SECTIGO
Certificate Manager

Documentation for Belnet’s customers

Author: Pascal Panneels (pascal.panneels (AT) belnet.be)

Initial version date: 13/03/2020

Last revision date: 08/05/2020

Content

0. Foreword

This documentation is not an official one coming from Sectigo but a little manual written by Belnet to help our customers to use the new Sectigo's portal. It may contain errors and can be changed at any time without any prior announcement.

The use of the portal from March 2020 is still considered as a beta testing phase.
While it is not the definitive version of the portal, the delivered certificates are effective ones that may be deployed on production's servers, services or for personal use. They will remain valid even after the closing of test period (on 30/04/2020).

In case of instability of the interface, no support will be obtained from Sectigo at the moment as it is still not the production phase.
Bug reports may be done to Belnet; we will then transmit it to the responsible contacts of the project at Sectigo via Géant Association's representative persons.

In the text below, there are some terms written in american english (like *organization*); this is intended to reflect the content of the current interface of Sectigo.

The Sectigo website is in english as well as the documentation (there is a local version in spanish though).

URL to access SCM for every customers : https://cert-manager.com/customer/Belnet

Glossary of used terms/acronyms :

- **MRAO** :*Master Registration Authority Officer*, typically a person from Belnet’s technical staff able to have a (±) full control of the various tasks on the interface such as creating new organizations.
- **RAO** : *Registration Authority Officer* : any person from an organization that will have the right to create/validate/authorize new users, new departments, new domains and new certificates ; also, able to revoke, modify, delete, edit a few parameters in the interface.
- **DRAO** : *Department Registration Authority Officer* : any person able to create certificates, domains, edit parameters within a department of an organization.
- **SCM** : *Sectigo Certificate Manager*, is the name of the Sectigo’s web portal. The term is used in the rest of the document to design the Sectigo’s portal.
- **DCV** : *Domain Control Validation*, is the procedure in place by the CAB/Forum to validate domains. The procedure requires to answer to an email, put something in place on a website or add a token as a CNAME in the DNS.
- **PKCS-12** : *Public Key Cryptography Standard number 12*, a de facto standard published by RSA Security a few years ago that defines a way to archive a certificate and private key in a bundle file that may be signed and/or encrypted.

1. Introduction

There is no automatic transfer of the actual data (institutions names, contact persons, domains...) used by DigiCert to Sectigo planned.

Thus, a few intial *bootstrap's work* needs to be done to make the new service operational, as it was already the case when we switched from Comodo to DigiCert a few years ago.

The management of SCM is splitted in 2:
- initial work made by Belnet’s MRAO;
- day-to-day management of each institutions settings by the local RAO.

2. Initial tasks made by Belnet's MRAO

The first thing to do is to define the institutions as a *New Organization*.
An organization is an entity by its own that is coupled to a legal institution (here in Belgium) and that will be verified and validated by Sectigo.

This is done by login in the portal with a main administrator login (=MRAO).

Click on **Settings->Organizations**, then push **[+Add]** button and fill in the data relative to the new organization. Required fields are marked with a red *.

Then, select the organization in the list and click on the **[Validate]** button and confirm the start of the validation process by clicking on **[OK]**.

The *validation status* turns to **[pending]**. It will become **[validated]** when the organization will have been checked by Sectigo’s validation’s team.

Then, create a RAO for that organization : click on **Admins** tab, then push on the **[+Add]** button and fill in the data relative to the new RAO. At least, one RAO per organization is needed. Local RAO will be able to create new RAO and DRAO.
The email address of the person will be used as his login and an intial password should be defined for the RAO.

Send an email with her/his credentials (login + password) using your normal mail client.

SCM sent automatically an email as well, but he needs to get his intial password from us.

update 06/04/2020: all customers have been created, with their associated domains and DCS_CP as well.

3. RAO's operations

The URL to access SCM is https://cert-manager.com/customer/Belnet for everyone.

When your account has been created by Belnet, you'd have received an email from Sectigo with instructions on how to access your account and an email from Belnet with your initial credentials (login + password).

3.1. Change your password

You will be invited to change your password the first time you login with the initial credentials received. Simply follow the instructions in the window after having clicked on the link in the received email from Sectigo.

3.2. Create domain names

You will need at least one domain validated in SCM to be able to ask for certificates (principal domain name of your organization such as *yourdomain.be*) .

update 06/04/2020: Belnet has defined all the domains that were set in DigiCert' system. You only need to apply DCV to them and create their wildcard versions. ***DCV is required before you can use them !***

Also, a long with your principal domain, you need to create a *wildcard domain per added domain*, such as **.yourdomain.be*. It is needed to simplify the creation of certificates in subdomains by avoiding the validation of every subdomains manually. When main domain is validated (see DCV further) associated wildcard is automatically validated as well.

Go to **Settings->Domains** then click on **[+Add]** button and fill in the form ; you will need to enter the domain name, click on **[Active]** checkbox if it is not checked yet and on the checkbox in front of your Organization's name. By default, it will mark the 3 checkboxes (SSL, Client Certificate and Code Signing) to let you ask for these types of certificates for your domain.

Click on **[OK]** in the window to confirm.

Don't forget to add the corresponding wildcard domain (**.yourdomain.tld*) using the same procedure.

Then, select your added domain in the list, and click on **[Approve]** button to let it be approved.

Last thing to do is to proceed to the DCV, otherwise you will not be able to use your domain in your certificates.

Click on **[DCV]** tab ; check the domain you want to validate and click on **[DVC]** button.

Then select the method you will use to validate your domain.

If you select CNAME, the instructions will be displayed in your browser, and it consists of putting a token associated to a CNAME in your DNS (everything is displayed, you'll simply need to do a copy-paste of the information in your DNS).

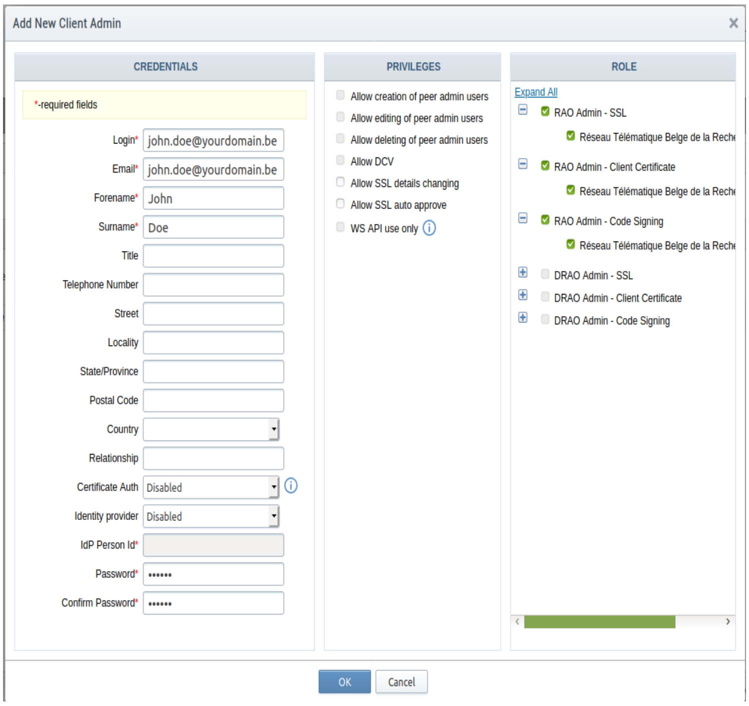
If you use email, you'll need to select the address from the fixed list of 5 (administrator@yourdomain, hostmaster@yourdomain, postmaster@yourdomain, …) and follow the instructions that you will receive in a mail sent to that address. Be warned that there is no other mail address possible that the fixed ones.

If you choose HTTP(S) method, instructions will be given in your browser as well, and it consists of setting a given token on your website's content.

You should do the same procedure for all your domains.

3.3. Setup your RAO/DRAO users

As RAO, you'll be able to create other users for your organization such as other RAO with same role as you, but also DRAO.



*-required fields

Login*	john.doe@yourdomain.be
Email*	john.doe@yourdomain.be
Forename*	John
Surname*	Doe
Title	
Telephone Number	
Street	
Locality	
State/Province	
Postal Code	
Country	
Relationship	
Certificate Auth	Disabled
Identity provider	Disabled
IdP Person Id*	
Password*	••••••
Confirm Password*	••••••

□ Allow creation of peer admin users
□ Allow editing of peer admin users
□ Allow deleting of peer admin users
□ Allow DCV
□ Allow SSL details changing
□ Allow SSL auto approve
□ WS API use only

Expand All
☑ RAO Admin - SSL
☑ Réseau Télématique Belge de la Reche
☑ RAO Admin - Client Certificate
☑ Réseau Télématique Belge de la Reche
☑ RAO Admin - Code Signing
☑ Réseau Télématique Belge de la Reche
□ DRAO Admin - SSL
□ DRAO Admin - Client Certificate
□ DRAO Admin - Code Signing

Go to **[Admins]** tab, then click on **[+Add]** button and fill in the form.
I propose to put the email address as login name.
Fill in all the required fields (marked with a red *) in the *Credentials* column.

Set the privileges for the user in the *Privileges* column. It consists of allowing him/her to create/edit/delete other RAO and change details in SSL certificates requests.

I propose to check following privileges :

- ✔ *Allow creation of peer admin users*
- ✔ *Allow editing of peer admin users*
- ✔ *Allow deleting of peer admin users*
- ✔ *Allow SSL details changing*

unless you really want to restrict the privileges.

Last thing to setup for the user is his/her roles in the third column.

I propose to check following 3 roles :

- ✔ *(D)RAO Admin – SSL*
- ✔ *(D)RAO Admin - Client Certificate*
- ✔ *(D)RAO Admin - Code Signing*

unless you really want to restrict to very specific role.

3.4. Setup departments

Sectigo has introduced the notion of departments within organizations to let you fine tune permissions and roles within your institution.

To add a department, click on **Settings->Organizations**, then select your organization in the list.

Click on **[Departments]** button, then **[+Add]** button in the open window.

Fill in the form (some fields are pre-filled in and cannot be changed) specifying the department’s name. You should click on the other tabs (Client Certificate, SSL Certificate and Code Signing Certificate).

In *Client Certificate*, you need to uncheck all the *Allow Key Recovery...* lines (unless you really want it, but you shouldn’t…).

In *SSL Certificate*, you should let everything unchecked.
In *Code Signing Certificate*, you should tick the **[Enabled]** checkbox (unless you don’t want to allow this kind of certificate to be generated by the department…your choice ; it can be modified later on anyway).

Then click on the **[OK]** button to close the window and have the department added.

4. Certificates

Sectigo has divided its offer in 3 categories :

- **SSL certificates** : group of all certificates used for servers/services such as simple SSL or EV, multi-domains, etc.
- **Client certificates** : personal certificates used for sending S/MIME emails.
- **Code Signing certificates** : used to sign development’s code in supported environment.

4.1. SSL Certificates

Choose Certificates → SSL Certificates to get to the correct page.
A list of already created certificates for your institution will be displayed. You may customize the list by clicking on the little tools button on the upper right corner of the list to add fields.

You may select a certificate in the list ; then other operation’s buttons will be displayed such as :

- Details : to display details of the certificate’s content ;
- Renew : to renew the certificate ;
- Revoke: to revoke the certificate ;
- Replace : to replace it by another one.

If you want to create a new one :

- create your CSR (Certificate Signing Request) using the tool of your choice (such as OpenSSL…) for your server;
- click on the [+Add] button ;
- choose « Manual creation of CSR »’s mode; other methods are available only if you’ve installed Sectigo’s agent application and have been delegated to use it (currently not documented here, please refere to official Sectigo documentation) ;
- in CSR section, you may either copy-paste the CSR you’ve created or use the [Upload CSR] button to choose the CSR’s file to upload ;
- click on the [Next >] button ;
- Basic information of your certificate will be displayed ; here you may customize the options for your certificates such as associated Department, Certificate type (any of Géant’s types, names are self explanatory ; you may not select ‘EV Anchor Certificate’ as it is a peculiar kind of certificate for Sectigo’s usage) , Validity Length in years, Server Softare to use such as ‘Apache/ModSSL’ or Microsoft IIS;
- click on the [Next >] button ;
- you may choose to auto-renew the certificate by ticking the « Enable auto renewal » checkbox ;
- click [OK] button
- the certificate will now be added in the list of your owned certificates ;
- click to select it ;
- as RAO /DRAOn you will receive an email from Sectigo to let you know that there is a certificate waiting for your approval/denial ;
- new buttons are now displayed :
  - Edit : before approving it, you may still modify the options entered before ;
  - Details : details what has been entered as well as its status ;

    - Approve : click on it to approve the request ; a small form is displayed to enter a message for approval (you are obliged to enter something such as ‘OK’) ; then click on the [OK] button ;
    - Decline : click on it to reject the request.

- After « approved », the certificate passed in the status « Applied » and then in « Issued »
- Requestor has now received an email to let him know that his/her certificate is ready to be downloaded and installed.

4.2. Clients Certificates

Choose Certificates → Client Certificates to get to the correct page.
A list of created persons of your organization will be displayed.

You may select a person in the list ; then other operation’s buttons will be displayed such as :

- Edit: to change informations of the person ;
- Delete : to delete the person ; it will also revoke all the certificates owned by that person;
- Certificates: to list all the certificates for the person ; it will open a pop-up window in which you’ll have several options to view, revoke, download certificate.

To create a new person able to get client certificate :

- press the [+Add] button ;
- Fill in all the necessary fields (marked with a red ‘*’)in the pop-up window ;
- press the [Ok] button to confirm the creation;
- the person will appear in the list ;

To create an invitation for a client certificate for the person :

- select him/her in the list ;
- click on [Certificates] button ;
- in the pop-up window, client on [Send Invitation] button
- in the new pop-up window named ‘Confirm Invitation’, select the duration (=term) of the certificate in the little dropdown (from 1 to 3 years) ;
- press the [OK] button ;
- in the window, the status ‘Invitation sent on: DATE HOUR UTC’ will be displayed.
- The person has now received an email from Sectigo with instructions to let him create his/her certificate.

The creation of the certificate is done by :

- click on the link in the email
- in your browser, user has to fill in some fields :
    - PIN code (twice) : used to encrypt the PKCS-12 file that will contain you certificate ;
    - Passphrase (twice) : NEED TO CHECK THE USAGE OF IT ;
    - User needs to scroll the ‘Terms of Service’ text box ;
    - User needs to tick the checkbox ‘Accept terms of service’ ;
    - User needs to click the [Submit] button ;
    - the window displays that the certificate is ready to be downloaded (it has been created by Sectigo) as a .p12 file;

    - User needs to click on the [Download] button to save his/her certificate on local machine.
    - He/She can then install the file where it is needed such as his/her web-browser, mail client, etc. The PIN code is needed to decode the .p12 file when asked by the program that will handle the installation of the certificate.

4.3. Code Signing Certificate

Choose Certificates → Code Signing Certificates to get to the correct page.

A list of already created certificates for your institution will be displayed. You may customize the list by clicking on the little tools button on the upper right corner of the list to add fields.

To create a code signing certificate :

- press the [+Add] button ;
- Fill in all the necessary fields (marked with a red ‘*’)in the pop-up window ;
- press the [Ok] button to confirm the creation;
- the person will appear in the list ;
- a mail is sent by Sectigo to the person with instructions ;

To create the certificate itself :

- Click on the link in the received email ;
- your browser has open a page with prefilled fields
- click on the [Generate] button

5. Other informations

5.1. CAA record for Sectigo in your DNS

Sectigo, such as many other CA, uses a CAA record in your DNS for the domain you’re requesting a certificate for.

If you have defined a CAA record for another CA in your DNS, don’t forget to add one for Sectigo otherwise you will encounter problem while asking certificates that are sometimes hard to troubleshoot.

In bind, such record are in the following format (syntax described in RFC3597) :

```
; CAA records to permit certificates issued by Sectigo
belnet.be       TYPE257 \# 18 000569737375657365637469676F2E636F6D
```

You may go to a site such as https://sslmate.com/caa/ to help you generate the corresponding record. Some versions of bind authorizes the more soft syntax :

```
belnet.be.      IN      CAA     0 issue "sectigo.com"
belnet.be.      IN      CAA     0 issuewild ";"
```

Check version of your DNS server for the correct syntax to use if you plan to add CAA records.

5.2. Certificates Discovery Service

Sectigo has introduced some tools to help you find and manage the certificates on your servers with some automation tasks.

5.2.1. Integrated Certificates Discovery Service in SCM

To create a discovery task :

- click on ‘Discovery’ tab ;
- select ‘Network Discovery Tasks’ ;
- to add a new task, click on [+Add] button ;
- in the window :
  - give a name to the task (whatever you want, for example « my discovery ») ;
  - in next to ‘Range to scan’, click on the [Add] to add a range of IP to scan ;
  - in the ‘Add scan range’, enter a range of IP to scan (for example, in CIDR, 1.2.3.0/24)
  - click [OK] to close the sub-window ;
  - redo the last operation for other domains you want to add to the task ;
- click on ‘Assignment Rules’ tab :
  - not mandatory but useful to the management of your certificates ;

        - you may select a/several rule(s) from the left listbox and click on the [→] button to assigned it to the task ;
        - to create a new rule, click on the « Create New Assignment Rule » button ;
            - in the sub-window, give a name to the rule (for example : ’certificates for my department’)
            - create a matching rule by combining the options in the several dropdown (for example : ‘Common Name’ - ‘Ends with’ - « mydomain.be »)
            - Use the ‘Assign to...’ rules to create the actions (for example : ‘Assign to...’ - ‘My organization’ - ‘my department’)
            - click on the [OK] button to close the sub-window ;
- click on ‘Schedule’ tab :
    - choose the ‘Frequency’ of the task (for example : ‘Manual’) ;
    - click [OK] button to close the window ;

To use the rule :

- select the task in the list ;
- a few buttons appears with options :
    - [Scan] : to launch the scan ;
    - other buttons for options are self explanatory.

When the task has finished, you may go to ‘Network Assets’ tab to have the list of discovered certificates in your specified’s IP ranges.

6. Usage of Sectigo's REST API

To use Sectigo's API, you first need to enable the API feature in the interface :

- click on *Settings*;
- click on *Organizations*;
- select your organization by clicking on the radio button;
- push the [Edit] button;
- in '*Client Certificate*'s tab, click the "Web API" checkbox;
- you need to create a *Secret Key* below (it is mandatory); it is a feature used by ancient SOAP calls, thus no use with REST, but specification is mandatory though.

You can find the documentation over the REST API at following URL :

https://support.sectigo.com/Com_KnowledgeDetailPage?Id=kA01N000000XDkE

6.1. Create a dedicated user to use the REST

It is best to create a user that will be used only for the access to the web API.

- Create an Admin user the usual way (by setting roles and privileges), but DON'T enable the permission "WS-API use only" at first ! (ie: *apiuser@your-org.be*)
- Logout of SCM and then log back in using the create user credentials; it will ask you to change the password; create a solid secure one (ie: *JHuj75$!JKJ452.36*)
- Now, open again Admins --> your user and click [Edit];
- Set the "WS-API use only" to checked; this way, your user will not be able to login into SCM anymore, but will be able to access/use the REST API.

6.2. Sectigo REST examples

6.2.1. Using 'curl' to retrieve a list of domains

```
curl 'https://cert-manager.com/api/domain/v1?size=10&position=0' -i -X GET \
   -H 'customerUri: Belnet' \
   -H 'login: apiuser@your-org.be' \
   -H 'password: 'Huj75$!JKJ452.36'
```

Note that ***customerUri*** is always set to '**Belnet**', even for your institution. It is the login that will determine which institution you belong to and filter the domains of your institution only.

6.2.2. Using Python to retriev a list of domains

Same purpose than previous example, but using a little script written in Python 3 :

```
#!/usr/bin/python3
#
# use Sectigo API to retrieve a list of domains
#
# by Pascal Panneels, 20200312 - Belnet
#

import json
import requests

api_url_base = 'https://cert-manager.com/api/domain/v1?size=10&position=0'
api_headers = { 'customerUri': 'Belnet',
                'login': 'apiuser@your-org.be',
                'password': 'Huj75$!JKJ452.36', }

resp = requests.get(api_url_base, headers=api_headers)

if resp.status_code!=200:
        print("error accessing the URL!")
        exit(1)

for item in resp.json():
    print('{};{}'.format(item['name'], item['id']))
```

7. GRID (IGTF) Certificates

To be able to ask for GRID certificate, you need to validate the name of your organization as a Second Orgnization Name using only ASCII characters (thus no accentuated or special characters).

Same as for the primary name :

- go into Settings --> Organization and select your organization by clicking the radio button on the left;
- click the [Edit] button;
- fill in the Secondary Organization Name with the name of your organization but in simple ASCII characters only.

After that, the name needs to be validated by Belnet.

Send a mail to services@belnet.be to ask for validation of the secondary organization name.

When validated, you will now be able to ask for IGTF certificates (it is a certificate type when you request a SSL certificate in the dropdown control, "*GÉANT IGTF Multi domain*")

If you don't validate the secondary organization name, the certificate type will be grayed and you will not be able to ask for.

8. Support in case of problems

In case of problems, you should contact Sectigo by filling in the support web form on

https://sectigo.com/support-ticket

As it was already the case with DigiCert, Belnet has no influence on the certificates delivery, timing for approval, or anything related to the work of Sectigo related to accounts, certificates, domains, etc.

Such demand should pass to Sectigo' support, no answer will be given to such request by Belnet anymore.