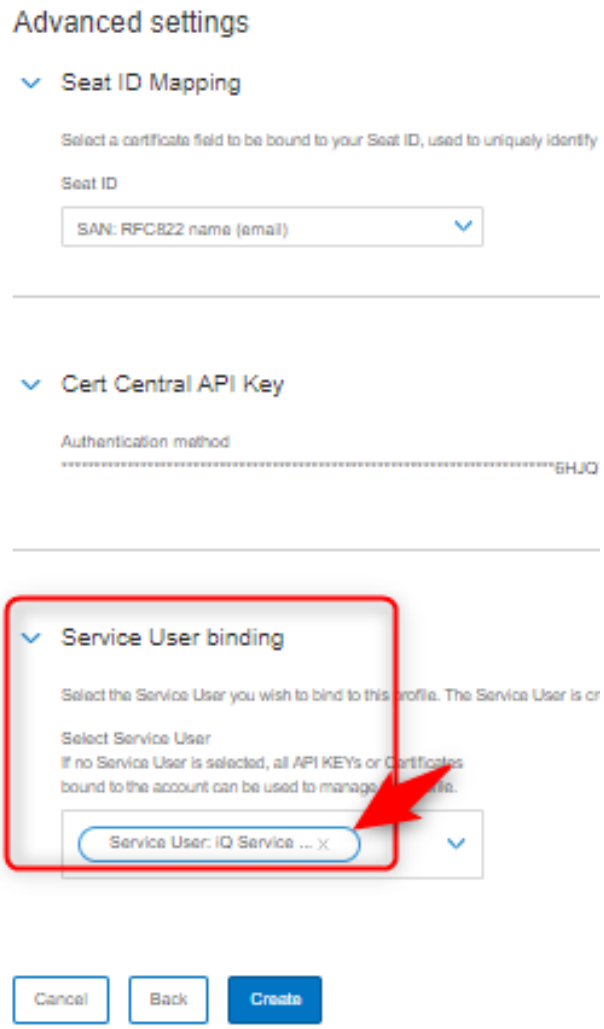


16. Bei **Extended key usage** behalten Sie die Default-Einstellungen bei:

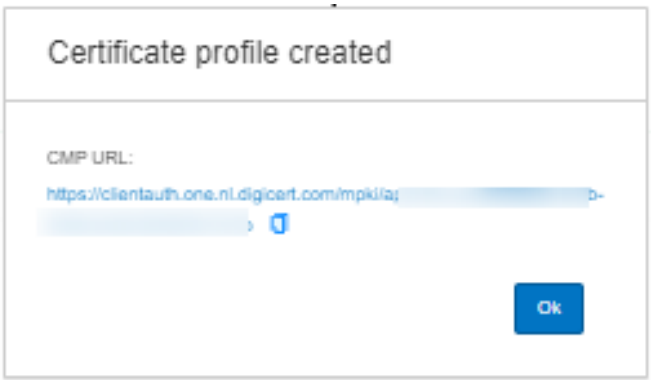
17. Unter **Manage > Profiles > Organization and contact details** wählen Sie die **Organzation** und einen **Organzation contact**. Optional können Sie einen Technical contact angeben:



18. Der oben angelegte **Service-Benutzer** muss zugeordnet werden. Wählen Sie hierzu bei **Service User binding** den angelegten Service-Benutzer:



Wichtig:
Nachdem das Profil angelegt ist, wird die **CMP URL** angezeigt. Dies ist die Verbindungs-URL, die in der iQ.Suite KeyManager-Konfiguration verwendet wird.

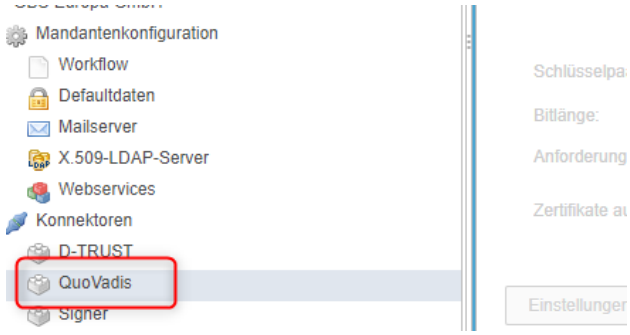


4.3 iQ.Suite KeyManager

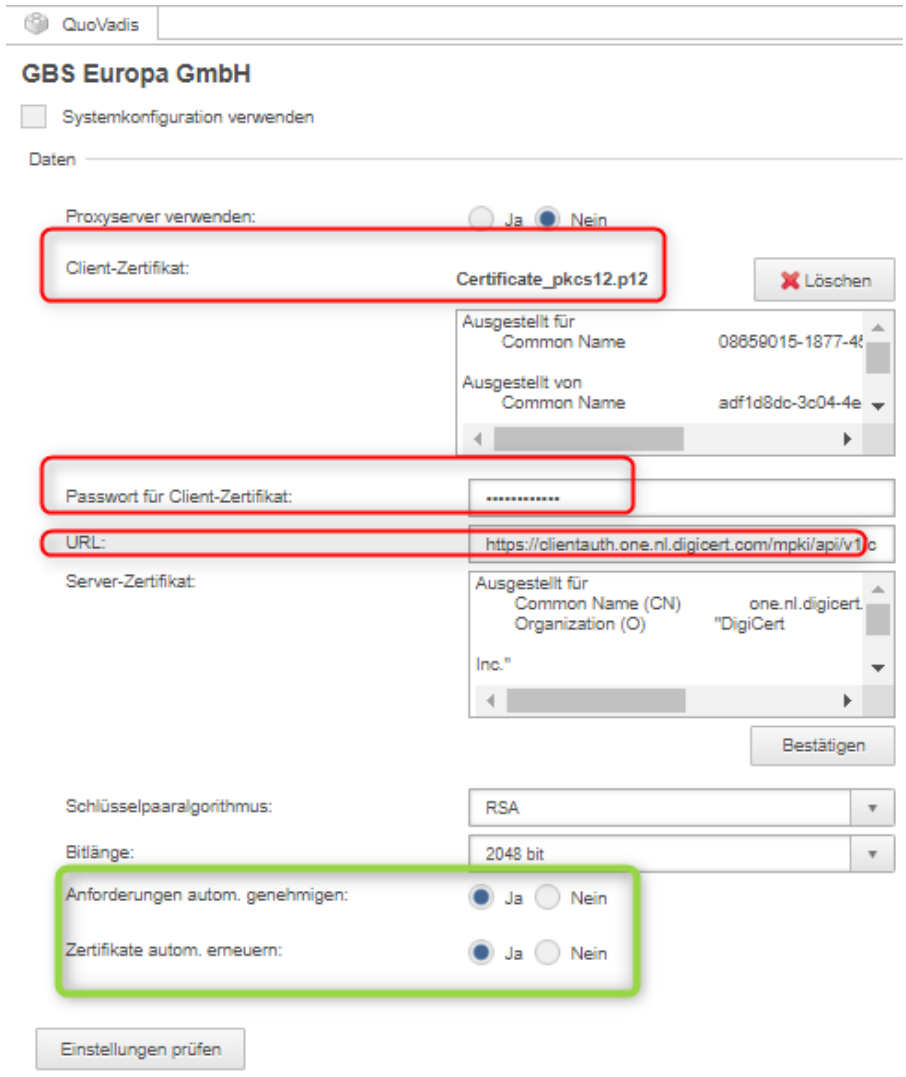
In iQ.Suite KeyManager muss die Verbindung zu DigiCert ONE wie folgt hergestellt werden:

1. Öffnen Sie die Konfiguration des Konnektors:

   DigiCert Connector (KeyManager ≥ 9) oder
   QuoVadis Connector (KeyManager ≤ 8.0.10)



2. Importieren Sie das **Client-Zertifikat** und tragen bei **URL** die CMP URL ein:



4.4 Weitere Dokumentationen

DigiCert hat eine Dokumentation zur iQ.Suite KeyManager-Anbindung erstellt:

https://docs.digicert.com/en/trust-lifecycle-manager/how-to-guides/issue-public-s-mime-certificates-from-certcentral-using-the-gbs-iq-suite-keymanager-software.html

Eine allgemeine DigiCert-Dokumentation finden Sie unter:

https://docs.digicert.com/en/certcentral/upgrade-to-certcentral.html

5 Über GBS

GBS Europa GmbH ist führender Anbieter von Lösungen und Services in den Bereichen Messaging Security und Workflow für die Domino und Microsoft Collaboration Plattformen. Weltweit vertrauen mehr als 5.000 Kunden und 4 Millionen Anwender auf die Expertise von GBS. Der Konzern ist in Europa, Nordamerika sowie Asien tätig.

Website: www.gbs.com

E-Mail-Adresse: info@de.gbs.com

Standorte: https://gbs.com/contact-us