Manual Managed PKI

Inhalt

1. Introduction

1.1 SwissSign and Managed PKI

SwissSign AG is an internationally recognised issuer of digital certificates.

The SwissSign Managed PKI web service is used for issuing and managing SwissSign certificates. The advantage when using the Managed PKI service is both in the fact that it is not necessary to set up and operate your own certification authority and also the quality of the obtained certificates with regard to the distribution in the root stores and their compliance with the corresponding international standards.

As part of this Managed PKI service, customers can request, approve, issue and revoke and also search for and manage certificates. Here the web portal supports the various roles (requester, approver, auditor) within a company with regard to certificate management. Here the customer takes on the task of a registration authority (RA), while SwissSign AG takes on the operation of the certification authority (CA) and generally appears as the certificate service provider (CSP) towards third parties. Of course the SwissSign Managed PKI web service also supports the mere operation of a customer CA.

1.2 Objective and purpose of this document

SwissSign Managed PKI service customers receive an individual setup on the SwissSign infrastructure in order to manage their certificates. This document shows how certificates can be managed with the Managed PKI service: request, issue, management and revocation.

1.3 Structure of this document

The structure of this document follows classic processes which are standard with private key infrastructures (PKI = private key infrastructure). These PKI processes and their roles are shown in an introductory chapter.

The index at the end of this instruction manual lets you quickly find answers to questions. The manual uses cross references, by selecting the chapter numbers in the text you can quickly find connected, relevant contents. The print screens in this manual were created with Internet Explorer 9, in other browsers there may be differences in the display.

1.4 Requirements for using the SwissSign Managed PKI web service

Any person who is a recipient of a signed document or logs onto a website is called «relaying party» and has to be able to rely on the content of the certificate. The person therefore trusts the certificate service provider. As a consequence of this chain of trust, the customer of a Managed PKI service signs the Declaration of Consent to the Delegation of Registration Authority Activity where the customer is subject to the rules of the certificate service provider and documents the particular responsibility and care used in dealing with and issuing certificates. The rules of the certificate service provider are described in detail in the certificate policy and certification practice statements CP/CPS (www.swisssign.com/support/repository).

SwissSign therefore – unlike with the certificate products in the webshop – does not carry out an individual check of the certificates with regard to the certificate subject if this fulfils the guidelines of the Declaration of Consent to the Delegation of Registration Authority Activity. In the Declaration of Consent to the Delegation of Registration Authority Activity the permissibilities and attributes of the certificate issuance are specified (e.g. the permitted domains, period of validity of the certificates, visibility of the certificates in the LDAP directory) and also the obligations, test processes and regulations regarding care with which the registration authority (RA) has to comply.

1.5 Project-specific exceptions

Some customers have adapted, project-specific web interfaces. This means that some of the pictures in this manual may differ from project-specific adaptations. The project-specific differences are, for example:

- **Login via smart card instead of via soft certificate**
- **Selection of products within the Managed PKI without the possibility of adding shop products**
- **CSR field means an obligation for certain Managed PKI products**
- **User ID in the subject**

There will be no details of the project-specific exceptions in the following. It must be noted, however, that there may be a different appearance with several print screens because of this.

2. PKI processes and roles

Certificates have two central tasks, on the one hand they are a container for the public key and, on the other hand, they connect the public key with the certificate holder/key holder. The task of a certificate service provider is to confirm and guarantee this connection as an independent third party at the level according to CP/CPS. So that this can be guaranteed, the following services, activities and roles are required:

Registration service

- **Certificate request by the requester**
- **Certificate request check by the registration authority officer (RAO) or, in the following, called access responsible.**
- **Approval of the certificate request by the access responsible**

Certificate generation service

- **Generation of the certificate**

Revocation service

- **Online revocation by the certificate holder**
- **Offline revocation by the Access responsible**

Dissemination services (distribution of information)

- **CP/CPS**
- **OCSP (Online Certificate Status Protocol) – online status regarding the validity of certificates**
- **CRL (Certificate Revocation List) – revocation lists (offline) of certificates**
- **LDAP (Lightweight Directory Access Protocol)**

The following table gives an overview of the activities and their representation in the Managed PKI service:

Activity	Role/who	MPKI support
Certificate request	Requester/system administrators	GUI
Approval	Access responsible	GUI
Issue/generation	-	CA
Installation	Requester/system administrators	E-mail with download link
Revoke	Requester/system administrator, Access responsible	GUI
Renewal	Requester/system administrator, Access responsible	Warning e-mail 10 days and 30 days before expiry
Search/Manage	Requester/system administrator, Access responsible	GUI
Inform/audit	Access responsible, auditor	GUI

3. Control concept

The user interface is written natively without use of any special software for the user interface. This is to meet the objective of security because the use of unknown, third-party software packages also always means a security risk. In this respect the use of graphics and icons in the user interface is minimised.

3.1 Basics

3.1.1 Roles within the Managed PKI of SwissSign

The system was developed to make the issuance and management of certificates as easy as possible. For this reason the system works with various roles which have different rights:

Requester	**Typically a user who can request a certificate. In this role they can request the certificates which have been activated for them.** **A requester logs in with user name/password or it is configured additionally or alternatively to enable the requester to log in with a certificate.**
Access responsible	**Takes on the functions of the administrator of a registration authority (RA). Can see all certificates of an RA, approve, request, revoke, view certificate requests and create accounts for requesters.** **The Access responsible manages also the access certificates for a secure TLS connection.**
RA distributor	**This is defined only when the Access responsible is not defined. Does not have an RA function. Sees all certificates of the RA, can request, view, revoke certificates or create requester accounts. This is interesting, for example, for SwissSign partners that want to sell the SwissSign Managed PKI via resellers to end customers and have an overview of the entire business.**
RA auditor	**Can see all certificates including detailed data of certificates such as date of issue, date of expiry, etc.**

3.1.2 Accounts

Accounts are used for managing certificates at the level of requesters or requester group and were also called profiles in earlier releases of the SwissSign Managed PKI.

An account represents a user or a group of users who can log in using user name/password or via certificate. Accounts are created by access responsibles within an MPKI setup and are connected with specific requesters within the Managed PKI setups. The access responsible can determine whether a certificate login is absolutely necessary for this account and whether the requester may also revoke the certificates.

An account comprises contact information, in particular the e-mail address for notifications and, optionally, a telephone number. The information can be changed by the account holder.

The requester can make certificate requests within the framework of the certificate types permitted for the RA. Each certificate request using this account is allocated to this account. The account information therefore does not have to be assigned individually for every certificate request. Every individual certificate request is forwarded via a workflow to the corresponding access responsibles who must check and approve this request.

Please note: The account within the scope of the Managed PKI on swisssign.net has nothing to do with the user accounts created if necessary in the webshop www.swisssign.com.

3.1.3 Access responsible

Access responsibles manage an RA (see chapter 3.1.4). Here they have typical basic functions available such as displaying, searching for and exporting certificates. Only access responsibles can issue certificates, approve requests for certificates (via user accounts with requester permission) and modify the rights of users. Overwriting passwords of requester accounts is also possible for access responsibles. All access responsibles have mutual access to the accounts which are connected with corresponding RAs.

Please note: The login as access responsible must definitely be done with the access responsible certificate set up beforehand by SwissSign.

3.1.4 Registration authority (RA)

A Managed PKI customer can have several registration authorities set up by SwissSign, as specified in the corresponding Declaration of Consent to the Delegation of Registration Authority Activity. It might therefore make sense, on account of different processes, to use one RA only for Gold certificates and another only for Silver certificates, or one for personal certificates and the other for SSL certificates. But large departments can also have an RA for themselves which is separate from the RA of another department.

The advantages are in the organisational processes: In the allocation of roles, for example, the role «requester» can then be later assigned only to a specific RA by the administrator and therefore become separate in organisational terms. The checking of the certificates can also be done separately for the registration authorities.

3.1.5 Certificate voucher

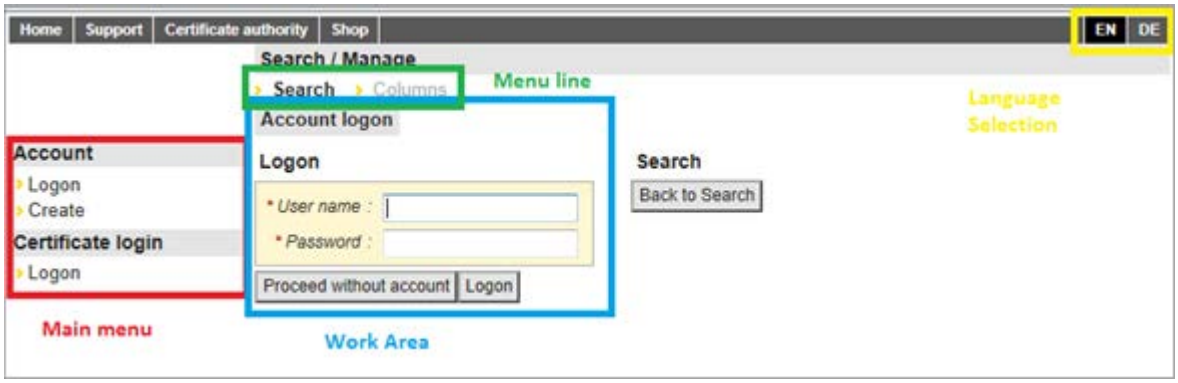
A certificate voucher is a code which allows the user to request a corresponding certificate. Within the framework of the Managed PKI the certificate voucher code is not used or is used only if very small quantities are needed of a specific certificate type. The certificate voucher code can be typically obtained in the SwissSign webshop.

3.2 Structure of the user interface

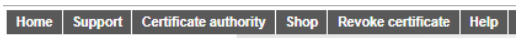
The user interface is divided into the following areas:

- **Header section: General information and language selection**
- **Main menu**
- **Menu line**
- **Work area**

The user interface is divided into the following areas which are referred to in the text below:



In the top left there are several buttons which are connected with links:



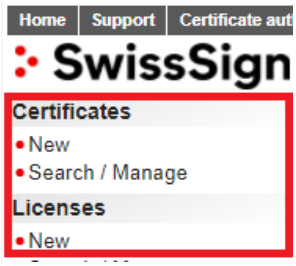
- ***Home: By pressing this button you are always taken back to the homepage of the user interface.***
- ***Support: A link to the helpdesk***
- ***Certificate authority: Here you are given general information about SwissSign and other links, e.g. to the CP/CPS and certificates of the root and intermediate CA.***
- ***Shop: Here you are taken to the SwissSign webshop.***
- ***Revoke certificate: Common information about possibilities for a revoke of a certificate***

Special feature: With a button in the very top right the user can hide this bar completely (including the logo) to have a bigger working area.

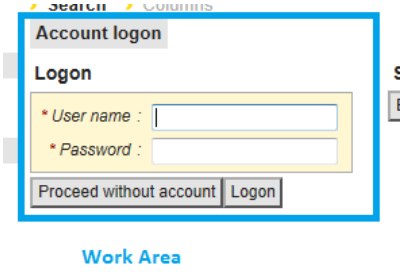
In the top right the language can be changed at any time.

DE: User interface in German
EN: User interface in English

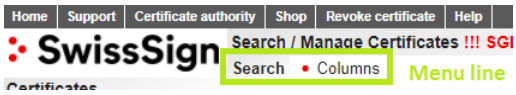
On the left is the main menu. Actions can be selected below the individual submenu headings.



Via the menu items in the main menu the application procedure is controlled in the work area.



Depending on the selected menu in the main menu, a workflow or procedure or several actions are possible. To control the work area accordingly, you can click on the buttons in the menu line above the work area.



3.3 Start and login on ra.swisssign.net

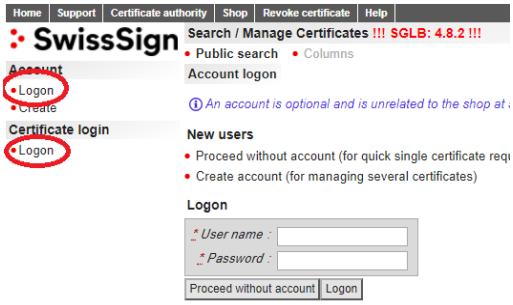
Before logging in for the first time, the customer receives the necessary configuration from SwissSign in order to work with the MPKI infrastructure. This configuration was stipulated beforehand in the Declaration of Consent to the Delegation of Registration Authority Activity documentation. Here as desired the customer receives one or more – normally three – access responsible certificates for authentication with respect to SwissSign and for access to the SwissSign CA at www.swisssign.net as an access responsible.

The certificate has to be set up in the operating system/browser or be available on a smart card to be able to use it for the login.

Generally there are two options for logging in:

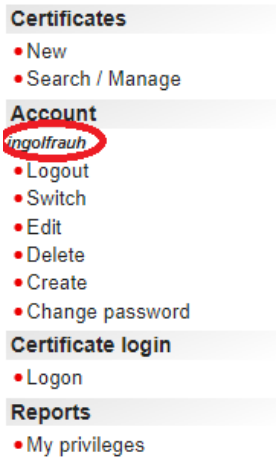
- Certificate login: As access responsible only possible with certificate. This is also possible via the main menu point on https://www.swisssign.net .
- Login with account which is allocated to the role requester, for example. The requester accounts are

generally created by the access responsible. This login is only via https://www.swisssign.net possible.



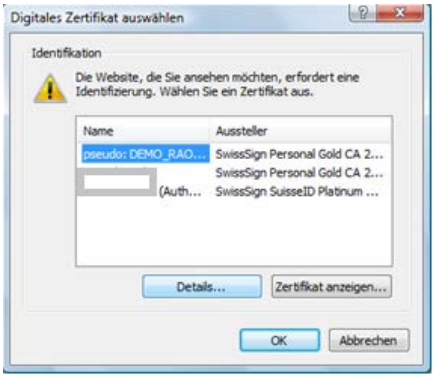
It is always possible to take on another role as an already logged in user and to log in with a corresponding account.

As soon as you are logged into the account, the profile name below the menu line «Account» will be displayed in italics and bold.

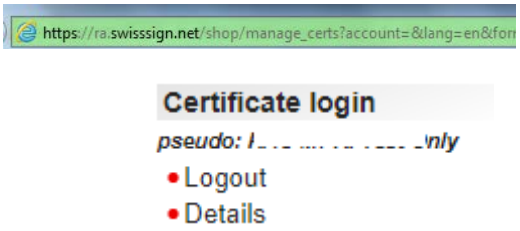


If you want to log in as an access responsible with a certificate, SwissSign has to set up a certificate for the access responsible. The access responsible can also set up a login using a certificate for other users later via «Permitted certificates».

You are first asked via a window of the operating system to select the certificate for the login. A SuisseID Platinum or a special RAO certificate is always configured for the access responsible.



A successful login as access responsible is displayed in the address bar of the browser: The address: ra.swisssign.net is selected. In the main menu it can now also be seen that the user has logged in with a certificate. The logged in user now appears below the menu line «Certificate login».



Please note:

- It must be ensured that you are logged in with only one account. With «Log out» you can log out of the corresponding account.

- When logging in, an accountsession cookie (signed) is created. This is valid for less than 30 minutes.
- A requester account is created for the customer by the access responsible. The access responsible also has the option of assigning a new password if the requester has forgotten the password in question.

3.4 Dealing with user accounts

A user can log into a user account. This account is essentially connected with various roles.

3.4.1 Creation of an account

Customers of a Managed PKI with an own registration authority should use only accounts which the access responsible has created for them. All other accounts are reserved for webshop users. The certificates requested via an account which was not set up by the access responsible cannot be seen in the RA management.

There will not be an explanation of the creation of accounts for webshop customers here.

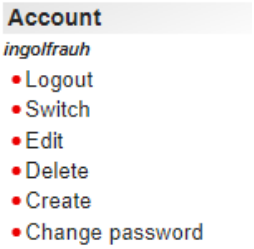
3.4.2 Logging into the account

A certificate requester can log into the account set up beforehand by the access responsible. The access responsible has specified whether the login has to be definitely done with user name/password or certificate. Accordingly the login has to be done under the menu item «Logon» in the menu «Certificate login» or the menu «Account».

3.5 Account management

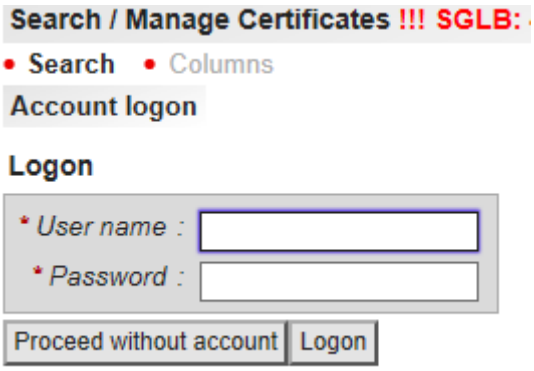
As a normal user you have the option to manage your account afterwards.

In the main menu you have the following options for managing your account under the menu item «Account»:



With «Logout» you can completely log off from the application and are practically a user without an account of the website. Users without an account can, for example, still search for and display publicly published certificates.

With «Switch» you can switch to another account by logging into this.



With «Edit» you can change the attributes of the account, e.g. the e-mail address or telephone number.

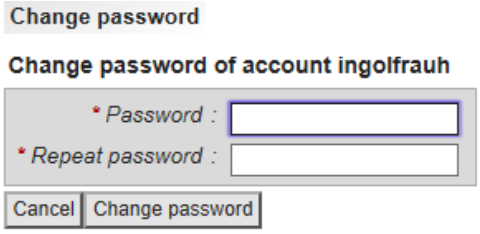
With «Delete» the already existing account can be deleted. Please note: The corresponding account will be deleted immediately.

With «Create» another account can be created. It is done in the same way as the initial account creation. In this case you have to specify a user name, a password, and an email address will which be used for all notifications of the certificates requested by this account regardless of the email address used in the certificate itself. The preferred language specifies the email notification language and language of the web GUI after login.

Password can be 49 characters containing the following characters:

A-Z, a-z, 0-9, space and ,;:!?&_*(){}/\\-"#$%@'+<=>`|^~

With «Change password » you change the password for an existing account.



3.6 Creation and management of requester accounts

3.6.1 Creating a new requester account as access responsible

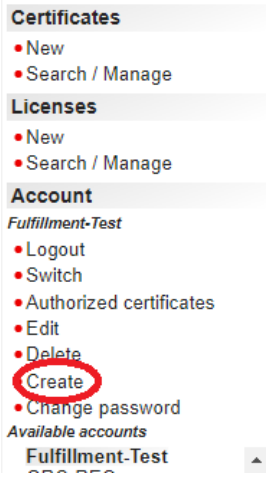
The access responsible has the option of allocating the role «requester» to certain users. The administrator can also specify that these people may log into the Managed PKI platform only with a certif-

icate and no longer with user name/password. A certificate has to be connected with an account for this. In the case of SwissSign certificates, at least a Gold certificate or a special configured RAO certificate has to be selected here. The access responsible can also stipulate for a user that it is compulsory to carry out future logins only with a certificate or can also allow both options (user name/password and certificate).

The access responsible can display all «authorized certificates», and also of course revoke and manage these. Initially it is described how a new user (e.g. as a requester) is created.

The access responsible logs into the RA as administrator first of all.

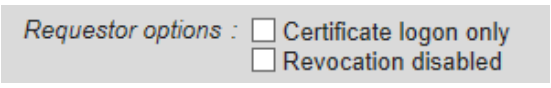
In the main menu the access responsible then goes to the menu item «Account» and selects the action «Create».



In the work area the access responsible now fills in the account details for the new account. These include:

- **User name under which the new user will soon log in.**
- **Password**
- **E-mail address of the user**
- **Optionally the telephone number**
- **Preferred language for the user guidance and for the e-mail communication (German /English)**
- **«Requester for»: Here it can be determined whether the user may also request within a selected RA certificate.**

As soon as the user may request certificates, the access responsible can determine other options here which expand automatically when selecting the buttons «Requester for»:



Certificate logon only: Security setting which prevents the user also being able to log in with user name/password apart from with the certificate.

Revocation disabled: The user is not allowed to revoke the requested certificates. In this case

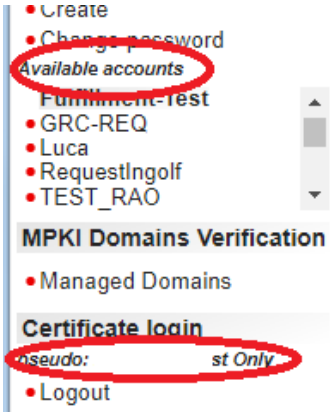
only the access responsible may do this.

Please note: When requesting certificates, the data is used from the account for notifications for the respective request. This means that the e-mail address and the certificate are automatically connected with the account if the requester does not explicitly change this.

3.6.2 Transferring requester role for existing account

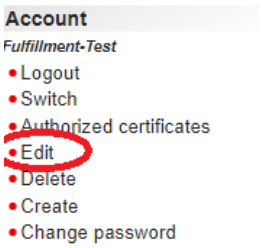
The access responsible logs into the RA as administrator first of all.

The access responsible now logs in under an account with user name/password or selects an existing account from the displayed overview under «Available accounts».

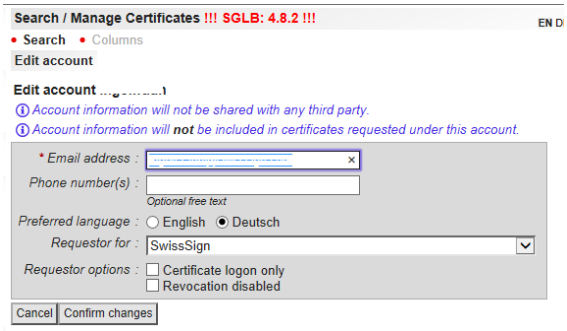


The selected account is then active if it is in bold and italics below the menu item «Account». In the adjacent example it is the account «Requestxxx».

Under the main menu item «Account» select the menu item «Edit».



In the work area the attributes of this account are now displayed. The attribute «Requester for» has to be changed by selecting the corresponding RA (if there are several). With the options the following checkboxes have to be selected optionally:



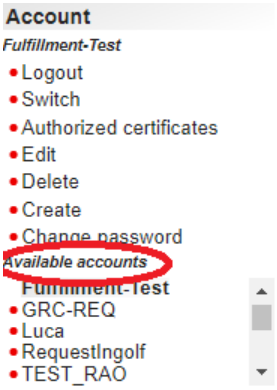
- Certificate logon only: Security setting which prevents the user also being able to log in with user name/password apart from with the certificate.
- Revocation disabled: The user is not allowed to revoke the requested certificates. In this case only the access responsible may do this.

3.6.3 Connecting an account with a certificate (for the login)

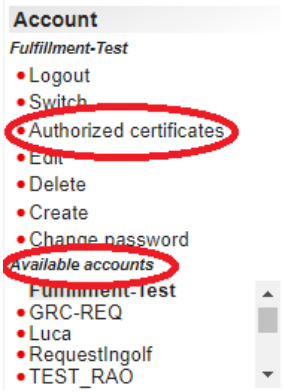
Especially for requesting certificates, the access responsible can specify for people who may request certificates that they may log in to the MPKI application only with a certificate (special configured RA operator certificates or level Gold or Platinum – SuisseID). The access responsible can also connect an MPKI account with several certificates so that holiday replacements etc. are possible.

Here the administrator has to connect an account with a certificate for the login process.

Initially the access responsible either selects the user under «Available accounts » or logs in to this account as access responsible.

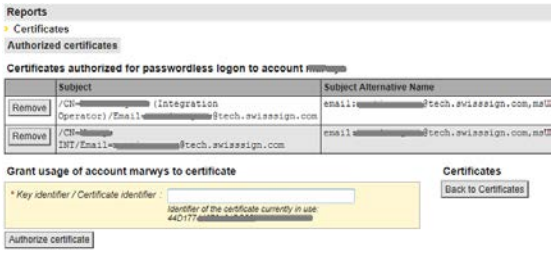


For this in the RA administration management there is the item «Authorized certificates» which is in the main menu on the left under «Account».



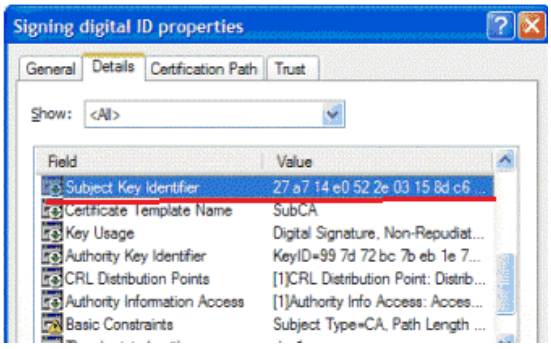
The tab «Authorized certificates» displays all certificates if these are already connected with an account.

A new certificate can be entered via the input field «Key identifier». Here the ID of the certificate has to be entered.



With the button «Remove» a certificate can also be removed from an account. The user then has to log in again with user name/password.

You can remove the key identifier from the standard certificate display of your operating system.



Please note: Basically the access responsible has access to all accounts within its Managed PKI. If another user also wants to have access to other accounts, the user has to integrate these individually via the function «Authorized certificates».

4. PKI processes and their representation in the software

4.1 Request process/requesting certificates

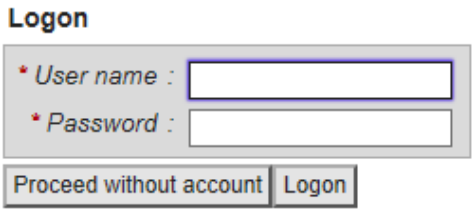
Every certificate request belongs to an RA. A certificate request is possible only with the certificate types stored and configured for this RA.

An MPKI customer of SwissSign can possess several own RAs under which different certificate types or domains are defined.

Users have to fulfil one of the following conditions to be able to make certificate requests:

- **Possession of a certificate voucher code (historically it was called "license" – the word will be used on some places in the GUI): Entry of a valid certificate voucher code. Certficate vouchers can be purchased in the SwissSign webshop and are generally not used by customers of a Managed PKI. Also the access responsible of a Managed PKI can generate certificate vouchers if this function is setup. A certificate voucher authorises a user to request a certain number of certificates – generally one single certificate. A certificate voucher determines a product and therefore an RA via which a request can be made. Certificate vouchers are normally used by requesters who request only one or two certificates. In this case it does probably not make sense to open for each requester its own account.**
- **The user is an access responsible (via certificate authentication)**
- **The user is an MPKI requester (via an MPKI requester account)**

When requesting as an administrator or user with an account, a login with password or certificate as described above is necessary.



If a certificate is purchased in the shop which should also appear in the management of the certificates of the Managed PKI, it must be ensured that this certificate is definitely requested with a user created by the Access responsible.

If someone is already logged in with another account (e.g. access responsible), it might make sense to log out first of all via the main menu and then to log into an account with which it is possible to request certificates. Or a new account can be created via the menu item «Create».

Simple users with a requester account must have the rights in order to request certificates.

Administrators can additionally use a separate account for requesting a certificate. This is not absolutely necessary, however. A separate

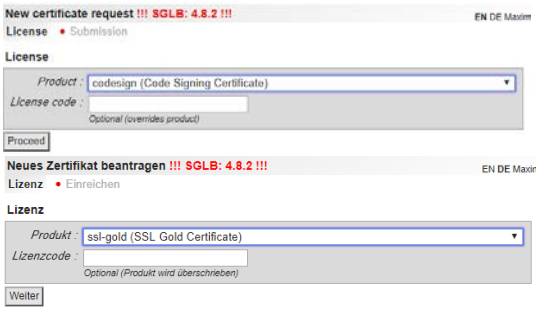
account offers the following advantages:

Account data (e-mail address, language setting) is transferred directly and added to the certificate as attributes when a certificate is created. This is not data which is contained in the certificate but rather, for example, allocated data such as the e-mail address to which expiry notifications regarding this certificate go.

It is possible to search for the certificates requested with an account on a targeted basis by using a filter (requester).

To request new certificates, the submenu item «New» has to be selected in the main menu on the left under the main item «Certificates».

Within the scope of the Managed PKI, in the work area under «Licence» you can select the appropriate certificate with the attribute «Product». If you have purchased a certificate voucher in the webshop, enter this under «Licence code ».



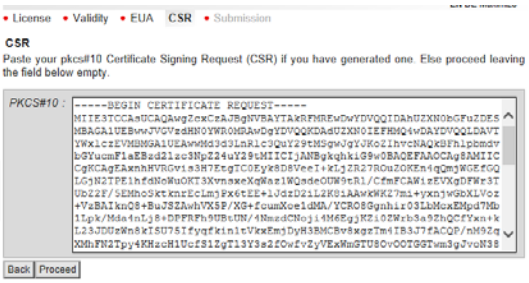
Please note: For users with a requester account it is only possible to select the products which have been activated for this account.

Depending on the certificate voucher or configuration the product is already preconfigured for a lifetime or can be configured in the next step.

In case the lifetime is not preconfigured you will be asked to mark the appropriate checkbox for the lifetime of the certificate. If the product is already preconfigured this step will be skipped.

In the work area the Subscriber Agreement now have to be read and accepted. To do this, press the button «I accept the above conditions». By selecting the word «Expand» the entire text of the Susbcriber Agreement can be read.

Optional: Enter certificate signing request (CSR). For the user there is the option of generating a key pair externally with the user's own tools (e.g. certtool.exe or OpenSSL) and requesting a certificate only for the public key. This request is done with a so-called CSR which these tools generate automatically. The CSR text generated by the external tool in PKCS#10 format has to be entered in the following field and the button «Proceed» must be selected. A typical signing request can be seen to the side.



If the user decides to have the keys generated by SwissSign, the field under PKCS#10 must be left empty and only the button «Proceed» pressed.

Please note: Alternatively the user can also commission SwissSign with generating the private and public key for the user. When generating the private key, this is immediately encrypted with a password which the user enters. SwissSign does not know this password and can also not recover it. It must therefore be stored carefully. If it is lost, all of the data encrypted with this key can no longer be read and no longer be used.

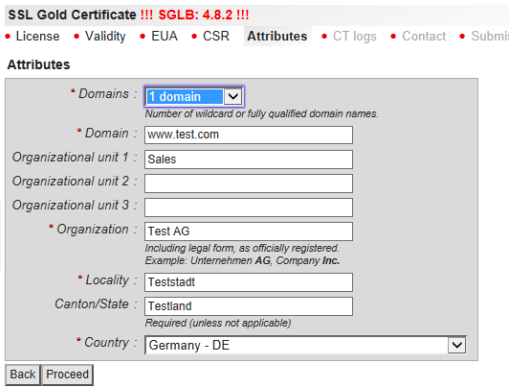
The SSL key pair generated by SwissSign remains on the platform for a short time (3 months). Key pairs for S/MIME personal certificates remain on the platform during their period of validity and can be downloaded again at any time by using the password.

The following steps now differ from certificate to certificate. The subchapters are therefore separated according to the certificate types.

4.1.1 Requesting SSL certificates

In the following the typical procedure when ordering SSL certificates is described.

In the work area the identity has to be filled in first of all: At first the certificate has to be allocated a domain name which will later also be in the subject of the certificate. The organisation in the case of a Managed PKI is preallocated, otherwise it can be entered with webshop users, for example. Location, if necessary canton/federal state and country with the headquarters of the organisation must be entered in the following fields. With Silver certificates only the entry of the domain name is obligatory. Afterwards the button «Proceed» must be pressed.



Hint: In case you request a wildcard certificate you have to enter in your domain name field a wildcard character as subdomain, e.g. "*.swisssign.com".

All mandatory fields are always indicated with a (*).

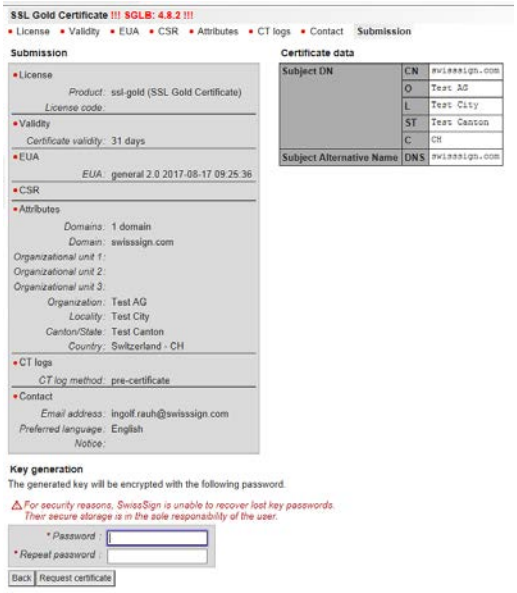
If you are logged in via Account, you will no longer be shown the displayed Contact view. In this case the contact data set stored in the account settings will be used as a contact. If you want to explicitly change this, however, you have to select the item «Contact» in the menu line at the top. The contact data entered here then overwrites the data stored in the account – but only for the certificate requested here.

Users without account login are automatically taken to this contact page and fill in the data e-mail address and preferred language. The e-mail settings affect notification e-mails informing that certificates will soon expire, for example.

The field “notice” {XE “Notice”} can be used for further administrative information to be backed up in combination with this request, like account number or device name, etc. This information will not be included in the certificate and will only be shown in reports.

Then the button «Proceed» has to be pressed.

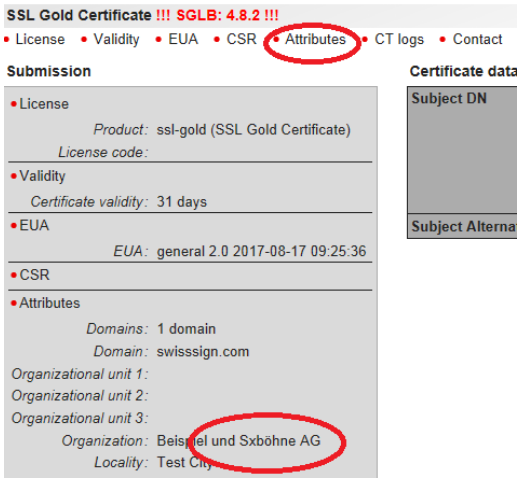
Now the certificate can be requested. All certificate data is shown again. If there are any errors, the previous menus can be selected again in the menu line at the top and the data can be changed. This can even been done in case the certificate data was entered with a CSR. In the event of key generation by SwissSign (no CSR was entered) a secure key must be entered in the password field for the transfer of the password. Then the button «Request certificate» must be selected.



If your certificate was not activated in the MPKI but instead you received a certificate voucher in the webshop, you will be asked in the case of Gold and Gold EV certificates to print out a request form and have this signed. In this the organisation and the belonged to domain must be confirmed.

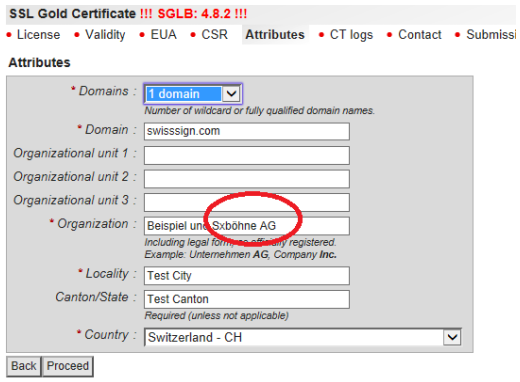
If you requested your certificate with the help of a CSR and the names used there contain an umlaut, you can see in the orange field under «Submission» whether the umlaut has been correctly interpreted. If this is not the case, you can correct the umlaut:

In the menu bar go back to the menu «Attributes».



The attributes displayed by you in the CSR have been allocated to the fields and can be edited. With «Proceed» you then go back to the recently shown «Submission» display.

Background information here: Umlauts are handled in certificates based on UTF-8 encoding (http://www.utf8-zeichentabelle.de/unicode-utf8-table.pl?start=128&number=128&names=-&utf8=string-literal). This means, for example, that a company name «Beispiel und Söhne» is encoded as follows in the background: «Test und S\\xc3\\xb6hne». The web interface does this without complication in the background, with CSR entries there can often be errors, however, depending on the quality of the CSR tool.



An SSL Silver certificate is requested in a similar way to the process described above:

In the work area only the domain name must be entered. It must be a fully qualified domain name and not an internal domain name or an IP address.

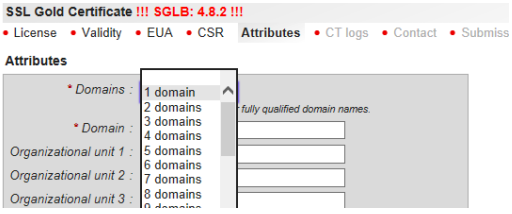
All mandatory fields are always indicated with a (*).

As far as you entered a domain containing “www” as subdomain you will be requested to include also the domain name without preceding “www” in the certificate (free of charge).

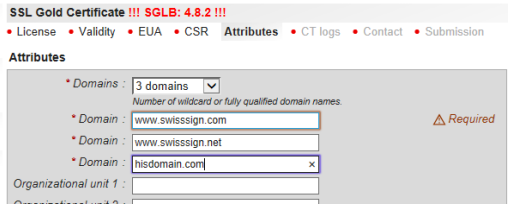
In case you have not requested a Silver SSL certificate designated within the framework of the MPKI but rather have used a certificate licence from the webshop, you will have to show the ownership/access control for this domain. For this you will be sent an e-mail to an e-mail account you indicated optionally which is connected with this domain.
The further procedure is then as with the SSL Gold certificate above.

A multi-domain certificate allows the entry of up to two hundred additional domains for one main domain:

The number of domains which will be included in the certificate in addition to the main domain must be selected.



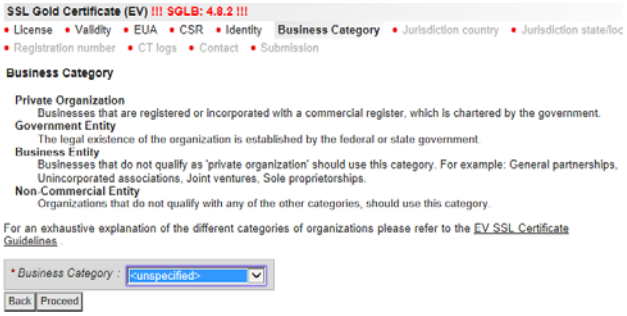
After the selection the input fields are displayed immediately and can be filled in accordingly. Please note: It is absolutely necessary that the organisation is also in possession of these domains or there is authorisation from the owner. In case of a MPKI the possible domains are pre-configured and can only be chosen by a dropdown menu.



The further procedure is then as described above.

With an SSL EV Gold certificate there are several particularities which still have to be borne in mind. Particular details are required as part of the certificate request:

After entering the certificate data the business category is still checked. This has to correspond with the entries in the commercial register or another register. Please have also a look to the description in www.swisssign.com (Product SSL EV) – Identity.

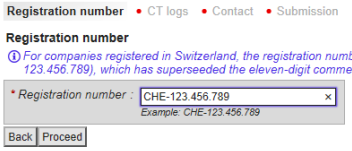


The country and, if necessary, province/canton/town where the organisation was registered must also be indicated.

Hint: the entered jurisdiction of incorporation and registration number must be unique. As far as the jurisdiction of incorporation is active on the locality level the locality must be entered together with the province and country. If the jurisdiction of incorporation is only active on the province level you have only to enter the province name. As far as the jurisdiction of incorporation is active countrywide the entry of the country is sufficient.

The corresponding registration number must be entered too. Please note that in Switzerland the new UID must be use.

The further procedure is then as described above.



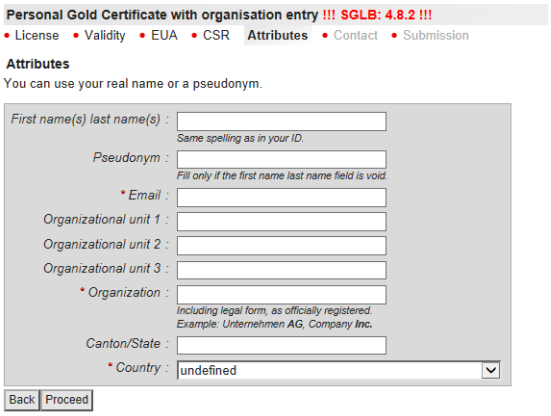
Please note: Secure passwords must be used for the keys generated by SwissSign. Insecure passwords (e.g. too short) must be confirmed explicitly. Passwords must be stored safely and must not be lost. SwissSign does not know these passwords and, if they are lost, cannot recover them either. The certificate and the data encrypted with it are then lost. Private keys of SSL certificates are also deleted after a short amount of time; these must be downloaded in sufficient time from the SwissSign system.

In case of a Managed PKI a lot of fields are already preassigned and cannot be changed. By this a compliant issuing is ensured.

4.1.2 E-Mail certificates (S/MIME)

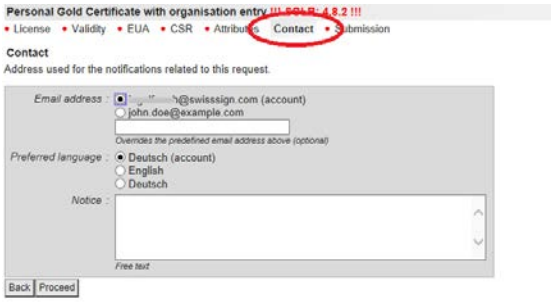
In the following the procedure for e-mail certificates is described:

In the work area the attributes for the e-mail certificate have to be entered. All required fields are indicated with an asterisk (*). In the case of a Gold certificate, first names and last names are entered. The use of a pseudonym is also allowed; in this case the field First name/last name must be left empty. It must be ensured that the names are used as they are also written in your own ID/passport. In the case of Silver certificates only the entry of the e-mail address is necessary, no person name will be entered. This has to already exist when the certificate is requested, however. Gold certificates with organisation entry are specified with the organisation here. Afterwards the button «Proceed» must be pressed.



Pseudonyms can be used for group accounts or anonymous mailboxes. It is at least important that somebody is responsible for this account. The name entered in the pseudonym field will be shown in the certificate as “pseudo: …”, e.g. if you enter “sales-mailbox” it will be shown as “pseudo: sales-mailbox”

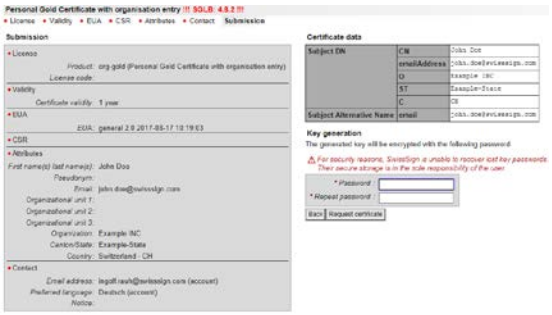
If you are logged in with an account, you will no longer be shown the displayed Contact view. In this case the data stored in the account settings will be used as a contact. If you want to explicitly change this, however, you have to select the item «Contact» in the menu line at the top. The contact data entered here then overwrites the data stored in the account – but only for the certificate requested here.



Users without account login are automatically taken to this contact page and fill in the data e-mail address and preferred language. The e-mail configuration affects notification e-mails informing that certificates are expiring, for example.

Then the button «Proceed» has to be pressed.

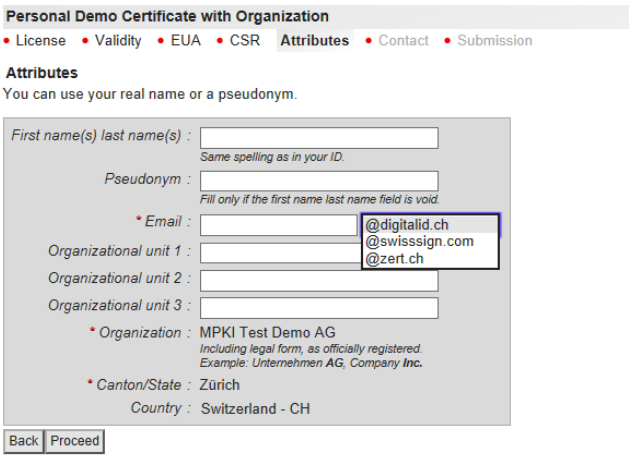
Now the certificate can be requested. All certificate data is shown again. If there are any errors, the previous menus can be selected again in the menu line at the top and the data can be changed. Otherwise in the event of key generation by SwissSign a secure key must be entered in the password field for the transfer of the password. Then the button «Request certificate» must be selected.



In the case of Gold certificates which were not obtained via the MPKI but rather via an additional webshop licence, the users are asked to print out a request form and have it signed. In this the organisation and the belonged to domain must be confirmed.

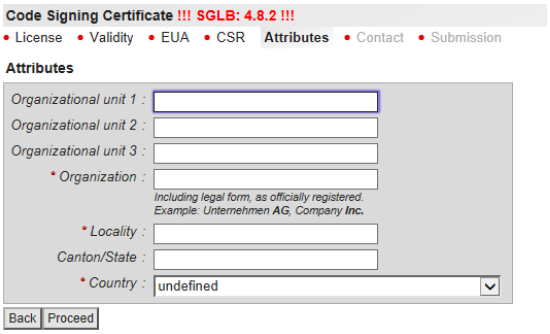
Please note: Secure passwords must be used for the keys generated by SwissSign. Insecure passwords (e.g. too short) must be confirmed explicitly. Passwords must be stored properly and must not be lost. SwissSign does not know these passwords and, if they are lost, cannot recover them either. The certificate and the data encrypted with it are then lost.

In the scope of a Managed PKI some fields are already preassigned, like the e-mail domain. This ensures the compliance during the request and issuing process.



4.1.3 Other certificate types: e.g. code signing certificate

Filling in is done like with the above examples. The CodeSigning certificate requires at least the entry of an organization and a country.



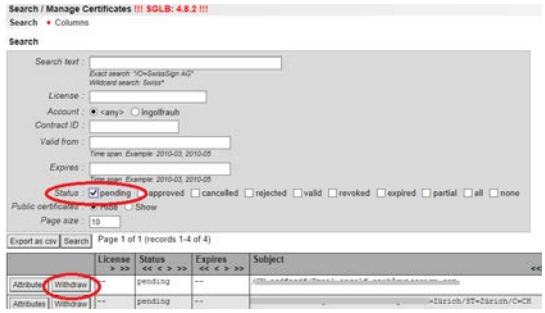
4.2 Withdrawing certificate requests

Certificate requests which, for example, were made by mistake can – as long as they have not been approved – be withdrawn. For this, it is necessary to search for the request of the certificate to be revoked first of all. Please note – the RAO can configure a requester account in a way that revocation of a certificate is forbidden.

In the main menu the menu item «Search/Manage» is selected.

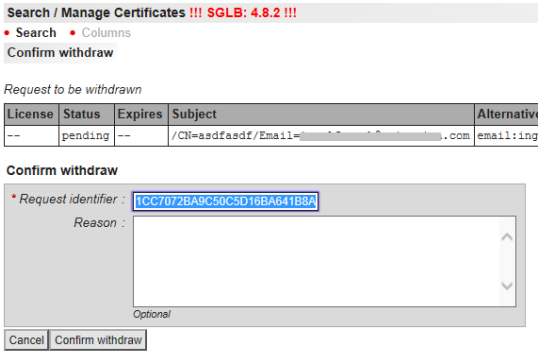
If no other search criteria are entered in the search field, all of your own requested certificates will be displayed. Users which have no account and which did request their certificate via certificate voucher have to enter their certificate voucher code into the field “License:”. By this they are afterwards entitled to change the certificate request or to revoke later the certificate.

Now you can find the certificate request and press the button «Withdraw».



In the following window the reasons for a withdrawal have to be entered (as free text).

Then the withdrawal has to be confirmed.



You will then receive a confirmation (also by e-mail).

Users which did their request by using a certificate voucher code can now reuse their code for a new request of the same certificate type.

4.3 Approval process

The certificate requests are then approved by the access responsible. The approval process is described further below.

4.4 Renewal process

As soon as a certificate expires it has to be renewed. A new certificate request according to the procedure described above has to be made in this case. There is (still) no renewal function which transfers the values of already issued certificates. It is recommended to issue the new certificate 1-2 weeks beforehand and to have it running alongside the expiring certificate. Within the framework of the Managed PKI, exceeding the certificate number by 10% is tolerated, in this respect this parallel use of two certificates within this period is not relevant for the billing.

4.5 Revocation process

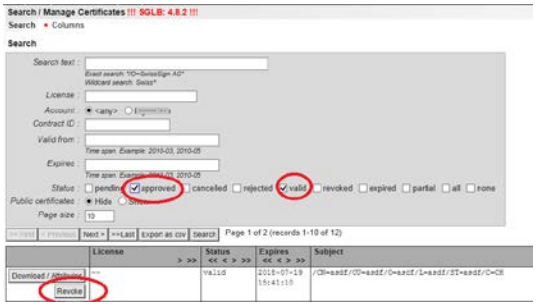
The requesters themselves can declare certificates invalid, i.e. «revoke» them. To do this, they log in under their login and search for the corresponding certificate.

In the main menu the menu item «Search/Manage» is selected.

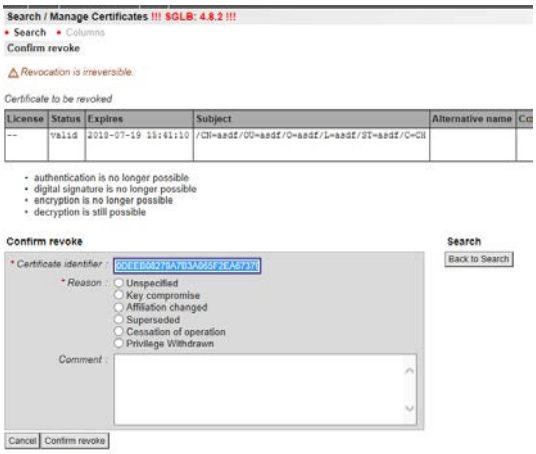
If no other search criteria are entered in the search field, all of your own requested certificates will be displayed.

Users which have no account and which did request their certificate via certificate voucher have to enter their certificate voucher code into the field “License:”. By this they are afterwards entitled to revoke the certificate.

Now you can find the certificate and press the button «Revoke».



In the following window the reasons for a revocation have to be entered:



- **Unspecified**
- **Key compromise: The private key has been stolen or there is the risk that it has been stolen.**
- **Affiliation changed: Subject information changed, e.g. change of company name or surname.**
- **Superseded: The certificate was replaced by another one.**
- **Cessation of operation: The certificate is no longer needed, e.g. an employee has left the company.**
- **Privilege Withdrawn: Authorisation revoked, e.g. on account of unpaid certificate licences.**

A comment can also be added optionally.

In case a voucher code was used for the revoked certificate the voucher code cannot be reused again after revocation.

Please note: A submitted revocation cannot be reversed. The certificate is indicated as invalid in all lists (CRL) or services (OCSP) used for a certificate validity enquiry.

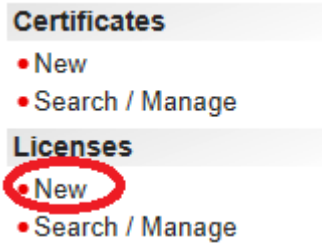
5. Certificate voucher Management

5.1 Issuing of Certificate vouchers

An access responsible has the possibility to issue certificate vouchers for a certificate request. This may be helpful for users who do not have a requester account. Users can use certificate vouchers with or without any account on the swisssign.net platform.

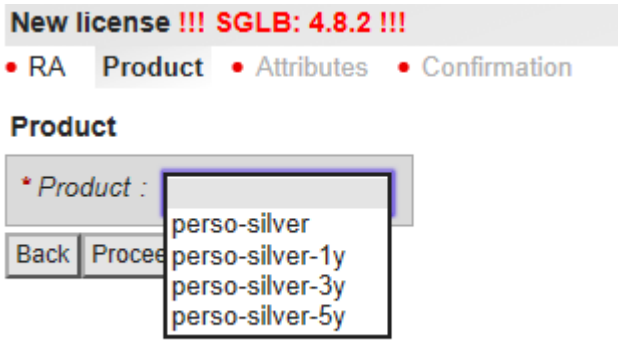
Hint: The CA software used historically the Anglo-Saxon word “license” instead of certificate voucher or certificate voucher code. The word license confuses with the term used in customs obligations and laws. In these documents often usage of software or use of an artificial work is mentioned. SwissSign will exchange the word “license” by “certificate voucher” or “certificate voucher code” in the future releases.

First the RAO selects the menu item „New” in the sub menu “Licenses”.



As far as the Managed PKI is configured for multiple RAs you have to select first the RA which is responsible for the product.

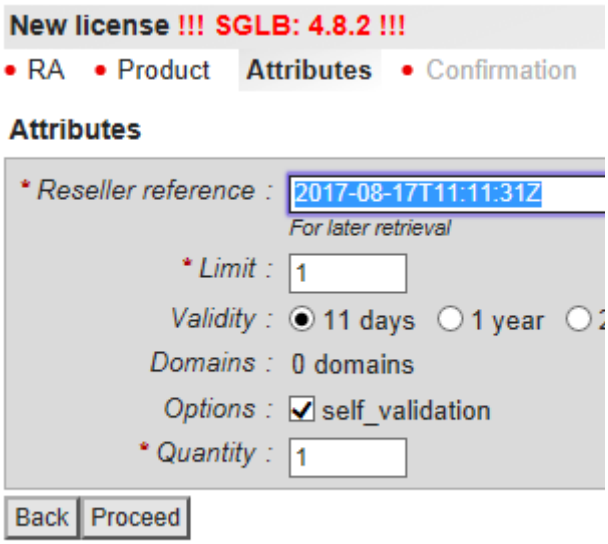
Afterwards the voucher product must be selected.

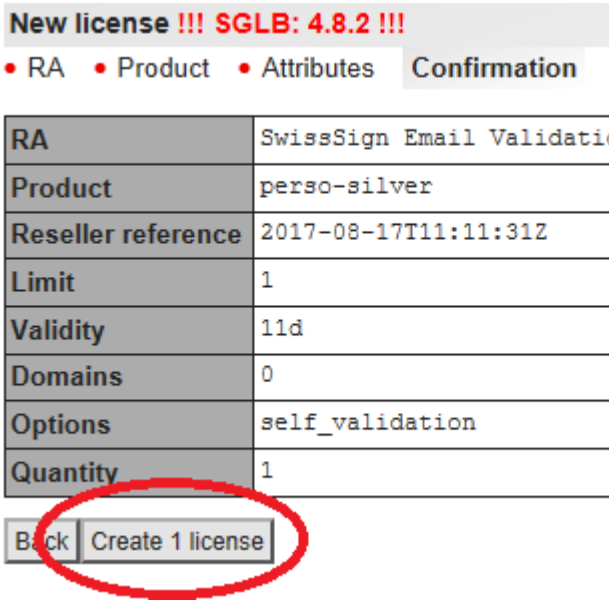


Data must be entered for the certificate voucher:

- **Reseller reference: An arbitrary self-chosen string for administration and billing of the issued certificate voucher.**
- **Limit: Usage limit. How many times the same certificate vouchercode may be used. By this a permanent certificate voucher can be created, e.g. which can be used 50 times.**
- **Validity: validity of the certificate (as far as not preconfigured by the product)**
- **Domains: can only be configured for a multi-domain certificate. Up to 200 domains are possible.**
- **Options: these should not be changed! The options are: multi_sld: only for multi-domain certificates. If not activated only subdomains of a main domain are allowed.**

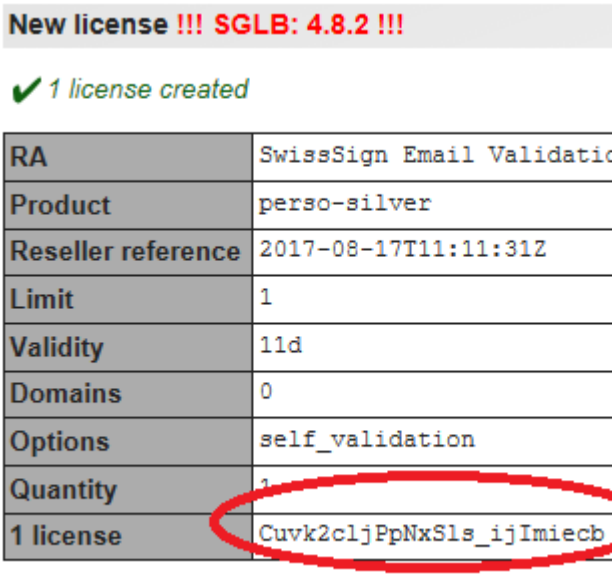
  self_validation: allows self-validation of Personal ID certificates (Silver).
  wildcard: allows wildcard entries in SSL Gold and Silver certificates.
- **Quantity: number of certificate vouchers to be created.**





Press „Proceed“ and „Create 1 certificate voucher“ in order to create a new certificate vouchervoucher code.

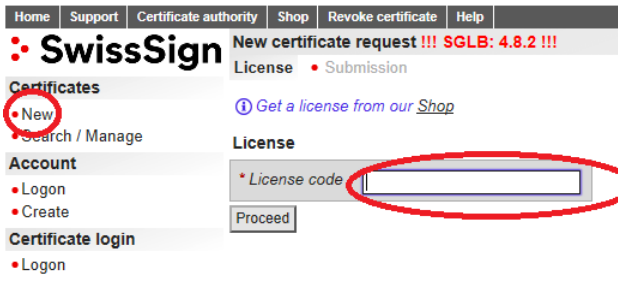
The certificate voucher displayed in the line of “1 license” can now be sent to an arbitrary user who wants to redeem the certificate vouchercode for a certificate request.



5.2 Redeem a certificate voucher

An arbitrary user has now the possibility to use the generated certificate voucher with or without an account on swisssign.net.

A user can select the menu item “New” in the submenu “Certificates” and enter the voucher code. In case the request should be changed later on or some information for the certificate has to be changed (e.g. e-mail address to be informed at the end of the validity) or in case of revocation the user must use the “Search/Manage” functionality in combination with this voucher code

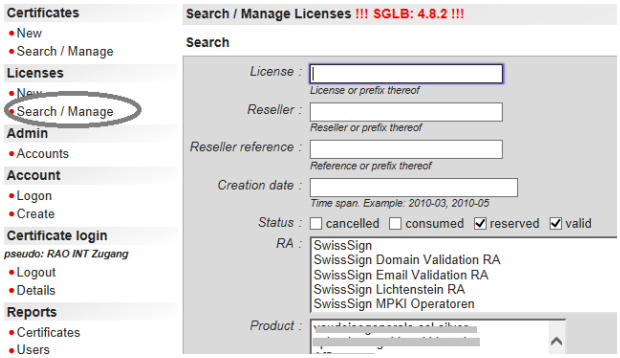


Even as a user with account or requester account within a Managed PKI can use the certificate vouchercode.

5.3 Search for certificate vouchers and administration

Access responsible and auditor have the possibility to manage issued certificate vouchers or to search for issued certificate vouchers.

You have to select „Search/Manage“ in the sub-menu “Licenses” of the main menu. The following criteria can be used for the search:



- Certificate voucher: Search for a certificate voucher code. It is sufficient only to enter the first letters of a code. A wildcard symbol is not necessary.
- Reseller: reseller’s ID (prescribed by SwissSign)
- Reseller reference: Search for a reference which was entered by the issuer of the certificate voucher. Also here the first letters can be sufficient.
- Status: Status of a certificate voucher:

  cancelled: Certificate voucher which was cancelled and which is no longer valid.
  consumed: certificate voucher which was already used for a certificate request and the corresponding certificate was already issued.
  reserved: certificate voucher was already used for a certificate request but the corresponding certificate voucher was not yet issued.
  valid: valid certificate voucher, not used before.
- Product: corresponding certificate product.

The result table shows all issued certificate vouchers. Certificate vouchers can be withdrawn with the “withdraw” functionality.

The titles mean the following:

- License: generated certificate voucher string
- Status: one of states mentioned before
- Usage: The third number indicates how many times a certificate voucher may be used. The first number indicates the number of certificate vouchers in the status “reserved”, the second (middle) number indicates the number of already used certificates.
- Product: corresponding product of the certificate voucher
- V: validity in years (y), months (m) or days (d)

- **D: number of domains**
- **O: options according to Fehler! Verweisquelle konnte nicht gefunden werden.**
- **Reseller: the reseller ID**
- **Ref: The chosen reference string**
- **RA: corresponding registration authority**
- **Created: when the voucher code was created**
- **Changed: last change of the voucher data set**

6. Management of certificates

6.1 Selection of rights

Certificates can be managed depending on the selected user role. A user without a login also has options for searching for public certificates, for example. The following overview shows the options:

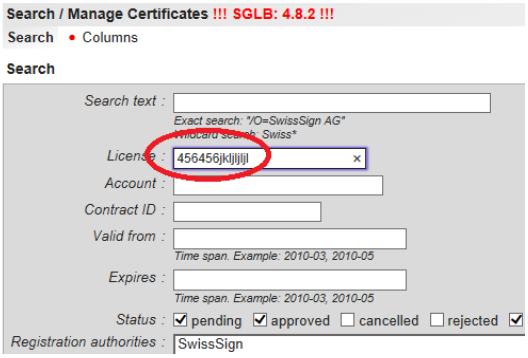
Rights	Options
Without login	• **Search for public e-mail certificates** • **Display results** • **Display certificate attributes** • **Download certain certificates for the encrypted e-mail communication**
Login as a user who is not an administrator	• **Search for own certificates** • **Display results** • **Display certificate attributes** • **Download own certificates if the person has the requester role.** • **Change attributes of own certificates** • **Download keys generated for oneself with password**
Login as access responsible	**All functions which are described in the following subchapters.**

Please note: If an access responsible wants to run another account, it has to explicitly log out first and then continue with the account (including login).

6.2 Search for certificates

In the main menu under the label «Certificates» the menu item «Search/Manage» is selected.

In the work area it is now possible to search for a certificate voucher or alternatively for a text which contains a certificate. The wild card character «*» can be used in the latter case.



Depending on the role, more search attributes can also be provided, e.g. the status of the certificates or certificate requests (e.g. «pending»).

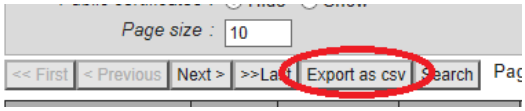
The number of results is limited to the number of certificates set under «Page size». The number can be changed.

Without entering search criteria, your own certificates will be displayed.

Please note:

- Changing the number of results (page size) to large numbers may result in a long time before the results of the query are displayed. If you want to export the results later (e.g. to Excel), only the displayed results will ever be exported. It may be recommended in this case to raise the number of displayed results so that all result data sets are displayed. These can then all be exported to Excel.
- The search for public certificates is always restricted to the display of the certficates for the corresponding complete e-mail address entered.

Issued data sets can be exported under «Export as csv» and imported to Excel, for example.

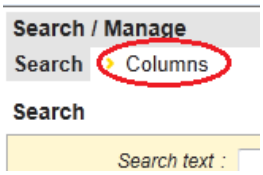


6.3 Display results

The display of individual attributes for a certificate can be controlled and determined easily:

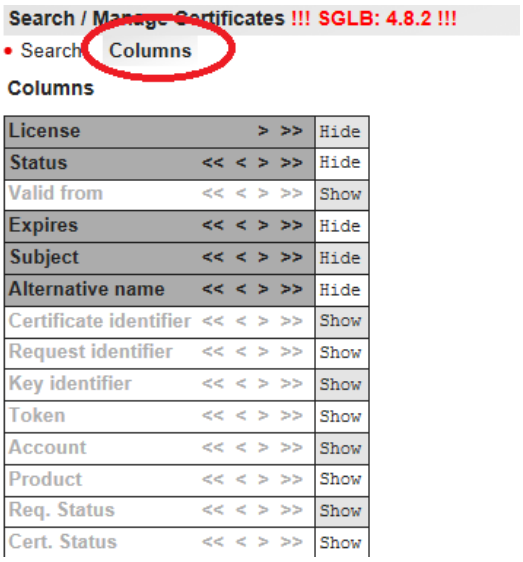
If you are not already in the «Search/Manage» menu, select this in the main menu under «Certificates», menu item «Search/Manage».

In the menu bar at the top select the menu tab «Columns».



You will now see a table of attributes with, on the right, a button «Show» or «Hide».

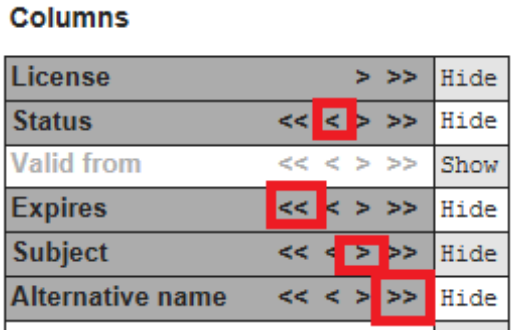
Those attributes which are currently displayed in the table of results for the search are shaded in grey and selected. The other possible attribute values are shaded in white and not selected.



Attribute columns in the list of results can now be switched on or off by pressing the button «Show» or «Hide».

Via the arrows «<» or «>» columns in the table of results can be moved one position to the left or right, like in the attribute list above.

With the double arrows «<<» or «>>» a column can be moved specifically to the left or right end of the table.



By selecting the right attribute an individual report of all own certificates is possible.

6.4 Approval, issue, rejection and revocation

An Access responsible has the task of approving or rejecting certificate requests. This is done according to the rules specified with SwissSign in the Declaration of Consent to the Delegation of Registration Authority Activity, e.g. when checking the person for whom the certificate is going to be issued. If the certificate request is approved, the certificate can be issued. If the certificate is no longer valid or has been compromised, it must be cancelled («revocation»).

First of all it is necessary to search for the certificates for which corresponding actions have to be initiated.

For example, for the process of approval or rejec-

tion all pending certificate requests can be selected. In this case the checkbox «pending» must then be selected, for example. Alternatively you can also use the links below of the search mask for typical frequent usages:

- Request to be authorized .....

For the revocation it is possible to search for specific certificates with a specific subject description.

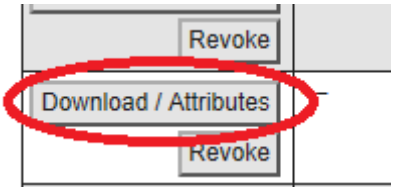
As well as the certificates in the list of results, the individual action buttons are now also displayed. In the adjacent example, for instance, a certificate can be revoked. Only the actions which are possible for the certificate are permitted. For example, only one certificate request can be approved. Certificates for already approved certificate requests can be issued so that the user can download them. Basically certificates can also be downloaded or the attributes of a certificate can be viewed.

Download / Attributes Revoke	--	valid
Issue Reject Attributes	--	approved

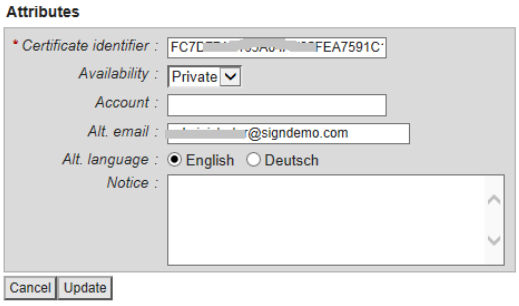
All certificates with the availability «Public download» can be displayed by any users and downloaded without a private key (e.g. e-mail certificates). Other certificates are not visible for unauthorised users.

6.5 Displaying/changing attributes/availability, downloading, transferring certificates

Afterwards it is possible to change some attributes associated with the certificate. To do this, the button «Attributes» has to be selected first of all in the list of results.



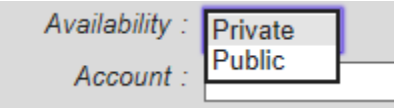
Then in the work area under «Attributes» settings can be made:



- The e-mail for the notification 10 or 30 days before certificate expiry can be changed for this certificate under «Alt. email», including the corresponding language under «Alt. language» (alternative language).
- The notice field can be used for arbitrary notices like the description of the associated device or the device responsible or an account number.
- The availability of the certificate in the swisssign.net certificate directory can be changed via a pick list.

If there are several accounts, the certificate can also be allocated to another account in this way. The corresponding checkbox for the account must then be selected.

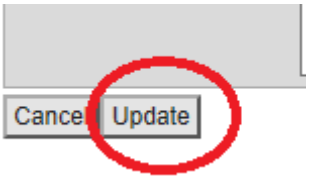
The availability can be changed to two values:



- Private
- Public

In the case of «Private», your certificate will not be displayed for outside users on swisssign.net. In the case of «Public», your certificate can be checked for validity by others. and is visible for everyone via the search or via LDAP request.

All changes must be concluded by pressing the button «Update».



7. CAA (Certificate Authority Authorization (RFC 8659)

SwissSign supports the CAA standard. If you configured your DNS entry that only certificates issued by another CA are accepted the certificate will not be issued by the SwissSign CA. Please refer to our FAQ section on www.swisssign.com how to configure CAA.

8. LDAP configuration

SwissSign also provides information about the certificates by using the "LDAP" service. The standard LDAP interface is used by many mail applications (for example, Outlook) and thus enables automated signature or encryption if the communication partner has a certificate with SwissSign and has enabled it for public search as shown in the previous section.

When configuring LDAP, refer to the instructions for your e-mail application. Enter the following setting parameters:

Servername: directory.swisssign.net

Port: 389

Search base: o=SwissSign,c=CH

9. Management of domains

As access responsible, you have the option to request new main domains for the Managed PKI as part of the procedure approved by the CA Browser Forum. They will be checked automatically by SwissSign.

The following procedures are permitted to check your access to the named main domains:

a. TXT Check
   You deposit a secret in a file with the path and name:

<domain>/.well-known/pki-validation/swisssign-check.txt
(no forwarding allowed)

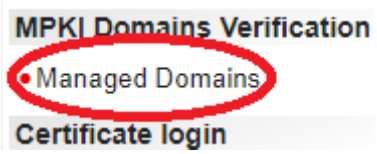
b. DNS entry
You deposit a secret in a TXT record of your DNS entry as follows:
"swisssign-check=*<random value>*"
(no forwarding allowed)

Within the scope of the automatic procedures described, the system checks for 30 days whether you have deposited the secret using one of the above-mentioned procedures. As soon as one of the tests is successful, the domain is automatically added to your Managed PKI. You can then issue e-mail certificates and SSL certificates for this domain and its subdomains.

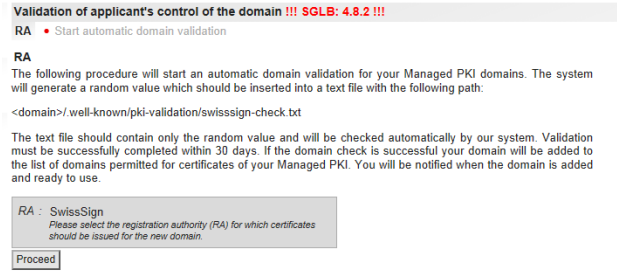
Please note that domain validation must not only be performed after an initial registration, but also periodically (at least every 13 months at Extended Validation level, otherwise at least every 24 months).

Please log in as access responsible.

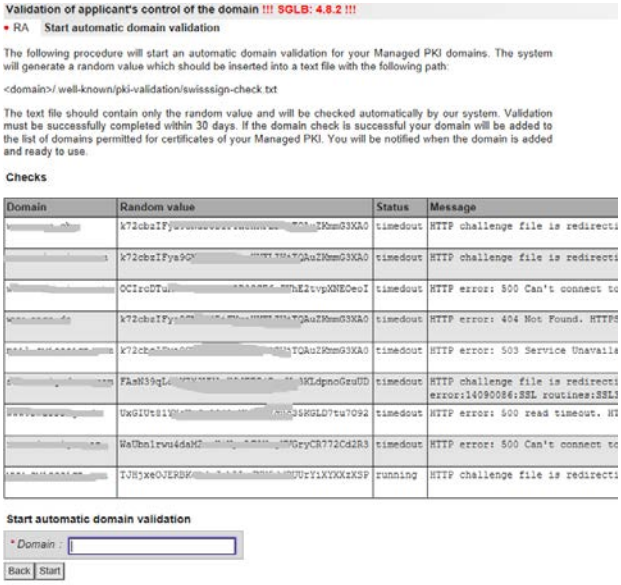
Call the menu item „Managed Domains“ within the MPKI Domains Verification section of the main menu.



The domain check is briefly described again. By activating the "Proceed" button, you enter your domains.



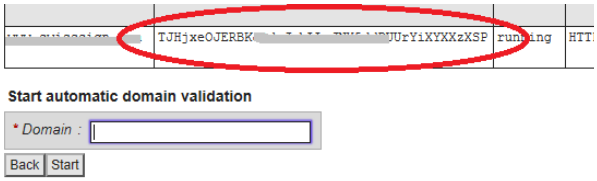
Please enter now the main domain names you want to add to your Managed PKI. After authorization and setup also the subdomains can be used within the Managed PKI.



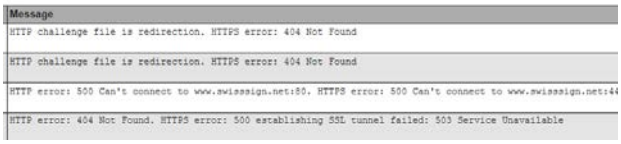
You will see a secret that you can insert into a swisssign-check.txt file without further additions. The file or page must be under

<Domain> /. Well-known / pki-validation

and accessible from outside through SwissSign. Alternatively, the secret can also be inserted into a TXT record of your domain name services (DNS). The form "swisssign-check=<secret>" has to be selected.



You can see from the status message whether the automatic check was successful or if there are problems probably due to firewall or access restrictions. Possible problem messages and times of the last check will help your and the SwissSign support in case of domain check problems.



As soon as the domain has been subjected to a last check and has been activated for your Managed PKI, you will receive an e-mail. The domain can now be selected as part of the managed PKI when ordering a certificate.

10. Reports

These reports can only be generated by the access responsible or auditor.

10.1 Certificates

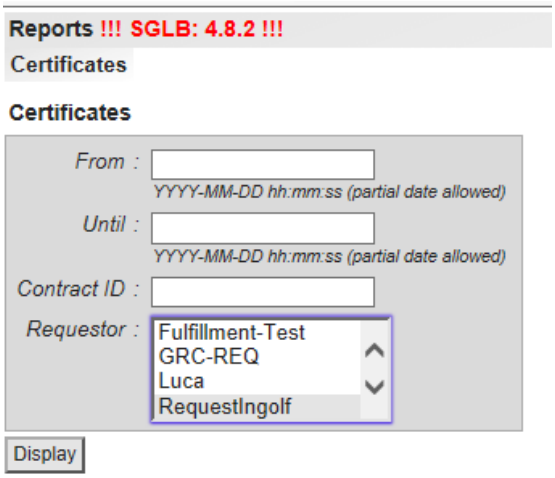
Log in as access responsible or auditor.

In the main menu open the evaluation «Certificates».

The evaluation is now displayed. It can be parameterised via the search window.

The following parameters can be entered:

- **From: beginning of observation period, just the date (without the time) is also permitted.**
- **Until: observation period end**
- **Affected RA**
- **Contract ID: The ID of the contract (was assigned by SwissSign)**
- **Requester: certificates of a requester are displayed.**



The menu item «Certificates» in the main menu / Reports gives a report of the following parameters:

- **Years: Observation period for the evaluation. An evaluation over half a year displays 0.5 here, an evaluation over a year 1.0. As standard without parameterisation, the evaluation is always displayed from the first day of the current month in the past year up to the first day of the month in the current year.**
- **Contract ID: ID of the contract (was assigned by SwissSign)**
- **RA: Registration Authority**
- **Requester: This column displays the requester. If the certificates were requested by the administrator, the entry remains empty.**
- **Product: Here the certificate product including the period of validity is displayed, e.g. personal-silver-1y for a Personal Silver ID certificate with a period of validity of one year.**
- **Product description: description of the certificate product according to the commercial order of the contract.**
- **Options: product options (like ability for multi-domain, wildcard possibility, etc.)**
- **Validity: Term of validity of the product**
- **CA: This is the CA which issued the certificate.**
- **Valid: Number of valid certificates on the last day of the observation period.**
- **Effective: All certificates are multiplied by the time period in which they were valid within the observation period and divided by the observation period. Example: If you had 10 certificates on 1 January of a year and 10 more half a year later, this gives the effective number of 15 certificates over the observation period 1.1. to 31.12 of the year. This calculation is used as the basis for any subsequent charging. In this respect, certificates issued during the year are not fully included in subsequent charging.**
- **Domains: Number of requested domains**
- **Issued: Number of certificates issued in the observation period.**
- **Expired: Number of certificates expired in the observation period.**
- **Revoked: Number of certificates revoked in the observation period.**

10.2 Users

Under the menu item «Reports/Users», users at the same authorisation level and lower authorisation levels are displayed with the respective rights. The item is visible only for logged in access responsibles.

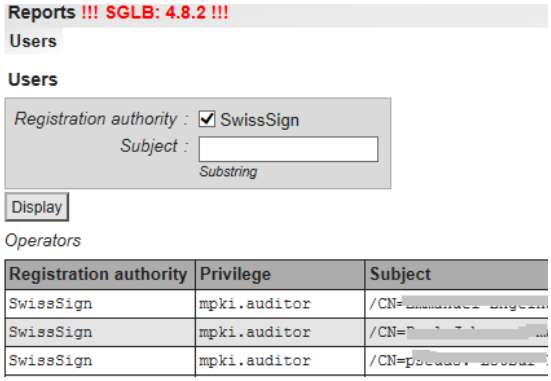
This evaluation can be started via the main menu item «Users» underneath «Reports»

The evaluation shows all users of the same or lower hierarchy level of an RA. You see

- **for which «registration authority» (RA) this user has been entered,**
- **what the user's authorisations are,**
- **what the status is,**

and the certificate necessary for the certificate login is displayed with key identifier and certificate identifier.

Operators are access responsibles and auditors, requesters are certificate requesters.



11. E-mail notifications

11.1 E-mail correspondence for certificate request by requester

For certain events the system generates e-mails which are sent to specific people. With the request of the certificate it has been determined who is the recipient of the e-mail of a certificate:

- **The certificate was requested under a specific account: The e-mail allocated to this account is used for all notifications regarding this certificate.**
- **The certificate was requested without an account: During the request process the contact data and therefore also the e-mail address for notifications about this certificate were determined.**
- **The certificate was requested as an access responsible: The certificate is then always connected with the role of the access responsible as requester, even if the access responsible has used a requester account. The access responsible e-mail is therefore used for notifications. If this is not wished, an access responsible has to explicitly log out and log in with user name/password or certificate of a specific requester.**

Excepted from these rules are so-called «proof of possession» e-mails – i.e. e-mails which check if the user has access to and control over a specific e-mail address. This occurs with certificates of level Silver which were not activated within the framework of a Managed PKI but whose licence was purchased in the webshop. With a Personal Silver ID certificate, the e-mail address which will be incorporated in the certificate is addressed directly. With a Silver SSL certificate the e-mail address indicated in the request is addressed.

Please note: Even when requesting from an account you are logged into, it is also possible to explicitly change the contact data connected with this request. This is described further above. See chapter 4.1

Please note: It is necessary to differentiate between the notification e-mail and the e-mails which are sent for verification of an e-mail or domain, e.g. to the e-mail address of the certificate holder. Here, unlike with all account settings or contact settings, the e-mail address of the certificate is always used or a message is sent to the access responsible of a domain if it is an SSL certificate. It must definitely be made sure that this e-mail address already exists if the certificate is being requested.

All e-mail notifications differ according to certificate type.

Typically there are the following events which lead to e-mails being sent. All e-mails are also additionally sent to the access responsible.

- **Request of a certificate: The recipient according to the account setting or contact setting for the certificate receives a confirmation e-mail. If required, the recipient has the option when purchasing the certificate in the webshop to download a necessary request document which is available by clicking on a link. The recipient also has the option to withdraw the request.**
- **After approval or rejection of the certificate by the registration authority: The recipient is sent an e-mail to the same address as when requesting a certificate. A link in the e-mail refers directly to the download page for the certificate.**
- **30 days before expiry of a certificate: 30 days before expiry of a certificate the recipient is sent an e-mail to the same address as when requesting a certificate, pointing out that the certificate is expiring.**

- **10 days before expiry of a certificate: 10 days before expiry of a certificate the user is told again about the expiry.**
- **Revocation: With a revocation of a certificate an e-mail is also sent, even if the user has carried out this revocation personally.**
- **Withdrawal of a request: If a certificate request has been withdrawn, this process is confirmed with an e-mail.**

Please note: If the e-mail address has changed and you want to allocate this to the already issued certificate, this is possible by making an attribute change for the certificate. See chapter 5.5.

11.2 Customer-specific e-mail notifications

E-mail notifications can be set to be customer-specific. For this there are template texts which can be adapted together with the SwissSign support team.

12. Support contact

For all questions the support team can be reached via helpdesk@swisssign.com or can be selected via the menu bar at the top:

13. Index