FAQ

Frequently Asked Questions

Allgemein

- Was ist TCS?
- Was ist ein TCS-Admin?
- Was ist DCV?

TCS Zusatzvereinbarung

- Informationen zu Beilage 1 (Nachweis der Rechtspersönlichkeit)
- Informationen zu Beilage 2 (Details zur Teilnehmerorganisation)
- Informationen zu Beilage 3 (Autorisierte Vertreter des Teilnehmers)

Admins im SCM (Sectigo Certificate Manager)

RAOs

- Anlegen der initialen Admins
- Anlegen weiterer Admins

DRAOs

- Anlegen von 'Department Admins'

Management von Domains

- Anlegen von Domains (*Add*)
- Delegieren von Domains (*Delegate*)
- Bestätigen von Domains (*Approve*)
- Validieren von Domains (*DCV*)
- Re-Validierung von Domains (DCV)
- Löschen von Domains (Delete)

TLS/SSL Zertifikate

- Zertifikatsprofile
- Erstellen eines CSR (Certificate Signing Request)
- Beantragung von TLS-Zertifikaten für Nutzerinnen, die nicht *RAOs sind
- EV (Extended Validation) Zertifikate
- Empfang und Verwendung der Zertifikate von Sectigo

S/MIME (Email bzw. Client) Zertifikate

- Zertifikatstypen
- Self Enrollment
- SAML Self Service Portal

Code Signing Zertifikate

Grid bzw. IGTF SSL Zertifikate

- Secondary Organization Name

API Verwendung

- 'WS API use only' Verwendung
- Was ist der 'customerUri'
- Zertifikate per API beantragen
- einfaches curl Beispiel

Allgemein

Was ist TCS?

TCS steht für Trusted Certificate Service.

GEANT, der Verband europäischer Wissenschaftsnetze, hat einen Rahmenvertrag über die Vergabe und Verwaltung von X.509 Zertifikaten mit der Firma Sectigo als CA (Certificate Authority) abgeschlossen und stellt dieses Service als Trusted Certificate Service (TCS) allen teilnehmenden Wissenschaftsnetzen zur Verfügung.

ACOnet ist diesem Vertrag ebenfalls beigetreten und stellt Zertifikate für ACOnet Teilnehmer unentgeltlich und in unlimitierter Anzahl zur Verfügung. ACOnet Teilnehmerorganisationen können, auf Basis der Zusatzvereinbarung zur ACOnet-Teilnahmevereinbarungbetreffend die Nutzung des Trusted Certificate Service, TCS Zertifikate beantragen. Die Zusatzvereinbarung muss von einer für die teilnehmende Institution zeichnungsberechtigten Person im Original unterfertigt und mit den geforderten Beilagen per Post an ACOnet gesendet werden, siehe auch http://tcs.aco.net/.

Der Vertrag mit Sectigo gilt ab dem 01.05.2020, initial für 2 Jahre und kann dann jährlich, bis zu einer Gesamtlaufzeit von 10 Jahren, verlängert werden.

Was ist ein TCS-Admin?

Jede ACOnet Teilnehmerorganisation die das Zertifikatsservice nutzen will, muss zumindest eine/n, sollte aber mehr als eine/n, TCS Administrator/in angeben und diese/n in die Zusatzvereinbarung eintragen. Für entsprechend authentifizierte und autorisierte TCS AdministratorInnen haben im Portal die Möglichkeit, beantragte Zertifikate ihrer eigenen Organisation zu sehen, zu bestätigen, abzulehnen oder zu widerrufen. Im Portal von Sectigo werden diese Admins als *RAO* (Registration Authority Officer) bezeichnet.

Was ist DCV (Domain Control Validation)?

Bei der Registrierung einer neuen Domain, wird mittels DCV automatisiert überprüft, ob die Person, die die Validierung einer Domain angestossen hat (TCS-Admin), auch "Kontrolle" über den bzw die Domain-Namen hat.

Es gibt 3 Möglichkeiten:

1. Email
2. DNS CNAME
3. HTTP/HTTPS File

1. Email:

Hierzu sendet der DCV Mechanismus ein E-Mail mit einem jeweils eindeutigen Code an einen definierten Satz von Adressen. Dieser Code wird durch den /die Empfänger dieser DCV Mails zur Validierung auf einer Webseite validiert (Email Challenge-Response Verfahren).
Erst nach dieser Validierung (bei Multi-Domain-Zertifikaten je Domain) wird das Zertifikat ausgestellt.

Folgende 5 generischen Email-Adressen stehen immer zur Verfügung:

- hostmaster@domain_name
- postmaster@domain_name
- webmaster@domain_name
- administrator@domain_name
- admin@domain_name

Zusätzlich kann das DCV Mail auch an alle Email-Adressen, die im 'whois-record' der Domain als tech- oder admin-contact gelistet sind, gesandt werden. Viele Domain Registrierungsstellen erlauben die Abfrage von Email-Adressen via whois allerdings nicht mehr. Der Grund dafür sind die strengen Richtlinien der DSGVO, wodurch personenbezogene Daten, wie Email-Adressen, nicht mehr abfragbar sind.
Die Email-Adressen (generisch oder via whois) sind nicht nur für den Domainnamen des Zertifikats verfügbar, sondern auch für Domains "darüber": z.B. um ein Zertifikat für www.bla.muh.ac.at zu erhalten, stehen folgende Mail-Domains für die DCV Bestätigung zur Verfügung:

- @www.bla.muh.ac.at
- @bla.muh.ac.at
- @muh.ac.at

2. DNS CNAME

Es wird ein hash erzeugt, der als DNS CNAME record für die Domain eingetragen werden muss und überprüft wird.

3. HTTP/HTTPS File

Es wird ein .txt File erzeugt, das im 'root' des Webservers abrufbar sein muss.

⚠️ **VORSICHT**: Diese Methode ist für die Validierung von Wildcard-Domains nicht mehr geeignet, siehe https://sectigo.com/resource-library/modifications-to-available-file-based-methods-of-domain-control-validation ⚠️

TCS Zusatzvereinbarung

Die TCS-Zusatzvereinbarung ist in der aktuell gültigen Version unter https://www.aco.net/tcs.html zu finden.

Informationen zu Beilage 1 (Nachweis der Rechtspersönlichkeit)

- Bei Körperschaften öffentlichen Rechts und ähnlichen, auf Grund von Gesetzen (z.B. FOG) existierenden Organisationen, hier bitte einen Verweis auf das entsprechende Gesetz, wenn geht paragraphengenau, angeben.

- Für Kapitalgesellschaften ersuchen wir um einen aktuellen Firmenbuchauszug, aus dem die Zeichnungsberechtigung des Unterfertigers der Zusatzvereinbarung für den Teilnehmer hervorgeht. Bei Abweichungen der Zeichnungsberechtigungen vom Firmenbuch benötigen wir auch eine Kopie einer notariell beglaubigten Vollmacht, aus der die Zeichnungsberechtigung für den Abschluß eines derartigen Rechtsgeschäftes eindeutig hervorgeht.
- Bei Vereinen bitte um eine ZVR-Zahl.

Informationen zu Beilage 2 (Details zur Teilnehmerorganisation)

Die Beilage 2 dient zum Anlegen einer Organisation bei Sectigo. Folgende Dinge sind dabei zu beachten:

- Die Informationen (Name, Adressdaten) müssen jenen Informationen entsprechen, die sich auch in den in Beilage 1 beigebrachten Dokumenten wiederfinden. Diese sollten auch als QIS (Qualified Information Source) dem Validierungsantrag der Organisation beigefügt werden.
  ⚠️ Da das Organisations Feld im Subject eines X509 Zertifikats maximal 64 Zeichen lang sein darf , darf auch die Bezeichnung der Organisation in Beilage 2 nicht länger als 64 Zeichen sein, wobei Sonderzeichen, z.B. Umlaute, als 2 Zeichen zu zählen sind. ⚠️
- **Auswahlboxen 'key recovery':** Sectigo bietet die Möglichkeit, den privaten Schlüssel von über das Sectigo Portal (SCM, Sectigo Certificate Manager) beantragten persönlichen Zertifikaten, verschlüsselt zu speichern (siehe Details zum Erstellen des Schlüssel). Diese privaten Schlüssel werden in einem "elektronischen Safe" hinterlegt und können im Notfall, ie. wenn damit verschlüsselte Daten gebraucht werden, der/die Mitarbeiterin oder der private Schlüssel aber nicht mehr greifbar sind, ausgelesen werden. Sobald dies geschieht, wird das jeweilige persönliche Zertifikat allerdings sofort widerrufen und kann nicht mehr zur Verschlüsselung und/oder Signierung verwendet werden.
  Ob ein solcher "elektronischer Safe" für eine Organisation erstellt wird oder nicht muss allerdings beim Anlegen der Organisation festgelegt werden und kann nachträglich nicht mehr verändert werden.
  Weiters muss vor Beantragung des ersten persönlichen Zertifikats der Schlüssel für diesen Safe erstellt werden (siehe Details zum Erstellen des Schlüssel). Wenn dieser Schlüssel verloren geht, gibt es keine Möglichkeit auf den Safe und damit auf die privaten Schlüssel zuzugreifen.

Informationen zu Beilage 3 (Autorisierte Vertreter des Teilnehmers)

siehe auch Was ist ein TCS-Admin?

In der Beilage 3 sind uns die Organisations Administratoren, RAOs (Registration Authority Officer) in Sectigo Nomenklatur, zu nennen. Diese Adminstratoren haben unter anderem folgende Berechtigungen:

- Validierung bzw. Revalidierung der Organisation anstossen
- Domains anlegen und DCV (siehe DCV) anstossen
- Departments und zugehörige Administratoren anlegen
- Domains an Departments delegieren
- Zertifikatsanträge genehmigen

Admins im SCM (Sectigo Certificate Manager)

RAOs

Anlegen der initialen Admins

Die initialen Admins werden auf Grund der Informationen in der Beilage 3 der TCS Zusatzvereinbarung angelegt. Siehe auch Informationen zu Beilage 3.

Anlegen weiterer Admins

Für das Anlegen bzw. Berechtigen weiterer RAOs gibt es 3 Möglichkeiten:

1. Sie schicken uns eine weitere, ausgefüllte und unterschrieben Beilage 3 der TCS-Zusatzvereinbarung (https://www.aco.net/tcs.html) mit den neuen RAOs. Hier genügt eine elektronische Version per Mail an tcs@aco.net.
2. Ein bestehender TCS Admin (RAO) schickt uns per Mail die notwendigen Informationen (wie in Beilage 3) zum Anlegen eines weiteren RAOs per Mail an tcs@aco.net.
3. Ein bestehender 'Department Admin' (DRAO, siehe Anlegen von 'Department Admins') kann vom ACOnet Team die Berechtigungen konfiguriert bekommen, um als RAO zu funktionieren. Dazu genügt ebenfalls ein Mail eines bestehenden TCS Admin (RAO) an tcs@aco.net.

DRAOs

Anlegen von 'Department Admins'

DRAOs, Admins auf Department Ebene, können RAOs selbst anlegen und berechtigen.

Management von Domains

Anlegen von Domains

Bevor sie Zertifikate beantragen können, müssen sie die entsprechenden Domains angelegt und validiert haben.

Wenn sie Domains anlegen müssen sie immer die eigentliche Domain und die dazu gehörige 'Wildcard Domain' anlegen, z.B. *example.at* und **.example.at*
Diese 'Eigenheit' bei Sectigo ist notwendig, um beliebige Subdomains bzw. Hostnamen in Zertifikaten verwenden zu können (z.B. *foo.bar.example.at*, aber auch *www.example.at*).
Es kann sein, dass die Validierung der 'Wildcard Domain' länger braucht, sobald jedoch die Hauptdomain erfolgreich validiert ist, können sofort Zertifikate beantragt werden, auch für Subdomains bzw. beliebige Hostnamen.

Wählen sie im SCM *'linkes Menü' Domains* '+'. Sie können an dieser Stelle auch gleich die Delegierung der Domain erledigen.

Delegieren von Domains

Wählen sie im SCM *'linkes Menü'* *Domains*, Domain wählen *Delegate Button* klicken und Organisation bzw. Department für den jeweiligen Zertifikatstyp anhaken.

Bestätigen von Domains

Vor der Validierung der Domain, muss die Delegierung bestätigt werden

Die Bestätigung der Delegierung von Domains kann nur von einem MRAO aus dem ACOnet Team durchgeführt werden. Das ACOnet Team wird automatisch notifiziert, sollte es zu Verzögerungen kommen, bitte ein Mail an tcs@aco.net schicken.

Validieren von Domains

> **CAA record**
>
> Überprüfen sie, ob ein CAA record für die entsprechende Domain existiert, der die Ausstellung von Zertifikaten durch Sectigo für diese Domain verhindert. Falls dem so ist, kann Sectigo keine Zertifikate für diese Domain ausstellen.
>
> Einfacher check: `dig caa <domain>` oder diverse online tools
>
> siehe auch Sectigo CAA info

Starten der Validierung:

Wählen sie im SCM *'linkes Menü'* *Domains*, Domain wählen, die sie validieren wollen *Validate* Button Methode wählen (zu den Methoden, siehe Was ist DCV?)

Re-Validierung von Domains

Ab 90 Tagen vor dem Ablauf der Validierung kann die DCV erneut angestossen werden. Eine automatische Re-Validierung von Domains durch Sectigo passiert nicht, diese muss also manuell (oder per API) angestossen werden.

Bis wann die Validierung gültig ist, finden sie im SCM *'linkes Menü'* *Domains*, Domain wählen, im DCV Bereich ('*Expires*')

Löschen von Domains

Domains können nur selbst gelöscht werden, bevor sie bestätigt sind (siehe Bestätigen von Domains).
Sobald die Bestätigung erfolgt ist, können Domains **nicht** mehr selbst gelöscht werden. Falls eine Domain gelöscht werden soll, kann ein dem ACOnet bekannter RAO ('organizational admin') den bzw. die Namen der zu löschenden Domains an tcs@aco.net senden und ein MRAO aus dem ACOnet Team wird die Domain(s) löschen.

TLS/SSL Zertifikate

Zertifikatsprofile

GÉANT OV Multi-Domain
wenn SANs gebraucht werden. Wir empfehlen allerdings, auch ohne SANs dieses Profil zu nehmen, Erklärung siehe *GÉANT OV SSL*

GÉANT OV SSL
wenn nur CN, kein(e) SAN(s) gebraucht werden - allerdings wird bei diesem Profil automatisch ein SAN in der Form www.<CN> hinzugefügt. Wenn man das nicht will, auch für diesen Fall *GÉANT OV Multi-Domain* verwenden

GÉANT Wildcard SSL
wenn sie ein Zertifikat für *.domain brauchen

GÉANT Unified Communications Certificate
speziell für Microsoft Exchange und/oder Microsoft Office Communication Server (OCS) Umgebungen

GÉANT EV Multi-Domain
können bzw. sollten nicht direkt beantragt werden, siehe EV (Extended Validation) Zertifikate

GÉANT EV SSL
können bzw. sollten nicht direkt beantragt werden, siehe EV (Extended Validation) Zertifikate

optionale Profile

für die Aktivierung/Freischaltung dieser Profile kontaktieren sie bitte das ACOnet Team unter tcs@aco.net

GÉANT IGTF Multi-Domain
spezielles Zertifikat zur Verwendung im "Grid Computing Umfeld", siehe auch Secondary Organization Name

Erstellen eines CSR (Certificate Signing Request)

Um Probleme bei der Beantragung von Zertifikaten zu vermeiden, empfielt es sich, nur den CN bei der Erstellung des CSR anzugeben. Sollten nämlich die anderen Felder angegeben sein, aber nicht mit den validierten Daten bei Sectigo übereinstimmen, kann es zu Fehlern und der Ablehnung des Zertifikatsantrags führen.

Beispiele für das Erstellen des CSR

Beantragung von TLS-Zertifikaten für Nutzerinnen, die nicht *RAOs sind

Sie können Personen, die keine Admins im SCM sind, erlauben, Zertifikate anzufordern.
Gehen Sie dazu zu *Enrollment Enrollment Forms*, wählen Sie *SSL Web Form* aus und klicken sie *Accounts*. Klicken sie *Add* oder wählen sie einen bestehenden Account und klicken *Edit.*

Vergeben sie einen Namen und wählen die Organisation und eventuell das Department aus. Wählen sie die 'Certificate Profiles' (im Normalfall die OV Profile und eventuell das Wildcard Profil), die verfügbar sein sollen und geben Sie einen selbst gewählten *Access Code* ein.
Unter https://cert-manager.com/customer/ACOnet/ssl können sie dann im ersten Punkt '*Certificate Enrollment*' mittels des erstellten 'Access Code' und Angabe einer Mail-Adresse das Zertifikat beantragen. Der Domain-Teil der angegebenen E-Mail Adresse muss dabei einer validierten Domain in der entsprechenden Organisation entsprechen, ansonsten wird der Zugriff verweigert.

Falls sie Teilnehmer an der ACOnet Identity Federation sind und einen dementsprechenden IdP betreiben, können Sie auch *Self Enrollment via SAML* aktivieren.
Gehen Sie dazu zu *Enrollment Enrollment Formss* und klicken *Add* oder wählen eine bestehende *SSL SAML self-enrollment form* aus und klicken *Edit*. Vergeben sie einen Namen und wählen die Organisation und eventuell das Department aus. Wählen sie die 'Certificate Profiles' (im Normalfall die OV Profile und eventuell das Wildcard Profil), die verfügbar sein sollen und klicken *Generate*.

Den URL unter dem Feld *URI Extension* an die Benutzer aushändigen. Nutzerinnen müssen sich dann bei ihrem IdP authentifizieren, bevor sie zu der gleichen '*Certificate Enrollment*' Seite wie oben kommen. Der Domain-Teil der E-Mail-Adresse, die von ihrem IdP mitgeschickt wird, muss dabei einer validierten Domain in der entsprechenden Organisation entsprechen, ansonsten wird der Zugriff verweigert.

> **No Auto Approve**
>
> Aktivieren Sie nicht die Option *Automatically Approve Self Enrollment Requests*, da sie Zertifikatsanfragen, die über diesen Weg eintreffen, manuell genehmigen werden wollen.

EV (Extended Validation) Zertifikate

EV Zertifikate haben auf Grund der Entscheidung der Browser Hersteller (Google Chrome Announcement, Mozilla Firefox Announcement) keinen signifikanten Vorteil im Vergleich zu OV (Organization Validated) Zertifikaten mehr. Sollten sie trotzdem ein Extended Validation Zertifikat beziehen wollen, muss vor der Beantragung und Ausstellung eines EV Zertifikats, ein '*EV anchor certificate*' beantragt werden.

Den Ablauf zur Beantragung eines 'EV Anchor Certificate' finden sie im Sectigo EV anchor and SCM Manual

Empfang und Verwendung der Zertifikate von Sectigo

> **Anmerkung**
>
> Ziel ist natürlich, dass Sectigo die `pem` Dateien in einer Form zur Verfügung stellt, in der sie direkt verwendet werden können. Bis es soweit ist, helfen eventuell folgende Tipps.

Prinzipiell brauchen sie bei Webservern das *Leaf-Zertifikat* und **nur** das *GEANT Intermediate Zertifikat* als Chain-Zertifikat zu verwenden - das Root-Zertifikat finden die Web-Browser und andere clients selbst (in ihrem '*truststore*').

Je nachdem welche 'Version' des `pem` Files sie von den angebotenen Links bei Sectigo herunterladen, sind unterschiedliche Zertifikate enthalten. Was allen Arten gleich ist, ist die falsche Reihenfolge der Zertifikate, ie. *Leaf Zertifikat* als unterstes, darüber eventuell ein oder mehrere *Intermediate Zertifikate* und darüber, als oberstes, das *Root Zertifikat*.
Fast alle devices brauchen die Zertifikate allerdings in umgekehrter Reihenfolge, ie. *Leaf Zertifikat* zu oberst, darunter das *Intermediate Zertifikat*.

Eine Möglichkeit ist das manuelle 'umsortieren' der notwendigen und gleichzeitige 'entsorgen' der unnötigen Zertifikate.
Eine andere Möglichkeit, ist die folgende:
Alle von Sectigo (und anderen CAs) ausgestellten Zertifikate werden in 'Certificate Transparency Logs' gespeichert. Diese Logs können abgefragt werden und auch Zertifikate können an dieser Stelle heruntergeladen werden. Sectigo betreibt eine Webseite zur Abfrage dieser *Transparency Logs* https://crt.sh/
Suchen sie ihr Zertifikat (CN) unter https://crt.sh/ - es werden zumindest 2 Zertifikate gefunden. Hier ist wichtig, dass bei 'Issuer Name' *C=NL, O=GEANT Vereniging, CN=GEANT*... steht. Mit Klick auf die ID kommen sie zum eigentlichen Zertifikat, wobei hier wichtig ist, dass bei '*Summary*' '*Leaf certificate*' steht (**nicht** *'Precertificate*').
Das Zertifikat können sie links unten unter '*Download Certificate: PEM*' herunterladen.

Wenn sie dann auf 'Issuer' klicken, kommen sie zur 'CA Id' Ansicht des passenden 'GEANT Inermediate', wo sie mit einem Klick auf die Nummer unter 'crt.sh ID' direkt zum passenden Zertifikat kommen
Auch hier haben sie links unten unter '*Download Certificate: PEM*' die Möglichkeit, das Zertifikat herunterzuladen.

Letztendlich muss im Zertifikatsfile des Webservers oben das '*Leaf certificate*' und darunter das *'Intermediate certificate'* stehen. Den Rest der Chain finden die Browser alleine, diese muss und soll nicht vom Webserver ausgeliefert werden.

S/MIME (Email bzw. Client) Zertifikate

Seit 01.09.2023 sind auch für die Ausstellung und Verwaltung von S/MIME Zertifikaten 'Baseline Requirements' des CA/Browser Forums in Kraft. Diese definieren 4 Zertifikatstypen, von denen 2 für das TCS relevant sind:

- **Sponsor-validated** entspricht "*GÉANT Personal email signing and encryption*" im TCS
- **Organization-validated** entspricht "*GÉANT Organisation email signing and encryption*" im TCS

Folgend sind Details zu den beiden Typen zu finden:

Zertifikatstypen

GÉANT Personal email signing and encryption

In Zertifikaten, die mit diesem Zertifikatsprofil ausgestellt wurden, sind sowohl die Organisation, als auch die Person validiert. Im Subject des Zertifikats findet sich der validierte Name der Person (CN, GIVENNAME und SURNAME), die validierte Organisation (O) und die Email-Adresse (E), deren Namensteil genau dieser Person zugeordnet sein muss und deren Domain-Teil implizit validiert ist.
Die Überprüfung und Validierung einzelner Personen liegt natürlich nicht im Bereich von Sectigo, sondern bei den jeweiligen Organisationen. Die erfolgte Überprüfung ('identity vetting') bestätigt die jeweilige Organisation bzw. deren Vertreter ('RAO') mittels des Attributs 'Validation Type' des Personenobjekts (*Persons*). Ein 'GÉANT Personal email signing and encryption' Zertifikat wird nur dann ausgestellt, wenn dieses Attribut den Wert '*High (Identity Validated for S/MIME Sponsored Enrollment)*' hat.
Um dieses Attribut zu setzten, gibt es mehrere Möglichkeiten:

- Verwendung des *SAML Self Service Portal*: In diesem Fall wird das Attribut nach erfolgreicher Authentifizierung automatisch auf 'High' gesetzt.
- Verwendung einer *Enrollment Form*: In diesem Fall muss das Attribut manuell, oder per API gesetzt werden. Dabei ist zwischen 2 Möglichkeitren zu unterscheiden:
    - Person existiert bereits: Das Attribut kann jederzeit gesetzt werden.
    - Person existiert noch nicht: In diesem Fall muss die Enrollment Form wie gewohnt genutzt werden. Nach dem erstmaligen Ausfüllen und anschliessendem Submit kommt allerdings eine Fehlermeldung: 'The person does not have a high validation status....'. Zu diesem Zeitpunkt wurde die Person allerdings bereits im System angelegt und das Attribut kann gesetzt werden. Ein weiterer Klick auf 'Submit' oder jede spätere Verwendung der *Enrollment Form* erlaubt dann die Ausstellung des Zertifikats.
- Verwendung der API: siehe API Verwendung

> **Validation Type High**
>
> Grundsätzlich ist zu beachten, dass das Setzen des '*Validation Types*' auf '*High*' bestätigt, dass eine ‘persönliche Identifikation‘ der Person erfolgt ist. Dies ist natürlich nur für natürliche Personen möglich.
> Sectigo überprüft ausgestellte 'GÉANT Personal email signing and encryption' Zertifikate auch laufend auf Einhaltung dieser Voraussetzungen und widerruft falsch ausgestellte Zertifikate.

GÉANT Organisation email signing and encryption

In Zertifikaten, die mit diesem Zertifikatsprofil ausgestellt wurde, ist nur die Organisation validiert. Im Subject des Zertifikats findet sich auch nur die validierte Organisation (CN) und die Email-Adresse (E), deren Domain-Teil implizit validiert ist.
Diese Zertifikate bieten sich z.B. für Gruppen-Postfächer oder Rollen Email-Adressen an. Für diese Zertifikate reicht es, wenn der "Validation Type" des Personenobjekts (*Persons*) auf 'Standard' gesetzt ist.

Zu beachten ist, dass diese Zertifikate **nicht** via *SAML Self Service Portal* ausgestellt werden können. Eine Ausstellung dieses Zertifikatstyps ist nur mittels *Enrollment Form* oder *API* möglich.

Zertifikatsaustellung

Für die Ausstellung von persönlichen Zertifikaten ('*Client Certificates*') stehen die beiden unten angeführten Methoden zur Verfügung. Natürlich ist das Austellen von persönlichen Zertifikaten auch über die API möglich.

Self Enrollment

Um 'self enrollment' für Client Zertifikate zu aktivieren , müssen sie unter *Enrollment - Enrollment Forms - Client Certificate Web Form* wählen - *Accounts* kli cken - *Add* klicken oder bestehenden Account wählen und *Edit* klicken.
'(Certificate) Profiles' wählen, die verfügbar sein sollen (im Normalfall '*GÉANT Personal email signing and encryption*' und/oder '*GÉANT Organisation email signing*') und einen 'Access Code' vergeben und die weiteren Einstellungen je nach Bedarf vornehmen.
Unter https://cert-manager.com/customer/ACOnet/smime können sie dann im ersten Punkt '*Certificate Enrollment by AccessCode*' mittels des erstellten 'Access Code' und Angabe einer Mail-Adresse, deren Domain-Teil an die Organisation/das Department für 'client certificates' delegiert und validiert sein muss, das Zertifikat beantragen.

> **Client Self Enrollment im Department**
>
> Wenn sie Client Zertifikate im 'self enrollment' für ein Department einrichten, beachten sie bitte die Einstellungen zur 'key recovery':
>
> Sollten sie unter bei den Einstellungen des Departments (*Organizations <entsprechendes Department> - Certificate Settings - Client Certificates)* 'Allow Key Recovery by Department Administrators' angehakt haben, müssen sie einen 'encryption key' im Department anlegen, ansonsten ist die Ausstellung von Zertifikaten nicht möglich. Die Fehlermeldung im 'self enrollment' lautet 'Your client certificate is currently unavailable. Please try again ...'.

Den 'encryption key' kann allerdings nur ein DRAO (Department Admin) mit der entsprechenden Berechtigung im Department erstellen, als RAO ist dies nicht möglich.

SAML Self Service Portal

Erreichbar ist das SAML Self Service Portal für Client Zertifikate unter https://cert-manager.com/customer/ACOnet/idp/clientgeant

Voraussetzung für die Verwendung ist die Teilnahme an der ACOnet Identity Federation und darüberhinaus an eduGAIN. Weitere Informationen zur korrekten Konfiguration ihres Shibboleth IDP finden sie unter TCS Personal Certs.
Abschliessend muss im SCM noch der korrekte Wert für schacHomeOrganization konfiguriert werden (i.d.R. auf den Wert der eigenen Attribute-"Scope"). Dazu bei den Einstellungen ihrer Organisation (*Organizations -> Org. wählen -> Edit (=Bleistiftsymbol)*) den Wert, der als schacHomeOrganization mitgeschickt wird, unter '*Academic code (SCHAC Home Organization)*' eintragen.

Bei Problemen gibt es folgende URLs, um sich die übertragenen Attribute anzeigen zu lassen. Diese URLs können nach erfolgreichem Login am eigenen IdP aufgerufen werden, um die übertragenen Attribute auf Richtigkeit und Vollständigkeit zu prüfen:
https://cert-manager.com/customer/aconet/ssocheck/ - visuell aufbereitete Seite von Sectigo
https://cert-manager.com/Shibboleth.sso/Session - Anzeige der Session Attribute des Shibboleth SP

Code Signing Zertifikate

Voraussetzungen:

- CS für die Organisation aktiviert
  - *Organizations - Org wählen - Certificate Settings - Code Signing Certificates - Enabled*
- Domain für Code Signing Certificates delegiert
  - *Domains - Domain wählen - Delegate - Hakerl bei Code Signing Certificate*
- Account in Enrollment Form 'CS Web Form' (alternativ eigene Enrollment Form)
  - *Enrollment - Enrollment Forms - 'CS Web Form' wählen - Accounts - '+'*
  - alternativ: *Enrollment - Enrollment Forms - '+'*

Beantragung Zertifikat:

- Email Invitation schicken
  - *Certificates - Code Signing Certificates - Invitations - '+'* - Email-Addr. eingeben und entsprechenden Enrollment Endpoint & Account wählen
- Link in Email klicken und Webformular entsprechend ausfüllen

Grid bzw. IGTF SSL Zertifikate

Für die Aktivierung/Freischaltung von IGTF SSL Zertifikaten kontaktieren sie bitte das ACOnet Team unter tcs@aco.net

Secondary Organization Name

Für die Verwendung von IGTF SSL Zertifikaten ist ein Organisationsname Voraussetzung, der nur ASCII Zeichen enthält. Dafür gibt es den '*Secondary Organization Name*', wo die 'asciified' Version des Organisationsnamen eingetragen werden kann. Auch dieser Name muss erneut validiert werden (siehe auch Spalte '*SECONDARY VALIDATION*' in der Übersicht).
Nur wenn es diesen '*Secondary Organization Name*' gibt, können IGTF SSL Zertifikate ausgestellt werden.

API Verwendung

Infos zur Verwendung des SCM REST API bei Sectigo

'WS API use only' Verwendung

Prinzipiell kann jeder Benutzer im SCM auch die API Funktionalität verwenden. Es ist jedoch aus Sicherheitsgründen sinnvoll, für das API einen eigenen Benutzer anzulegen und diesen auf die Benutzung des API einzuschränken. Dazu dient der Parameter 'WS API use only' bei den Privileges eines Benutzers. Auf Grund der Art der Benutzerverwaltung bei Sectigo ist es jedoch auch bei einem solchen Benutzer notwendig, dass bei der Anlage gesetzte Passwort, nach erstmaligem Login zu ändern. Es empfielt sich somit folgender Ablauf:

1. API Account anlegen bzw. vom ACOnet Team anlegen lassen, falls er auf Organisationsebene funktionieren soll (siehe oben), 'WS-API use only' noch nicht wählen
2. Mit dem API Account im SCM anmelden - Passwort ändern
3. Dann 'WS-API use only' wählen bzw. dem ACOnet-Team Bescheid geben, dass wir das tun sollen.
4. Ab dann funktioniert der User per API, kann sich aber nicht mehr im SCM anmelden.

Was ist der 'customerUri'

Customer aus Sectigo Sicht ist immer ACOnet, der korrekte Wert ist also `'customerUri: ACOnet'`

Zertifikate per API beantragen

Um Zertifikate (Client oder SSL) per API beantragen zu können ist es notwendig, die Option *'Web API'* im jeweiligen Register anzuhaken. Es ist auch notwendig, einen *'Secret Key'* zu vergeben, welcher allerdings für das REST-API nicht in Verwendung ist (dieser Key würde für die alte SOAP API verwendet werden).

einfaches curl Beispiel

Anzeigen der eigenen Organisation(en) ink. dazugehöriger Informationen:

```
curl 'https://cert-manager.com/api/organization/v1' -i -X GET -H 'customerUri: ACOnet' -H 'login: <login>' -H
'password: <password>'
```