



iQ.Suite KeyManager

Verwendung und Konfiguration von
DigiCert S/MIME-Zertifikaten

Dokumentversion 3.2

Stand: 19.03.2024

Inhalt

1	Einführung	3
2	Konto in DigiCert ONE.....	4
3	Konto in CertCentral	5
4	Konfiguration der Schnittstelle	6
4.1	CertCentral	6
4.2	DigiCert ONE	8
4.3	iQ.Suite KeyManager	23
4.4	Weitere Dokumentationen	24
5	Über GBS	25

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 gleichzeitig 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

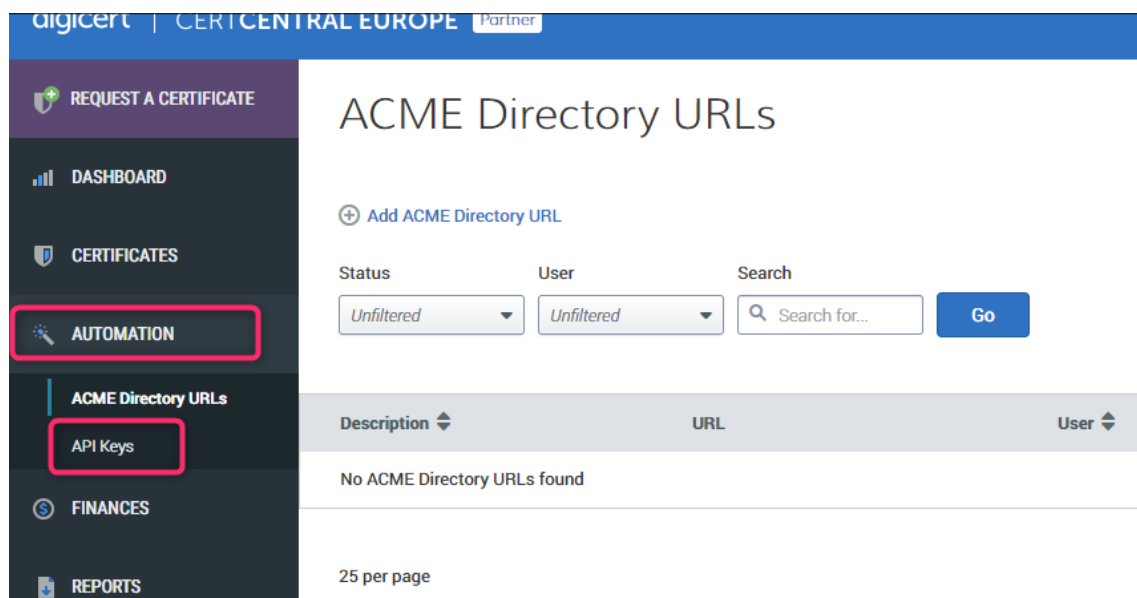
4.1 CertCentral

Melden Sie sich an CertCentral an:

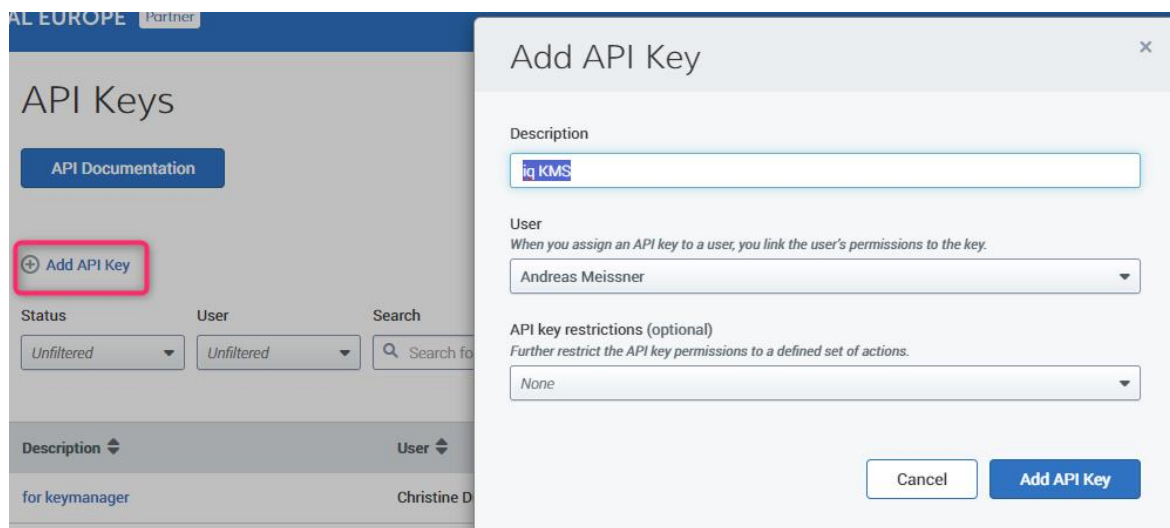
<https://certcentral.digicert.eu/account/login.php?lang=de>

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/>):



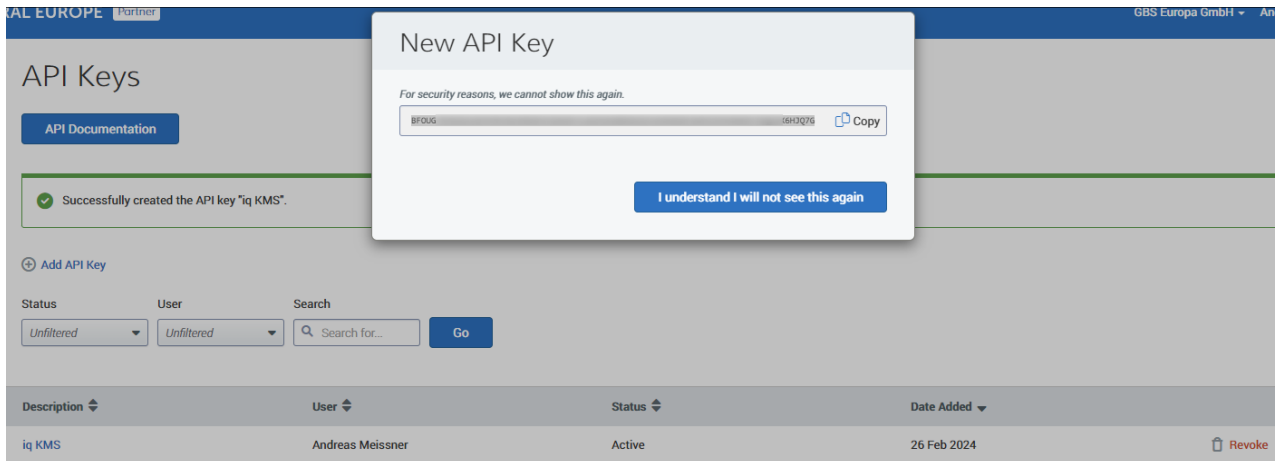
2. Klicken Sie auf **Add API Key** und tragen Sie bei **Description** den gewünschten Namen ein:



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.



API Keys

API Documentation

Successfully created the API key "iq KMS".

I understand I will not see this again

Add API Key

Status: Unfiltered, User: Unfiltered, Search: Search for... Go

Description	User	Status	Date Added
iq KMS	Andreas Meissner	Active	26 Feb 2024


Revoke

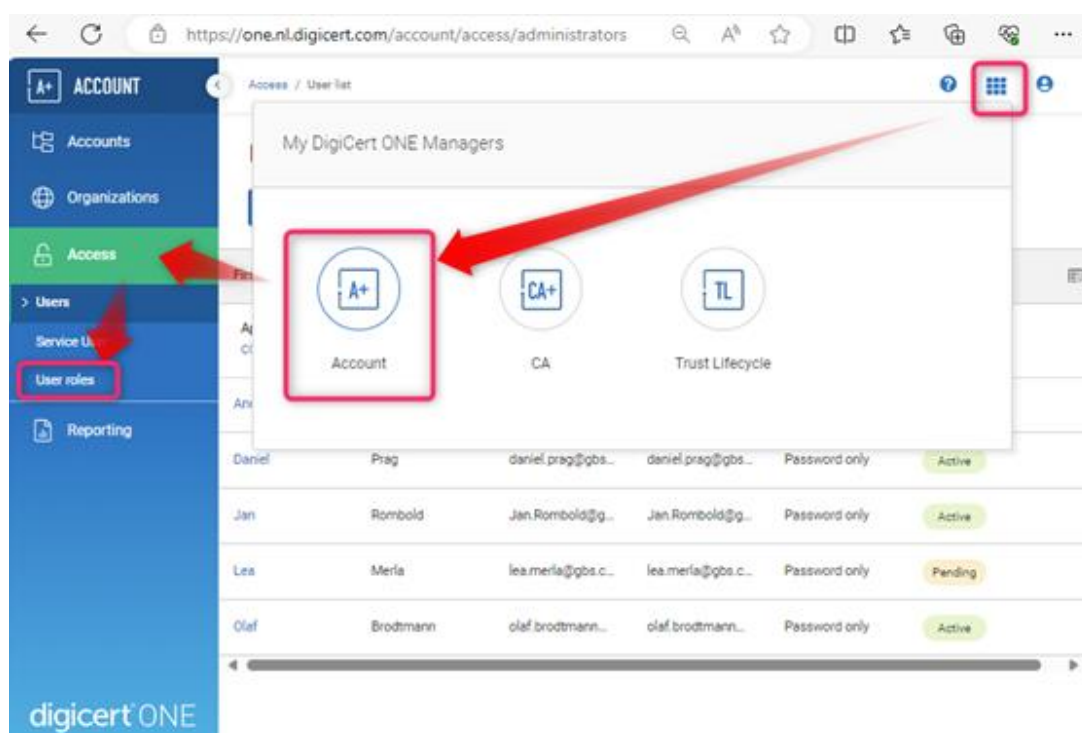
4.2 DigiCert ONE

Melden Sie sich an DigiCert ONE an:

<https://one.nl.digicert.com>

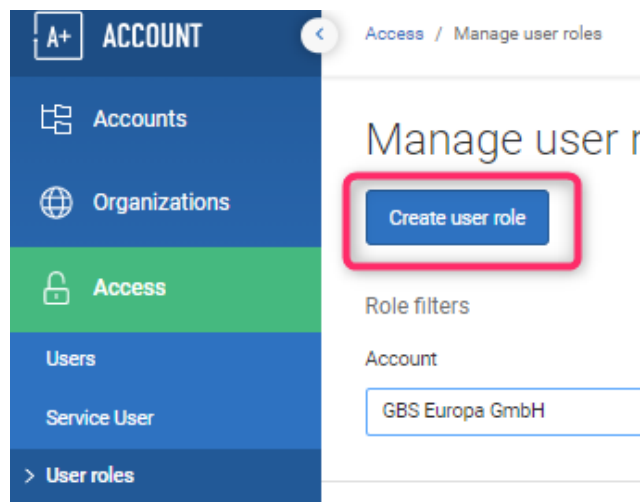
In DigiCert ONE gehen Sie wie folgt vor:

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

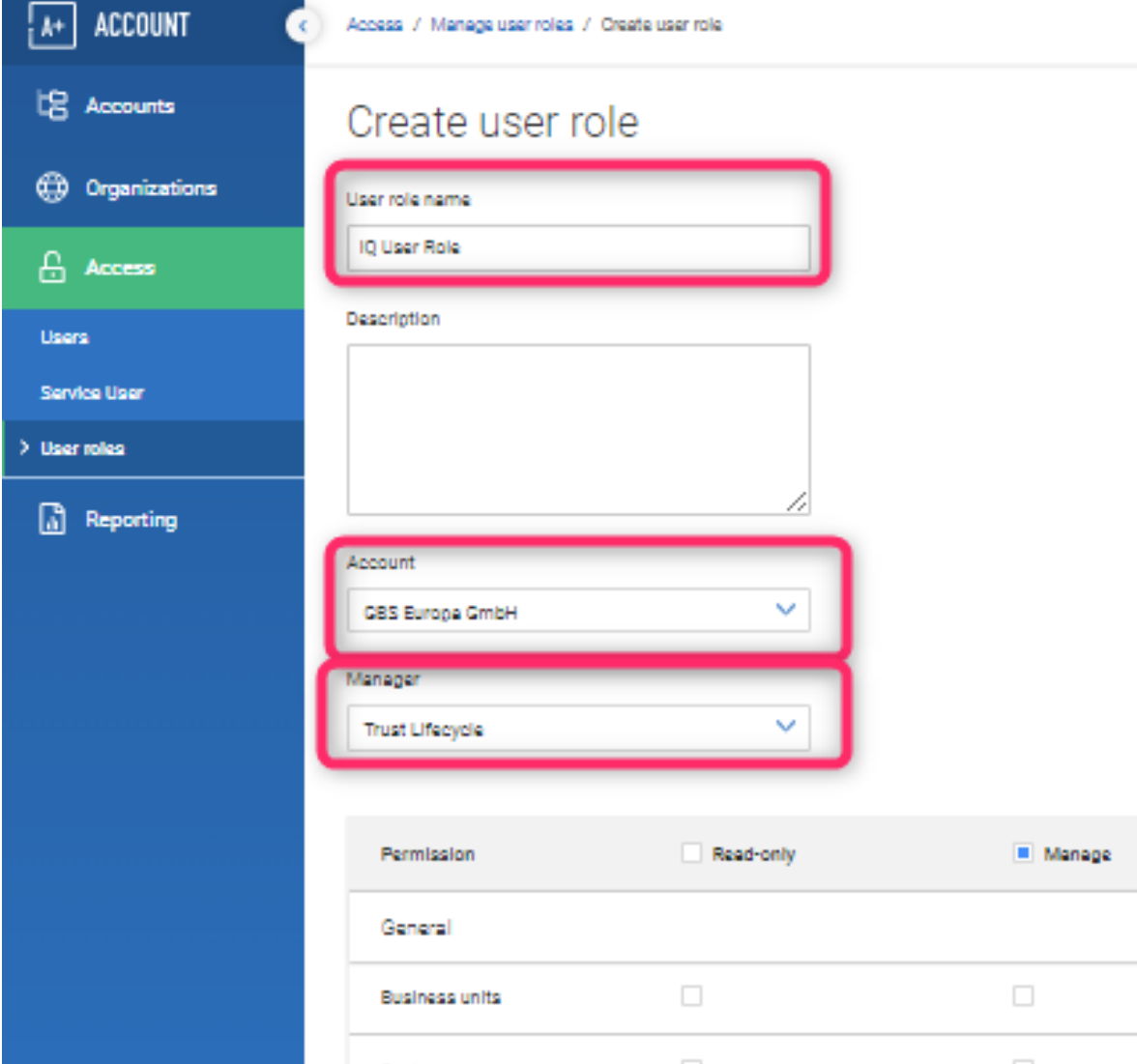


URL: <https://one.nl.digicert.com/account/access/manage-user-roles>

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:



ACCOUNT

Accounts

Organizations

Access

Users

Service User

User roles

Reporting

Access / Manage user roles / Create user role

Create user role

User role name

IQ User Role

Description

Account

GBS Europa GmbH

Manager

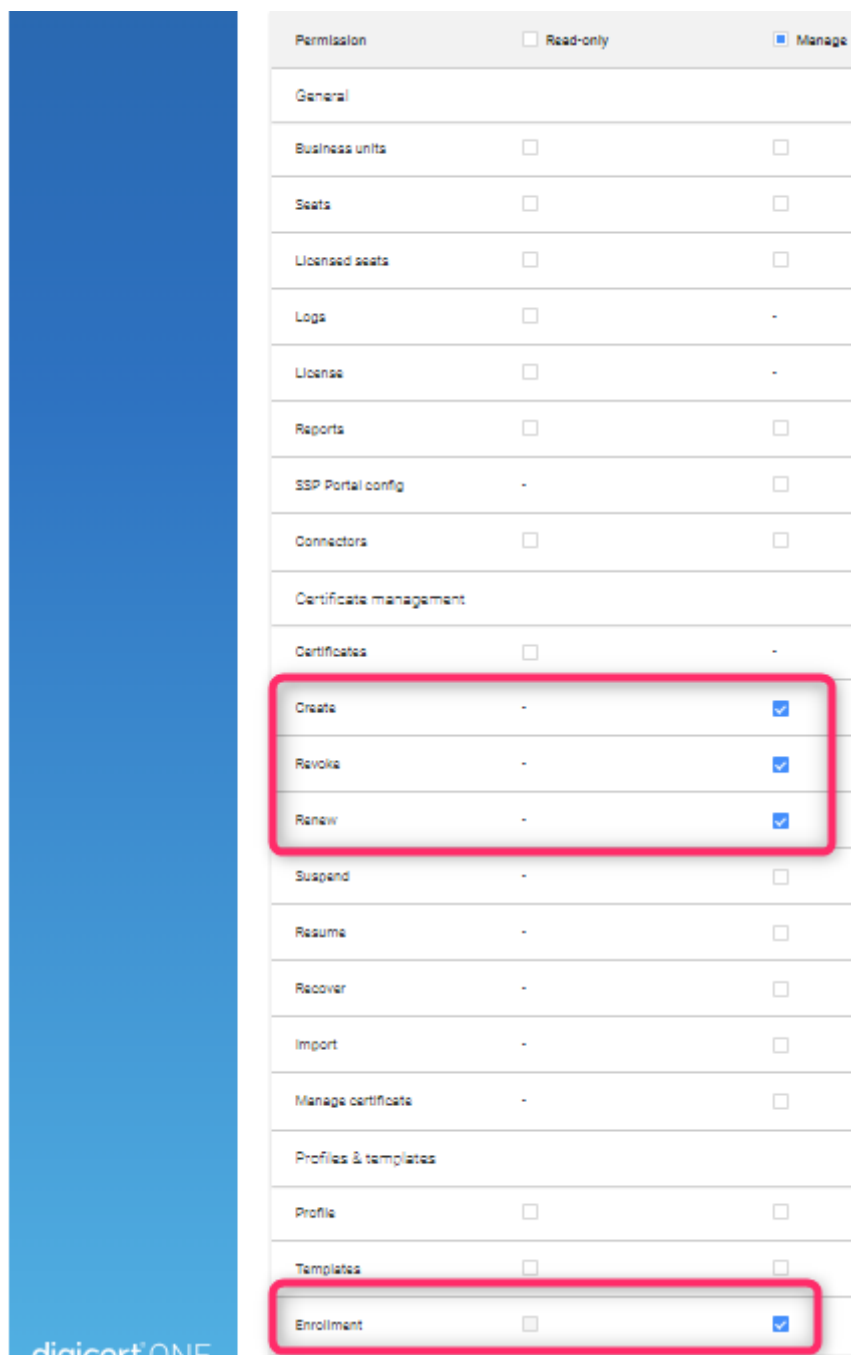
Trust Lifecycle

Permission	<input type="checkbox"/> Read-only	<input checked="" type="checkbox"/> Manage
General		
Business units	<input type="checkbox"/>	<input type="checkbox"/>
Costs	<input type="checkbox"/>	<input type="checkbox"/>

- 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.

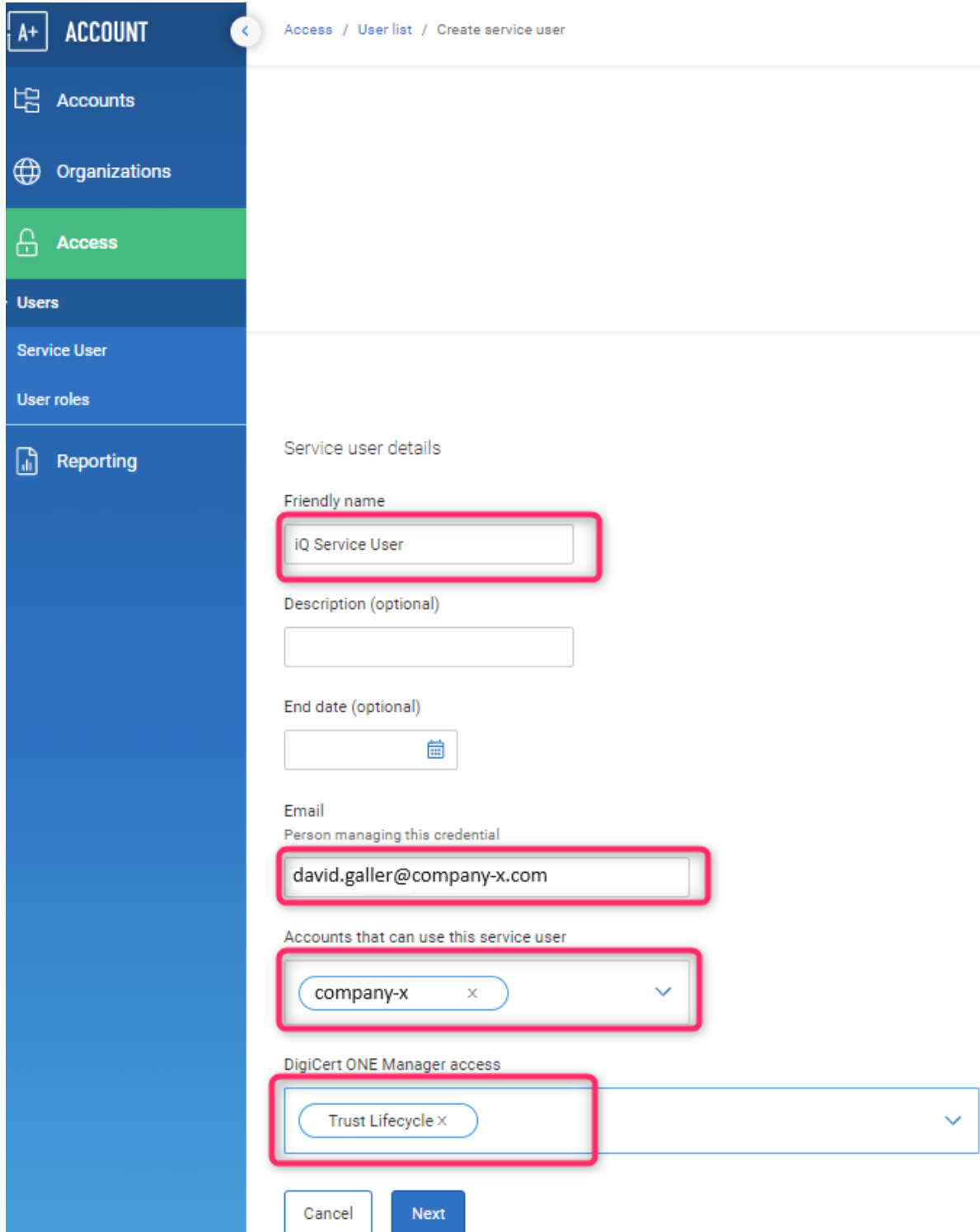
3. In der Tabelle unter dem Feld „Manager“ aktivieren Sie in der Spalte **Manage** folgende **Berechtigungen**:

- Create (notwendig)
- Revoke (empfohlen)
- Renew (empfohlen)
- Enrollment (notwendig)



Permission	<input type="checkbox"/> Read-only	<input checked="" type="checkbox"/> Manage
General		
Business units	<input type="checkbox"/>	<input type="checkbox"/>
Seats	<input type="checkbox"/>	<input type="checkbox"/>
Licensed seats	<input type="checkbox"/>	<input type="checkbox"/>
Logs	<input type="checkbox"/>	-
License	<input type="checkbox"/>	-
Reports	<input type="checkbox"/>	<input type="checkbox"/>
SSP Portal config	-	<input type="checkbox"/>
Connectors	<input type="checkbox"/>	<input type="checkbox"/>
Certificate management		
Certificates	<input type="checkbox"/>	-
Create	-	<input checked="" type="checkbox"/>
Revoke	-	<input checked="" type="checkbox"/>
Renew	-	<input checked="" type="checkbox"/>
Suspend	-	<input type="checkbox"/>
Resume	-	<input type="checkbox"/>
Recover	-	<input type="checkbox"/>
Import	-	<input type="checkbox"/>
Manage certificate	-	<input type="checkbox"/>
Profiles & templates		
Profile	<input type="checkbox"/>	<input type="checkbox"/>
Templates	<input type="checkbox"/>	<input type="checkbox"/>
Enrollment	<input type="checkbox"/>	<input checked="" type="checkbox"/>

4. Erstellen Sie unter [Access > Service User](#) einen Service-Benutzer wie folgt:



ACCOUNT Access / User list / Create service user

Accounts

Organizations

Access

Users

Service User

User roles

Reporting

Service user details

Friendly name

iQ Service User

Description (optional)

End date (optional)

Email

Person managing this credential

david.galler@company-x.com

Accounts that can use this service user

company-x

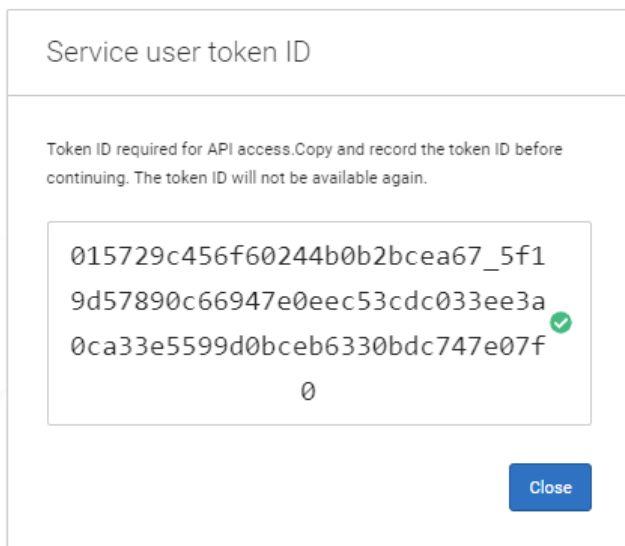
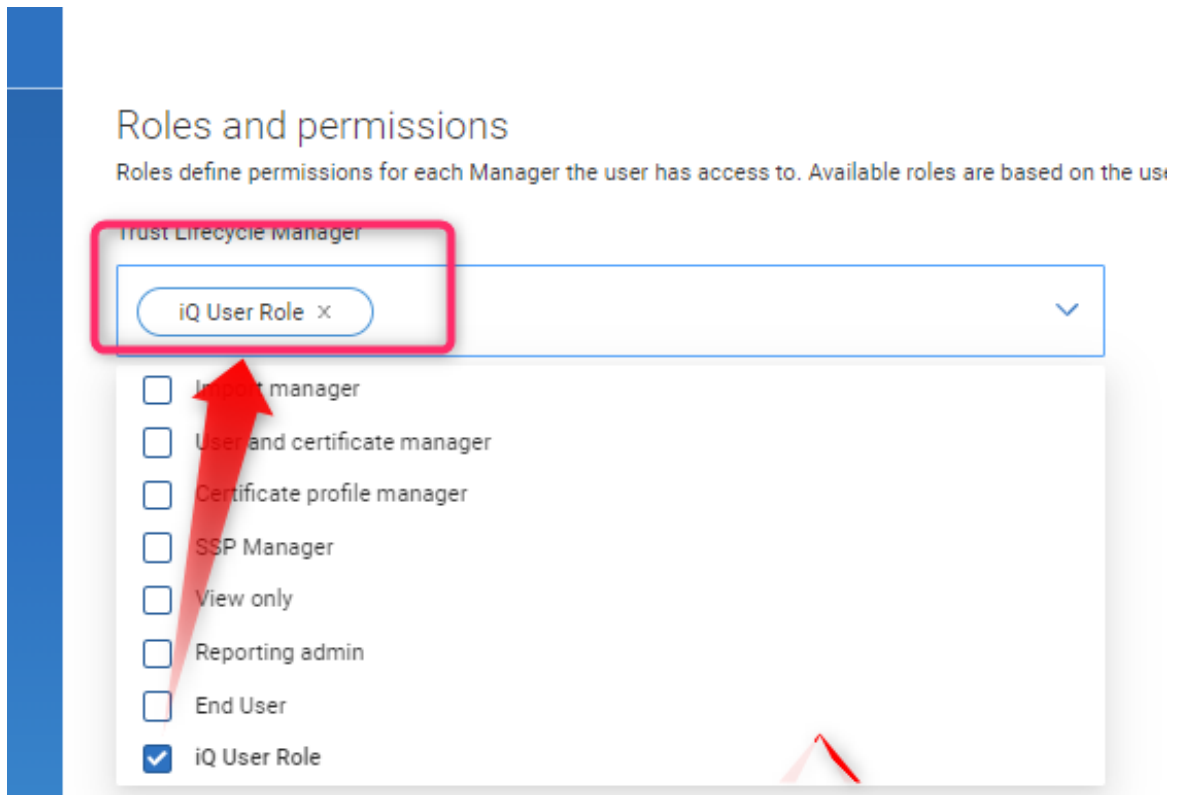
DigiCert ONE Manager access

Trust Lifecycle

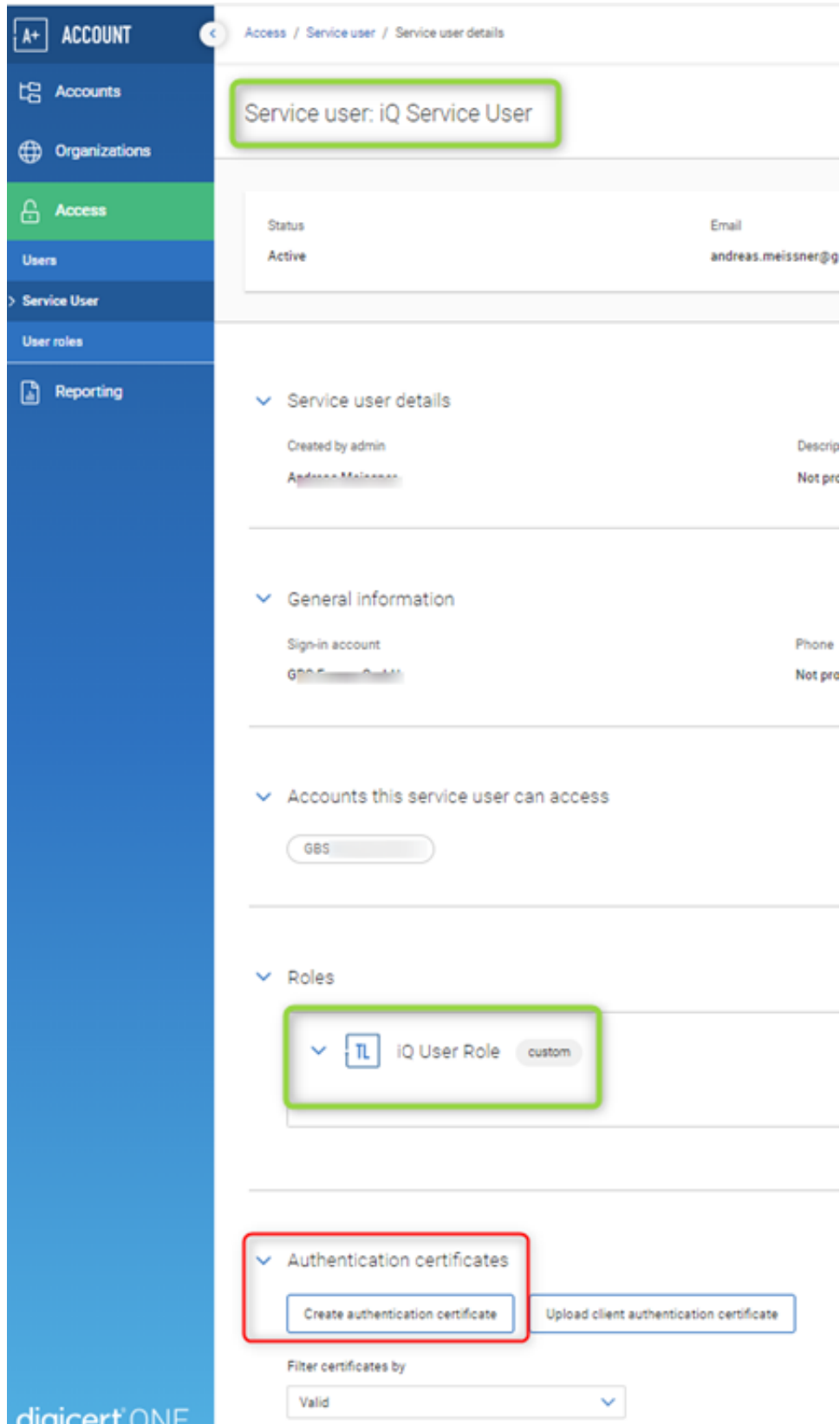
Cancel Next

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.

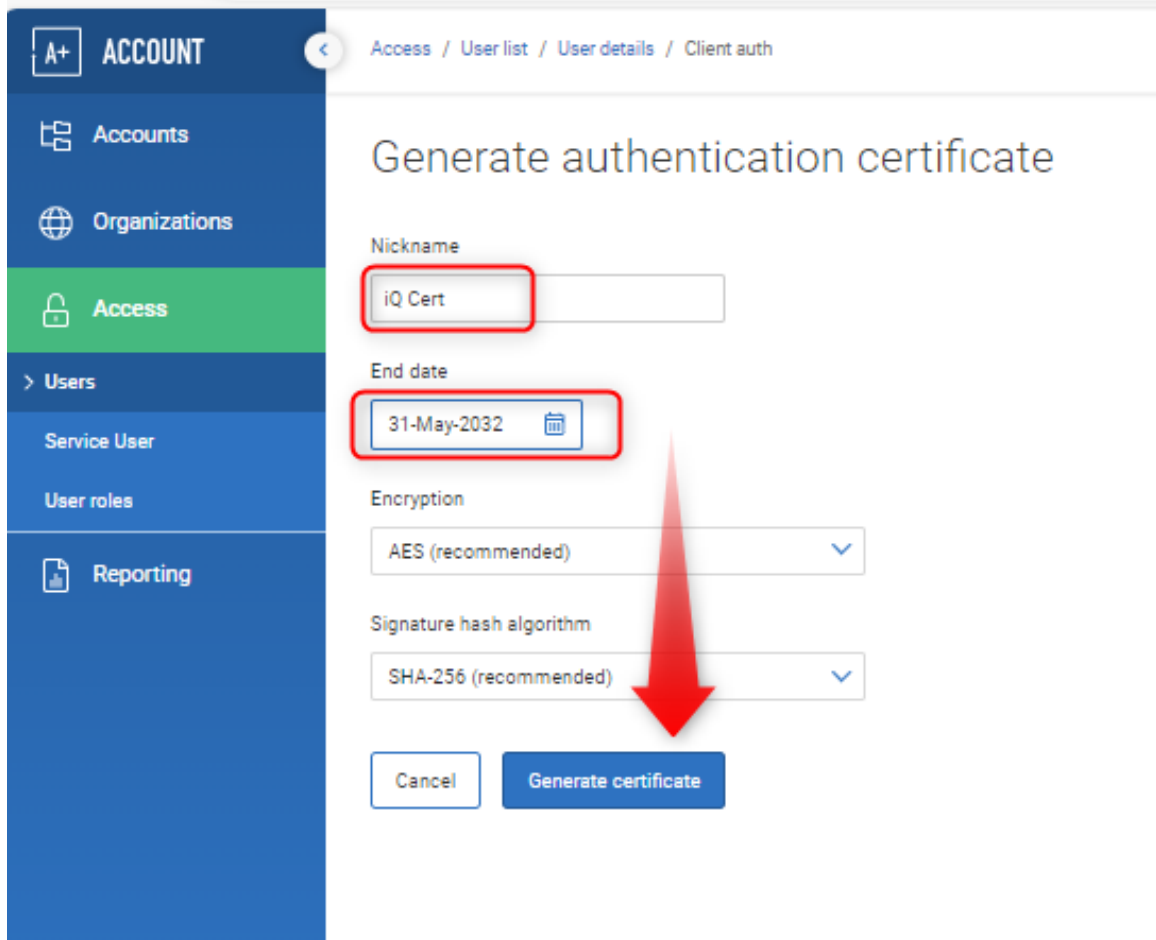


The screenshot displays the 'Service user details' page for 'Service user: iQ Service User'. The page is divided into several sections:

- Service user details:** Status: Active, Email: andreas.meissner@gbs.com
- Service user details:** Created by admin: Andreas Meissner, Description: Not provided
- General information:** Sign-in account: GBS Service User, Phone: Not provided
- Accounts this service user can access:** GBS
- Roles:** iQ User Role (custom)
- Authentication certificates:** Create authentication certificate, Upload client authentication certificate

The 'Create authentication certificate' button is highlighted with a red box, and the 'iQ User Role' is highlighted with a green box.

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



ACCOUNT

Access / User list / User details / Client auth

Generate authentication certificate

Nickname

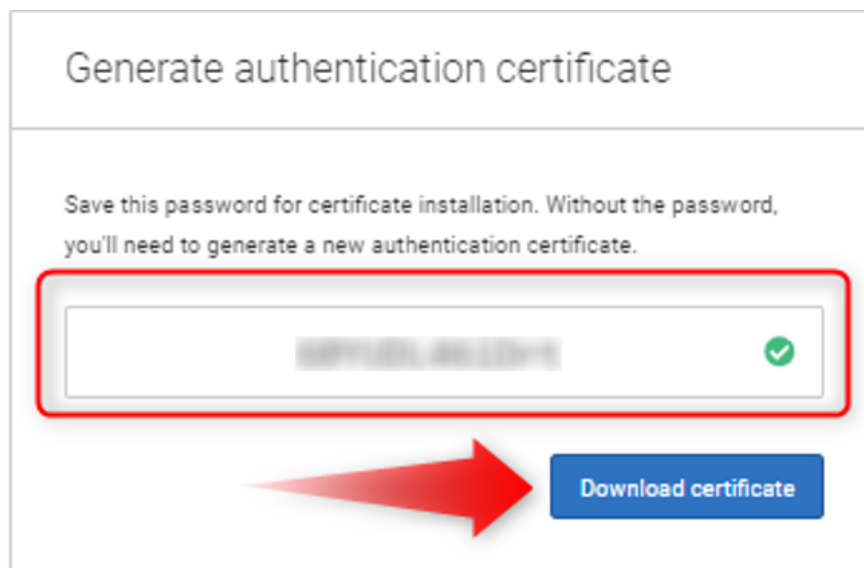
End date

Encryption

Signature hash algorithm

Cancel 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:

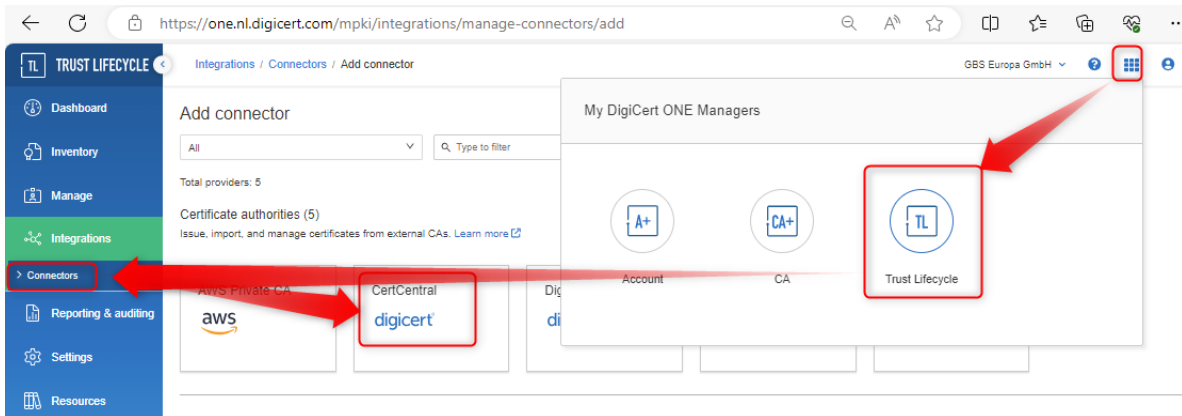


Generate authentication certificate

Save this password for certificate installation. Without the password, you'll need to generate a new authentication certificate.

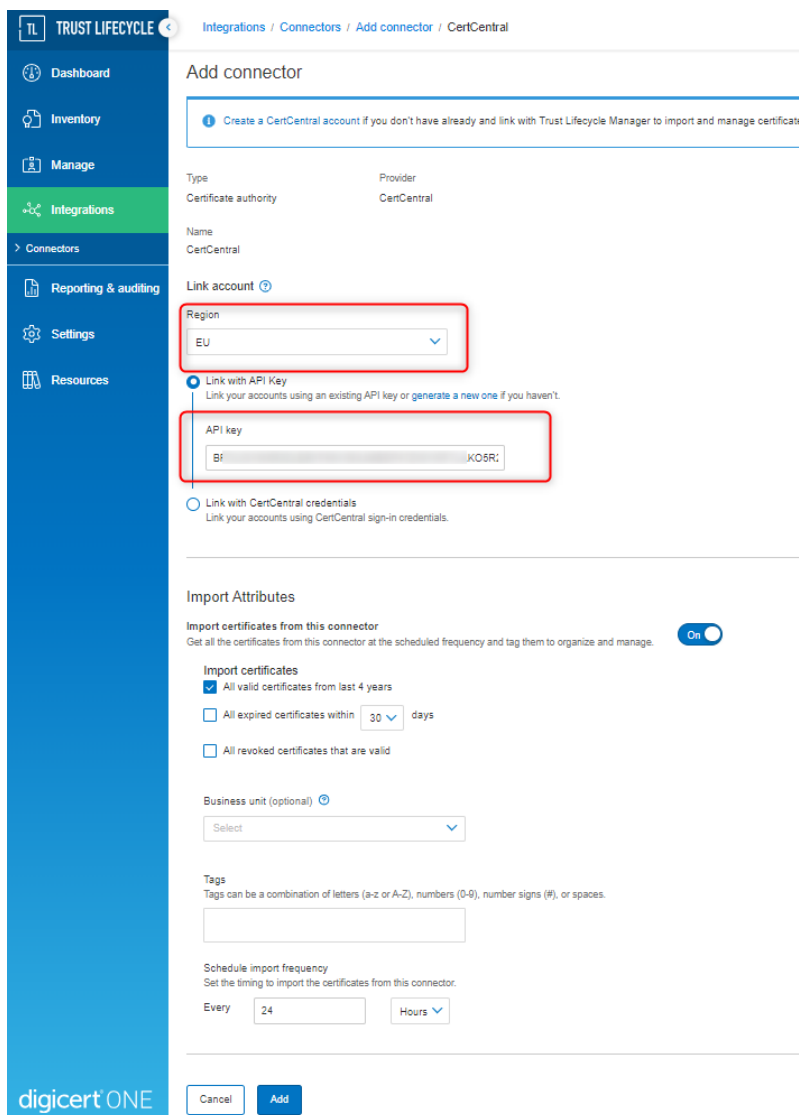
Download certificate

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

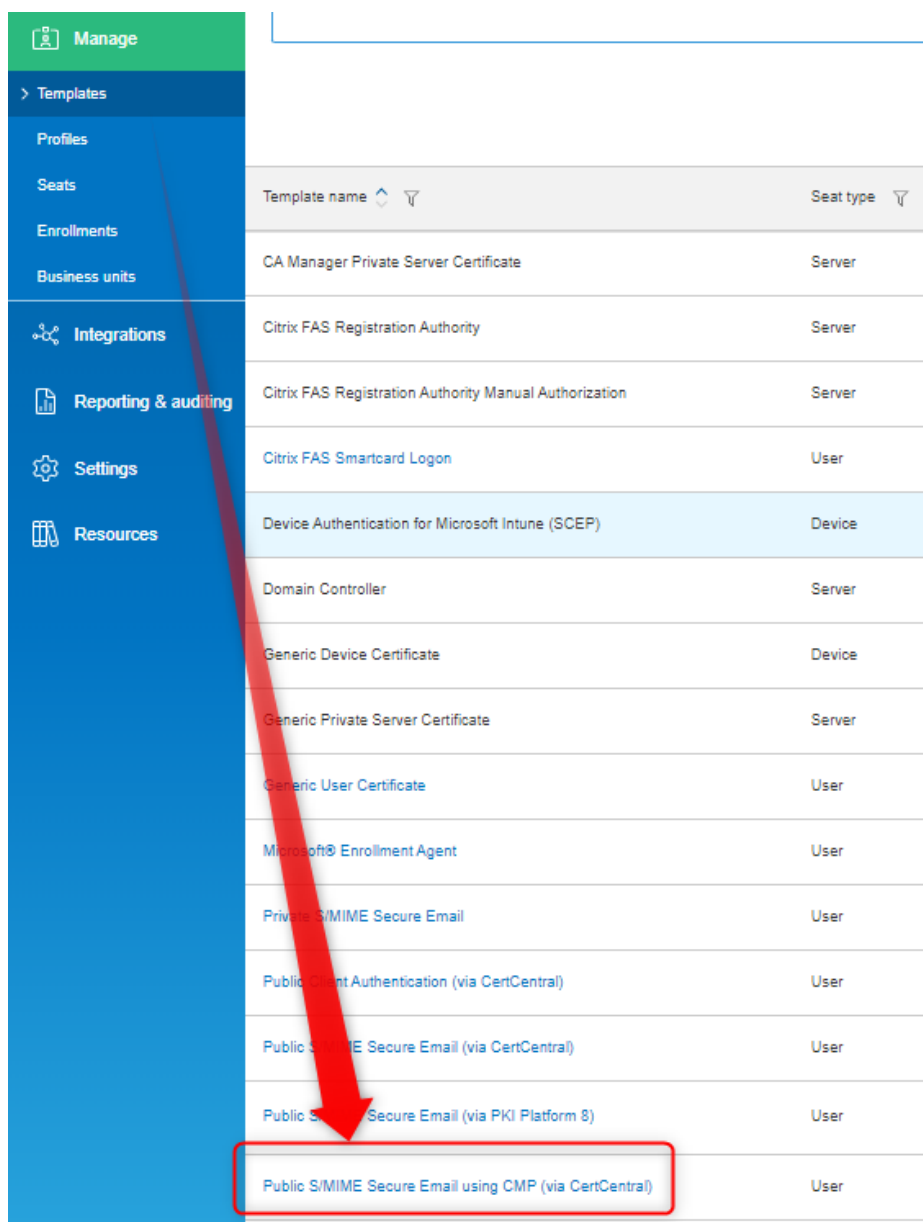


URL: <https://one.nl.digicert.com/mpki/integrations/manage-connectors>

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)**:



Template name	Seat type
CA Manager Private Server Certificate	Server
Citrix FAS Registration Authority	Server
Citrix FAS Registration Authority Manual Authorization	Server
Citrix FAS Smartcard Logon	User
Device Authentication for Microsoft Intune (SCEP)	Device
Domain Controller	Server
Generic Device Certificate	Device
Generic Private Server Certificate	Server
Generic User Certificate	User
Microsoft® Enrollment Agent	User
Private S/MIME Secure Email	User
Public Client Authentication (via CertCentral)	User
Public S/MIME Secure Email (via CertCentral)	User
Public S/MIME Secure Email (via PKI Platform 8)	User
Public S/MIME Secure Email using CMP (via CertCentral)	User

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

Primary options

✓ General information

Base template

Public S/MIME Secure Email using CMP (via CertCentral)

Description

Enables issuance of S/MIME certificates issued by a Public Issuing CA that c


Use Case

Email Signing and Encryption (S/MIME)

Profile name

Business unit

▼

Certificate type 

▼

Issuing CA

▼

✓ Enrollment method

Enrollment method

CMP

✓ Authentication method

Authentication method

TLS Certificate Auth

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

[Manage](#) / [Profiles](#) / Create certificate profile

Signing algorithm

Available algorithms are based on the Issuing CA (ICA) selected for this profile, e.g. if the ICA is an RSA CA, then you

sha256WithRSA 

Key type and sizes

Select the key type and sizes allowed to issue certificates against this profile.


Key type

RSA 

Key size

2048 

✓ Flow options

 Once the profile is saved, these options will be locked and you will not be able to modify them. A new

Duplicate certificate

If enabled, it allows the issuance of duplicate certificates using the exact same Subject DN.

Allow duplicate certificates


Yes

✓ Renewal options

Renewal window

Number of days before or after the certificate expires when you can submit a certificate renewal request. In this request

Note: any remaining validity from the to-be-renewed certificate will be added to the renewed certificate.

30 Days (Recommended) 

✓ Subject DN and SAN fields

Select additional fields 

Add 

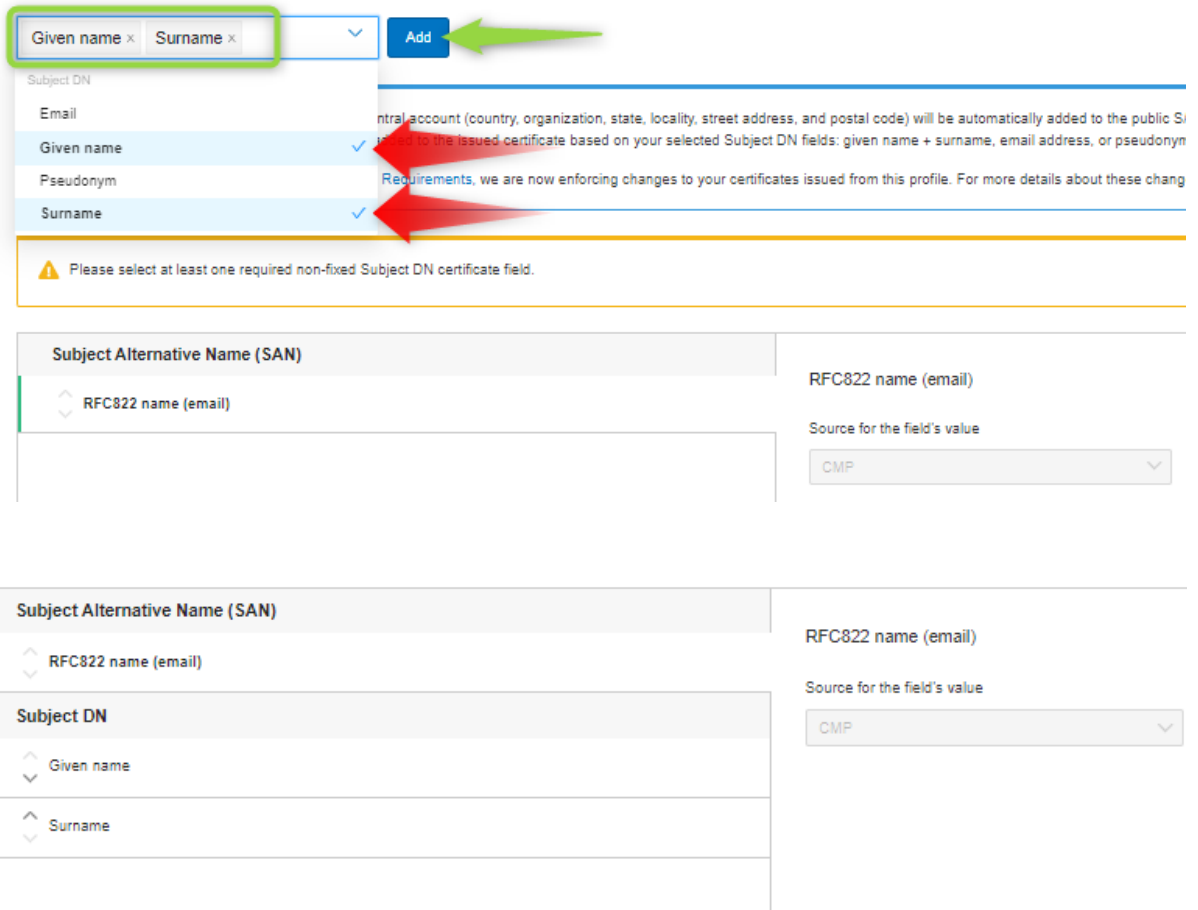
- All organization details included in your CertCentral account (country, organization, state, locality, street)
- The common name (CN) will be automatically added to the issued certificate based on your selected

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

Subject DN and SAN fields



Given name x Surname x Add

Subject DN

- Email
- Given name
- Pseudonym
- Surname

Please select at least one required non-fixed Subject DN certificate field.

Subject Alternative Name (SAN)

- RFC822 name (email)

RFC822 name (email)

Source for the field's value

CMP

Subject Alternative Name (SAN)

- RFC822 name (email)

RFC822 name (email)

Source for the field's value

CMP

Subject DN

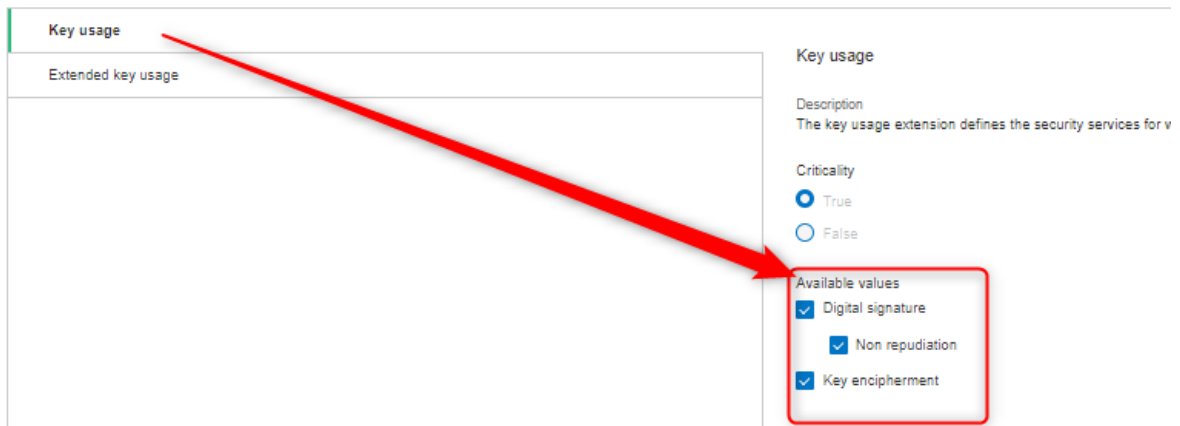
- Given name
- Surname

15. Bei **Standard Extensions** aktivieren Sie folgende Checkboxes:

- Digital signature
- Non repudiation
- Key encipherment

Extensions

▼ Standard extensions

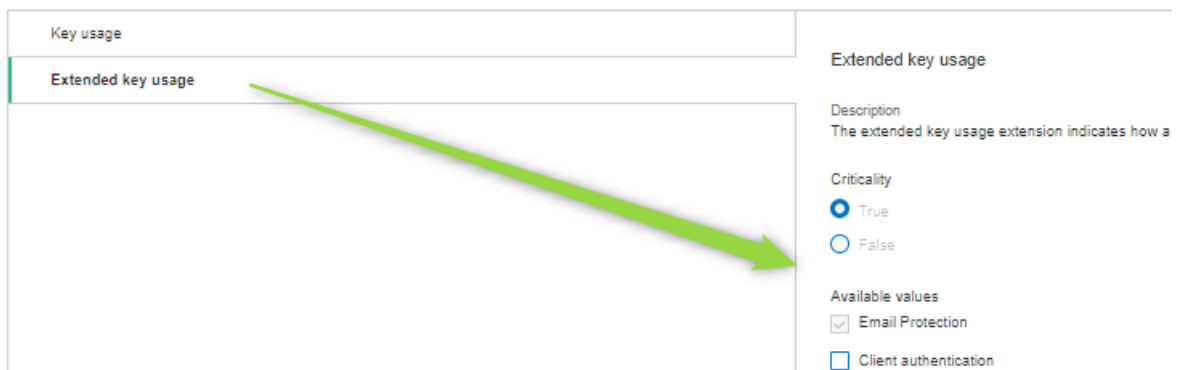


The screenshot shows the configuration for the 'Key usage' extension. On the left, there are two tabs: 'Key usage' (selected) and 'Extended key usage'. On the right, the configuration details for 'Key usage' are shown, including a description, a 'Criticality' section with 'True' selected, and an 'Available values' section with three checked items: 'Digital signature', 'Non repudiation', and 'Key encipherment'. A red arrow points from the 'Key usage' tab to the 'Available values' section.

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

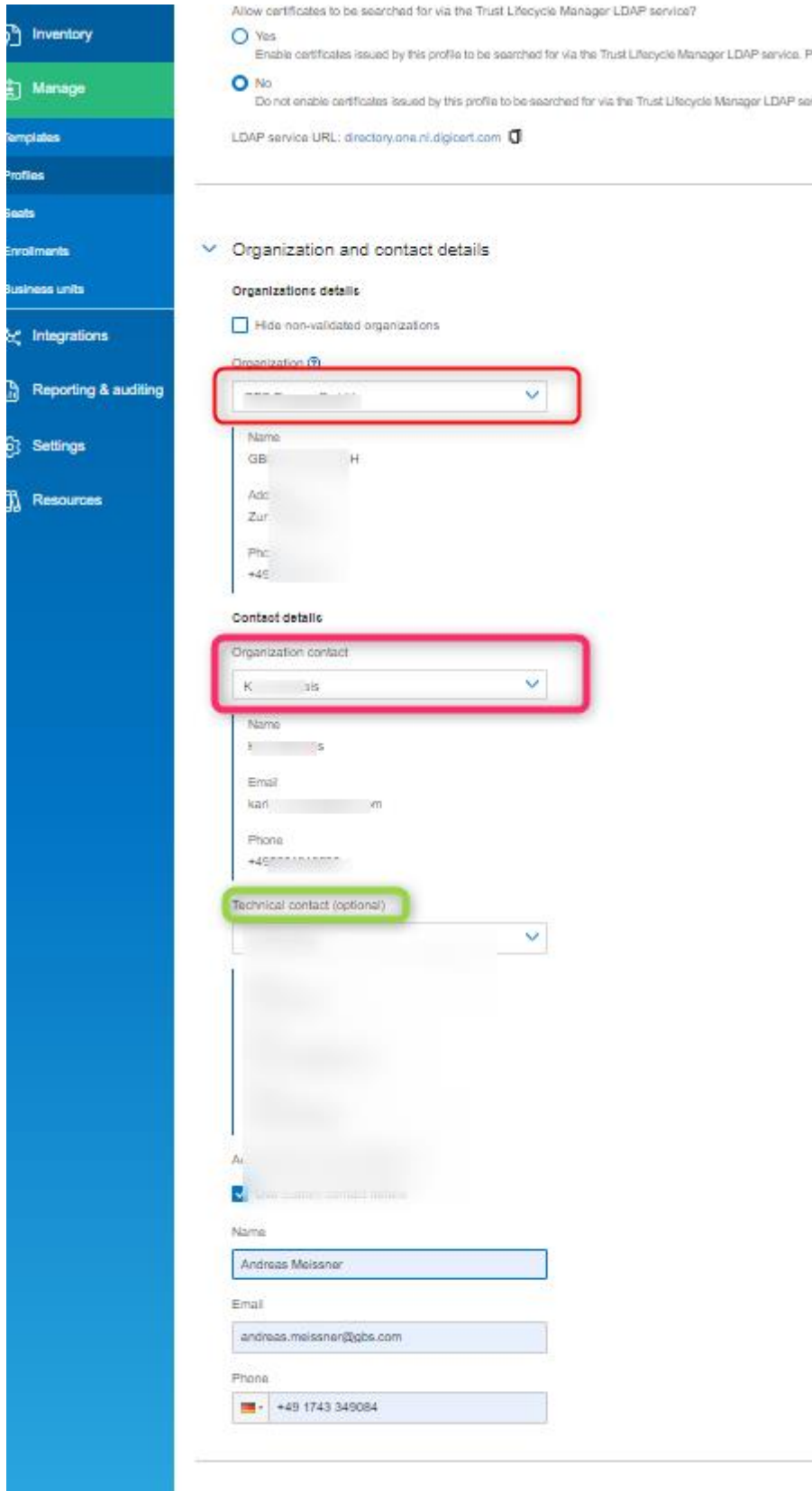
Extensions

▼ Standard extensions



The screenshot shows the configuration for the 'Extended key usage' extension. On the left, there are two tabs: 'Key usage' and 'Extended key usage' (selected). On the right, the configuration details for 'Extended key usage' are shown, including a description, a 'Criticality' section with 'True' selected, and an 'Available values' section with two unchecked items: 'Email Protection' and 'Client authentication'. A green arrow points from the 'Extended key usage' tab to the 'Available values' section.


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



Allow certificates to be searched for via the Trust Lifecycle Manager LDAP service?

Yes
Enable certificates issued by this profile to be searched for via the Trust Lifecycle Manager LDAP service. Pa


No
Do not enable certificates issued by this profile to be searched for via the Trust Lifecycle Manager LDAP serv

LDAP service URL: 

Organization and contact details

Organizations details

Hide non-validated organizations

Organization 

Name
GB: ... H

Ad:
Zur: ...

Ph:
+49 ...

Contact details


Organization contact

Name
K ... s

Email
karl ... m

Phone
+49 ...

Technical contact (optional)

 View sample contact details

Name

Email

Phone

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

Advanced settings

✓ Seat ID Mapping

Select a certificate field to be bound to your Seat ID, used to uniquely identify

Seat ID

SAN: RFC822 name (email) ▼

✓ Cert Central API Key

Authentication method

.....6HJQ

✓ Service User binding

Select the Service User you wish to bind to this profile. The Service User is or

Select Service User

If no Service User is selected, all API KEYS or Certificates bound to the account can be used to manage

Service User: IQ Service ... X ▼

Cancel Back Create

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.

Certificate profile created

CMP URL:
<https://clientauth.one.nl.digicert.com/mpki/q;...>

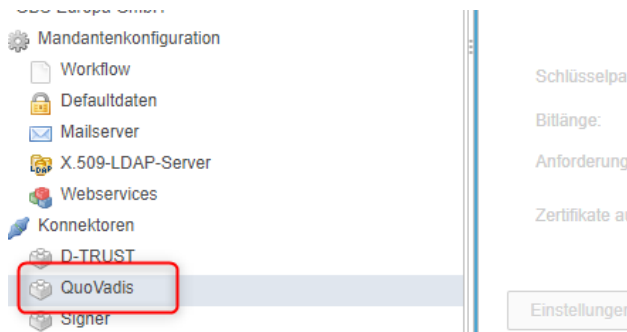
Ok

4.3 iQ.Suite KeyManager

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

- Öffnen Sie die Konfiguration des Konnektors:

DigiCert Connector (KeyManager \geq 9) oder
QuoVadis Connector (KeyManager \leq 8.0.10)



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

QuoVadis

GBS Europa GmbH

Systemkonfiguration verwenden

Daten

Proxyserver verwenden: Ja Nein

Client-Zertifikat: Certificate_pkcs12.p12 ✖ Löschen

Ausgestellt für Common Name	08859015-1877-4f
Ausgestellt von Common Name	adf1d8dc-3c04-4e

Passwort für Client-Zertifikat:

URL: https://clientauth.one.nl.digicert.com/mpki/api/v1/c

Server-Zertifikat:

Ausgestellt für Common Name (CN) Organization (O) Inc."	one.nl.digicert. "DigiCert Inc."
--	--

Bestätigen

Schlüsselpaaralgorithmus: RSA

Bitlänge: 2048 bit

Anforderungen autom. genehmigen: Ja Nein

Zertifikate autom. erneuern: Ja Nein

Einstellungen prüfen

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.

© 2024 GBS Europa GmbH

Die Produktbeschreibungen haben lediglich allgemeinen und beschreibenden Charakter. Sie verstehen sich weder als Zusicherung bestimmter Eigenschaften noch als Gewährleistungs- oder Garantieerklärung. Spezifikationen und Design unserer Produkte können ohne vorherige Bekanntgabe jederzeit geändert werden, insbesondere, um dem technischen Fortschritt Rechnung zu tragen.

Die in diesem Dokument enthaltenen Informationen stellen die behandelten Themen aus der Sicht der GBS Europa GmbH (nachfolgend ‚GBS‘ genannt) zum Zeitpunkt der Veröffentlichung dar. Da GBS auf sich ändernde Marktanforderungen reagieren muss, stellt dies keine Verpflichtung seitens GBS dar und diese kann die Richtigkeit der hier dargelegten Informationen nach dem Zeitpunkt der Veröffentlichung nicht garantieren. Dieses Dokument dient nur zu Informationszwecken.

GBS schließt für dieses Dokument jede Gewährleistung aus, sei sie ausdrücklich oder konkludent. Dies umfasst auch Qualität, Ausführung, Handelsüblichkeit oder Eignung für einen bestimmten Zweck.

Alle in diesem Dokument aufgeführten Produkt- oder Firmennamen können geschützte Marken ihrer jeweiligen Inhaber sein.

Website: www.gbs.com
E-Mail-Adresse: info@de.gbs.com
Standorte: <https://gbs.com/contact-us>

