

## **Certificate Platform swissign.net**

### Instruction Manual

Glattbrugg, December 2014

## Contents

1.	Introduction	4
1.1	SwissSign	4
1.2	Objective and purpose of this document	4
1.3	Structure of this document	4
1.4	Requirements for using the SwissSign Managed PKI web service	4
2.	PKI processes and roles	4
3.	Control concept	6
3.1	Accounts	6
3.2	Certificate license	6
3.3	Structure of the user interface	6
3.4	Start and login on <a href="http://www.swissign.net">www.swissign.net</a>	8
3.5	Dealing with user accounts	10
3.6	Account management	10
4.	During license activation a csv/Excel file is shown	12
5.	Request certificates	13
5.1	Requesting SSL certificates	15
5.2	Personal certificates (S/MIME)	20
5.3	Other certificate types: e.g. code signing certificate	21
5.4	Organization certificate HSM	22
5.5	Organization certificate on smart card with USB reader	22
5.6	CSR entry and check	23
5.7	Withdrawing certificate requests	24
5.8	Approval process	25
5.9	Renewal process	25
5.10	Revocation process	26

6.	Management of certificates	28
6.1	Selection of rights	28
6.2	Search for certificates	28
6.3	Display results	29
6.4	Displaying/changing attributes/availability, downloading, transferring certificates	30
6.5	Create Request Form Again	31
6.6	Resend of proof of possession emails	31
6.7	Proof of Possession Email	32
7.	Authorization of the Certificate Request – File in the form	33
8.	Authorizations	35
9.	Download of the issued certificate	35
10.	E-mail notifications	36
10.1	E-mail correspondence for certificate request by requester	37
11.	Import Root and Intermediate certificates	38
12.	Support contact	39
13.	Typical Problems	39
14.	Index	42

## 1. Introduction

### 1.1 SwissSign

SwissSign AG is an internationally recognised issuer of digital certificates.

The SwissSign certificate platform [swissign.net](http://swissign.net) is used for issuing and managing SwissSign certificates. The advantage when using the platform 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 certificate platform service, customers can request, and revoke and also search for and manage certificates and pending certificate requests.

### 1.2 Objective and purpose of this document

This document shows how certificates can be managed with the Managed PKI service: request, , 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 signs the General Terms and Conditions 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.swissign.com/cpcps](http://www.swissign.com/cpcps)).

## 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 RA administrator.
- Approval of the certificate request by the RA administrator (RAO)

#### Certificate generation service

- Generation of the certificate

#### Revocation service

- Online revocation by the certificate holder
- Offline revocation by the RA administrator (RAO)

#### 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)

As far as no managed PKI service is used SwissSign takes over the role of the RA administrator (RAO).

The following table gives an overview of the activities and their representation in the swissign.net platform:

Activity	Role/who	Support by swissign.net
Certificate request	Requester/system administrators	GUI
Approval	RA administrator	SwissSign / Silver certificates via proof of possession email
Issue/generation	-	CA
Installation	Requester/system administrators	E-mail with download link
Revoke	Requester/system administrator, RA administrator	GUI
Renewal	Requester/system administrator, RA	Warning e-mail 10 days and 30

	administrator	days before expiry
Search/Manage	Requester/system administrator,	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 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 platform.

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 the user himself in order to redeem a license from the web shop.

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 obtained license for a specific certificate type. The license permits only the request of the certificate type the license was bought for. 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 RA administrators at SwissSign 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](http://www.swisssign.com).

#### 3.2 Certificate license

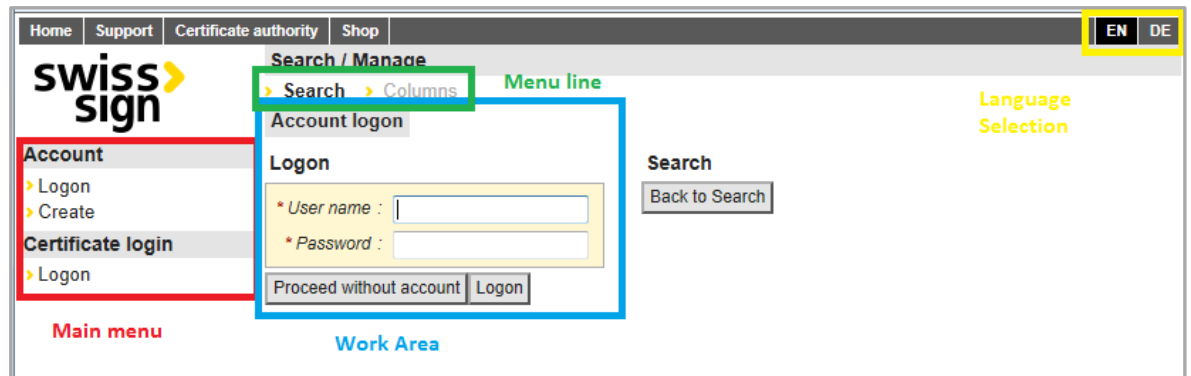
A certificate licence is a code which allows the user to request a corresponding certificate. The licence code can be typically obtained in the SwissSign webshop.

#### 3.3 Structure of the user interface

The user interface is divided into the following areas:

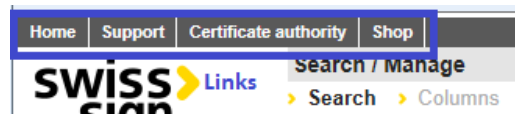
- Header section: General information and language selection
- Main menu
- Menu line
- Work area

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.



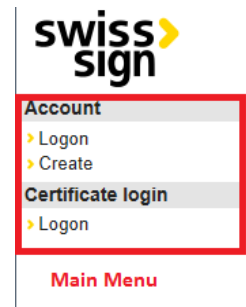
Special feature: With a button in the very top right the user can hide this bar completely (including the logo) to have a bigger working area.

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

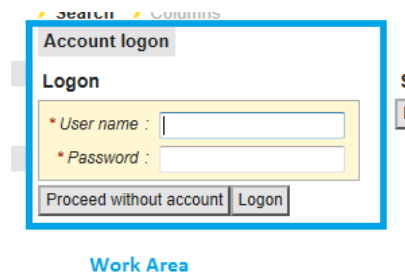


DE: User interface in German  
EN: User interface in English

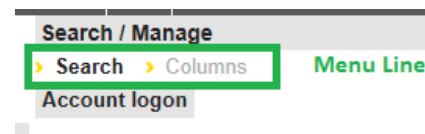
On the left is the main menu. Actions can be selected below the individual submenu headings.



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 parallel actions are possible. To control the work area accordingly, you can click on the buttons in the menu line above the work area.



### 3.4 Start and login on www.swissign.net

Users obtaining a license from the shop can decide if they want to continue with or without an account.

The use of an account offers different advantages:

- Management for multiple certificates is easier (reports, overviews, etc.)
- Revocation is easier
- Central site to download certificates

If you have clicked on a link in the swissign.com webshop you are automatically forwarded to the following page.

ID	PRODUCT	STATUS
1530	1-year Personal Gold Certificate without organisation entry	Reserved

You can now continue without account (“Proceed without account”), with login (“Logon”) or by creating a new account via the main menu on the left hand side (“Account -



Create”).

As far as you have not activated this link you can login at the platform with:

<https://web.swissign.net>

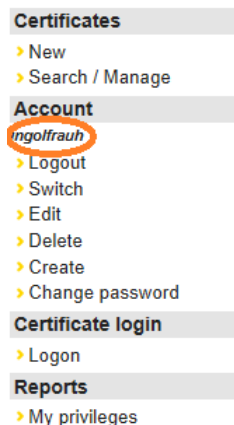
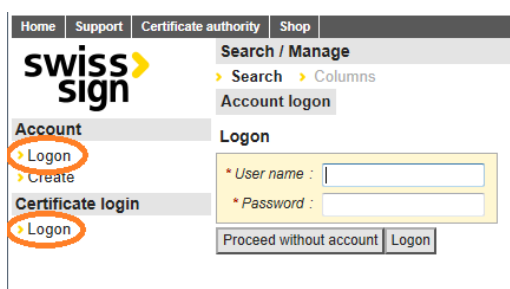
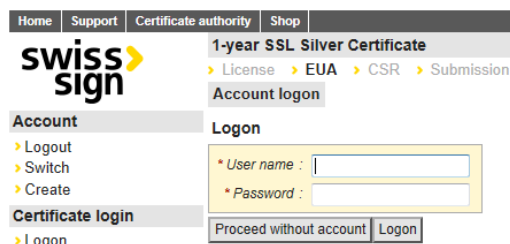
In this case an installed certificate is necessary.

Generally there are two options for logging in:

- Certificate login: This is only possible if you configured your account by authorizing a certificate logon (see below).
- Login with account and password.

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.



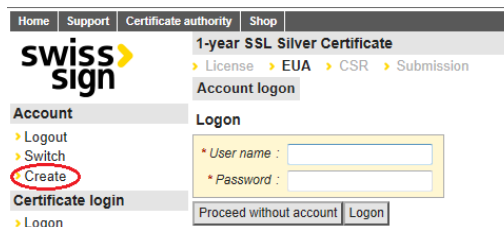
### Please note:

- 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, a profile session cookie (signed) is created. This is valid for 30 minutes.
- If you lost your password please contact our customer support.

## 3.5 Dealing with user accounts

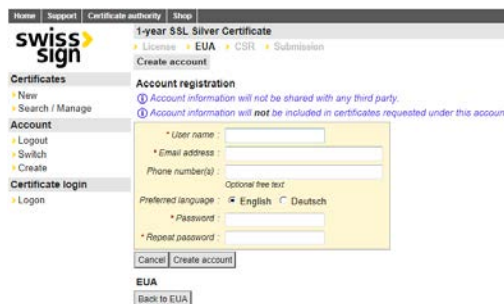
### 3.5.1 Creation of an account

A certificate requester can create an account if this does not already exist. He chooses the main menu item “Create” below the menu “Account”.



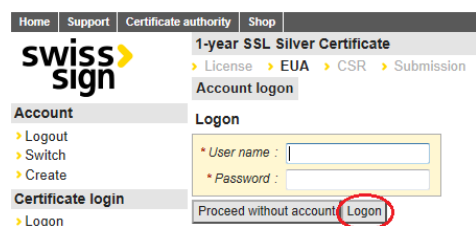
The user may now enter the attributes of his account.

He has to enter his email address which will be used for all notifications concerning his certificates independently from the email address which will be probably used in the certificate. The preferred language will be used in these email as well as platform language after login. A phone number can be entered optionally to ease the support of SwissSign.



### 3.5.2 Logging into the account

A certificate requester can log into the account set up beforehand by him. He enters the user name (account name) and password and clicks on “Logon”.



## 3.6 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 profile 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.

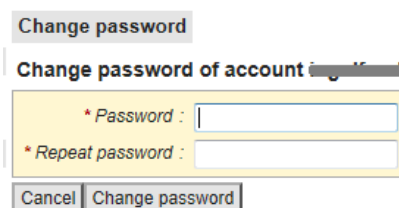
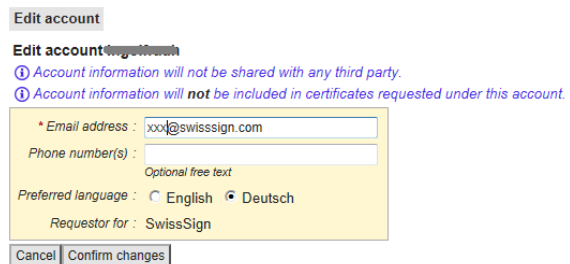
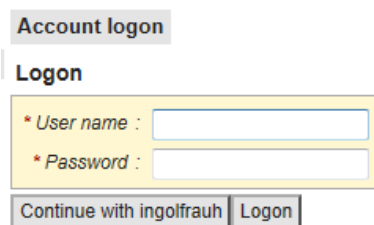
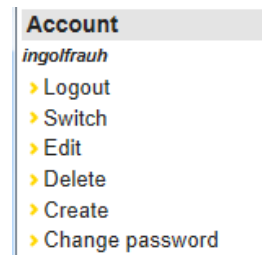
With «Switch» you can switch to another account by logging into this.

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 which will 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.

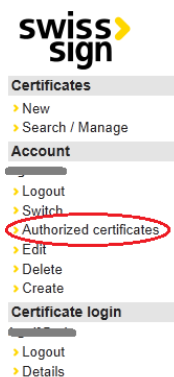
With «Change password » you change the password for an existing account.



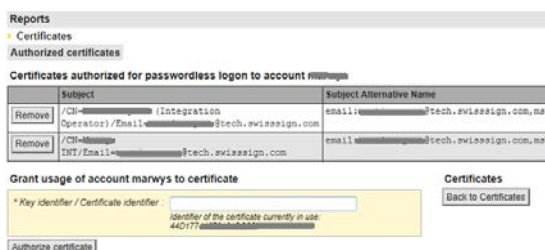
**Please note:** When requesting certificates, the data is used from the profile for notifications for the respective request. This means that the e-mail address and the certificate are automatically connected with the profile if the requester does not explicitly change this.

It is also possible to enable a certificate based access to this account by using the menu item "Authorized certificates". Afterwards you can directly login with certificate instead of using username and password. Please note that you need at least a Personal ID certificate which allows a secure login in its key usage like the SwissSign Gold Personal ID.

Please choose first the menu item "Authorized certificates".



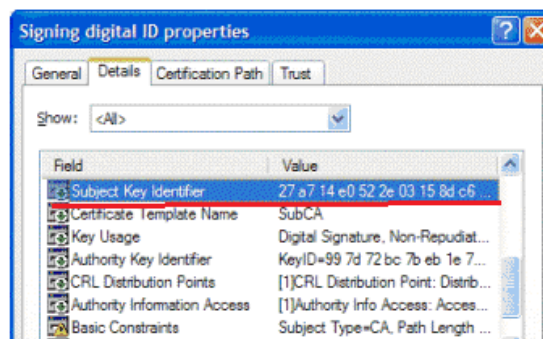
The tab «Authorized certificates» displays all certificates if these are already connected with an account.



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.



#### 4. During license activation a csv/Excel file is shown

Sometimes it happens that you activate the link you obtained via your reseller or you found in the license overview of the shop and the browser offers to you a download of a csv/Excel file with name "certificates.csv".

In this case a license key was used which was already redeemed for a certificate which is already issued.



The important attributes of this certificate are shown in the csv file:

	A	B	C	D	E	F
1	Status	Läuft ab	Subjekt	Alternativer Name	Anforderungsidentifikator	Konto
2	valid	10/10/2019 19:33	/CN=Email: [redacted]	email: [redacted]	9E27BF0C-7A50-4E77-92E1-C49D4A [redacted]	[redacted]

## 5. Request certificates

Every certificate request is based on a license code and the certificate types admitted by this license code.

Licences can be purchased in the SwissSign webshop. A licence authorises a user to request a certain number of certificates – generally one single certificate. A licence determines a product via which a request can be made.

The use of a user account is always recommended. Please log first in.

**Account logon**

**Logon**

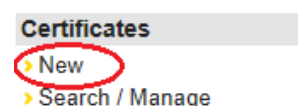
\* User name :

\* Password :

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.

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





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

## 5.1 Requesting SSL certificates

In the following the typical procedure when ordering SSL Gold 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 organization, locality, if necessary canton/federal state and country can also be entered in case of Gold certificates. With Silver certificates only the entry of the domain name is obligatory.

Afterwards the button «Proceed» must be pressed.

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.

Then the button «Proceed» has to be pressed.

**1-year SSL Gold Certificate**  
 > License > EUA > CSR > **Attributes** > Contact > Submission

**Attributes**

\* Domain :   
Fully qualified domain name of your server.  
 Example: www.company.com

Email :

Organizational unit :

Organization :   
Including legal form, as officially registered.  
 Example: Unternehmen AG, Company Inc.

Locality :

Canton/State :

Country :

Back Proceed

**1-year SSL Gold Certificate**  
 > License > EUA > CSR > Attributes > **Contact** > Submission

**Contact**  
 Address used for the notifications related to this request.

Email address :   
Overrides the predefined email address above (optional)

Phone number(s) :

Preferred language :  Deutsch (account)  
 English  
 Deutsch

Back Proceed

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 be 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.

In the case of Gold and Gold EV certificates you are asked to print out a registration 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».

**1-year SSL Gold Certificate**

[License](#) > [EUA](#) > [CSR](#) > [Attributes](#) > [Contact](#) **Submission**

**Submission**

> License  
 Product: 1-year SSL Gold Certificate  
 License code:

> EUA  
 EUA: gold 2.0 2014-12-01 12:31:23

> CSR

> Attributes  
 Domain: www.mydomain.com  
 Email:  
 Organizational unit:  
 Organization: SwissSign AG  
 Locality: Glatbrugg  
 Canton/State: Zürich  
 Country: Switzerland - CH

> Contact  
 Email address: [www@mydomain.com](mailto:www@mydomain.com) (account)  
 Phone number(s):  
 Preferred language: Deutsch (account)

**Certificate data**

Subject DN	CN	www.mydomain.com
	O	SwissSign AG
	L	Glatbrugg
	ST	Zürich
	C	CH
Subject Alternative Name	DNS	www.mydomain.com

**Key generation**  
 The generated key will be encrypted with the following password.

▲ For security reasons, SwissSign is unable to recover lost key passwords. Their secure storage is in the sole responsibility of the user.

\* Password :

\* Repeat password :

**1-year SSL Gold Certificate**

[License](#) > [EUA](#) > [CSR](#) > **Attributes** > [Contact](#) [Submission](#)

**Submission**

> License  
 Product: 1-year SSL Gold Certificate  
 License code:

> EUA  
 EUA: gold 2.0 2014-12-01 12:31:23

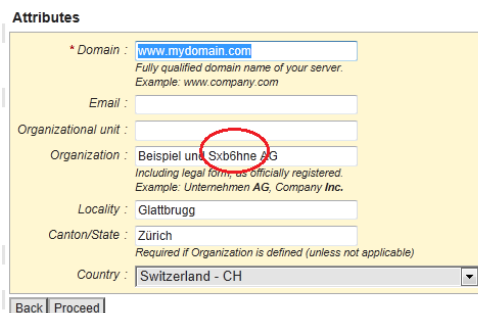
> CSR

> Attributes  
 Domain: www.mydomain.com  
 Email:  
 Organizational unit:  
 Organization: Beispiel un Sxb6hne AG  
 Locality: Glatbrugg



The attributes displayed by you in the CSR have now 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.

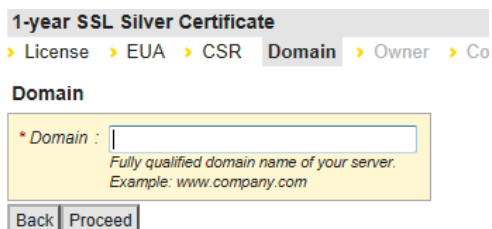


**Please note:** The organization of the certificate should be spelled exactly in the same way as it can be found on the trade registry excerpt. Also any additional organization forms should be spelled in the same way (e.g. “Inc.”).

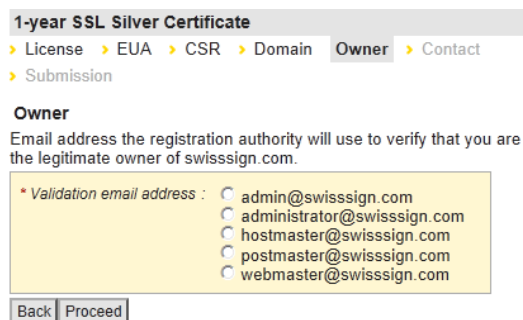
An SSL Silver certificate is requested in a similar way to the process described above:

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 (\*).



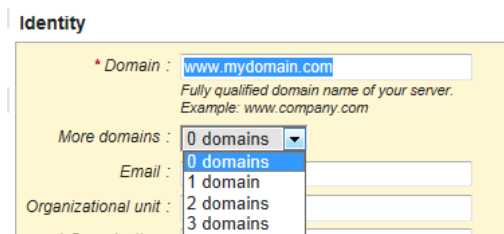
You will now have to show the ownership/access control for this domain. For this you will be sent an e-mail to an e-mail account you indicated optionally which is connected with this domain.



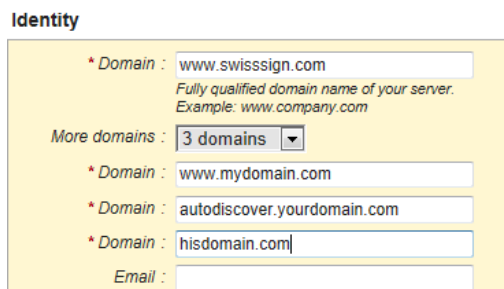
The further procedure is then as with the SSL Gold certificate above.

A multi-domain certificate allows the entry of up to twenty 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.

**1-year EV SSL Multidomain Gold Certificate**

[License](#) > [EUA](#) > [CSR](#) > [Identity](#) > **Business Category** > [Jurisdiction country](#)  
[Jurisdiction state/locality](#) > [Registration number](#) > [Contact](#) > [Submission](#)

**Business Category**

**Private Organization**  
 Businesses that are registered or incorporated with a commercial register, which is chartered by the government.

**Government Entity**  
 The legal existence of the organization is established by the federal or state government.

**Business Entity**  
 Businesses that do not qualify as 'private organization' should use this category. For example: General partnerships, Unincorporated associations, Joint ventures, Sole proprietorships.

**Non-Commercial Entity**  
 Organizations that do not qualify with any of the other categories, should use this category.

For an exhaustive explanation of the different categories of organizations please refer to the [EV SSL Certificate Guidelines](#).

Business Category :

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

**1-year EV SSL Multidomain Gold Certificate**

[License](#) > [EUA](#) > [CSR](#) > [Identity](#) > [Business Category](#) > **Jurisdiction country**

**Jurisdiction country**

Specify the country of the incorporating/registration agency of your organization.

\* Jurisdiction country :

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.

**1-year EV SSL Gold Certificate**

[License](#) > [EUA](#) > [CSR](#) > [Identity](#) > [Business Category](#) > [Jurisdiction country](#)  
[Jurisdiction state/locality](#) > [Registration number](#) > [Contact](#) > [Submission](#)

**Jurisdiction state/locality**

Jurisdiction state/province :

*Leave blank if the agency operates at the country level*

**1-year EV SSL Gold Certificate**

[License](#) > [EUA](#) > [CSR](#) > [Identity](#) > [Business Category](#) > [Jurisdiction country](#)  
[Jurisdiction state/locality](#) > **Registration number** > [Contact](#) > [Submission](#)

**Registration number**

Enter the registration number that was assigned to your organization by the incorporating or registration agency of your jurisdiction.

\* Registration number :

**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.

## 5.2 Personal certificates (S/MIME)

In the following the procedure for personal certificates is described:

In the work area the attributes for the personal 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. 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 profile – 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.

**1-year Personal Gold Certificate with organisation entry** EN DE Maximize

[License](#) > [EUA](#) > [CSR](#) > **Attributes** > [Contact](#) > [Submission](#)

**Attributes**  
 You can use your real name or a pseudonym.

First name(s) last name(s) :   
Same spelling as in your ID.

Pseudonym :   
Fill only if the first name last name field is void.

\* Email :

Organizational unit :

Organization :   
Including legal form, as officially registered  
 Example: Unternehmen AG, Company Inc.

Country :

**1-year Personal Gold Certificate with organisation entry**

[License](#) > [EUA](#) > [CSR](#) > [Attributes](#) > **Contact** > [Submission](#)

**Contact**  
 Address used for the notifications related to this request.

Email address :   (account)  
 john.doe@testcompany.com  
Overrides the predefined email address above (optional)

Phone number(s) :

Preferred language :  English (account)  
 English  
 Deutsch

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 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.

**1-year Personal Gold Certificate with organisation entry** EN DE Maximize

[License](#) > [EUA](#) > [CSR](#) > [Attributes](#) > [Contact](#) > **Submission**

**Submission**

> License  
*Product:* 1-year Personal Gold Certificate with organisation entry  
*License code:*

> EUA  
*EUA:* gold 2.0 2014-12-01 12:31:23

> CSR

> Attributes  
*First name(s) last name(s):* John Doe  
*Pseudonym:*  
*Email:* john.doe@testcompany.com  
*Organizational unit:*  
*Organization:* Testcompany AG  
*Country:* Switzerland - CH

> Contact  
*Email address:* martin.wyser@tech.swissign.com (account)  
*Phone number(s):*  
*Preferred language:* English (account)

**Certificate data**

Subject DN	CN	John Doe
	emailAddress	john.doe@testcompany.com
	O	Testcompany AG
	C	CH
Subject Alternative Name	email	john.doe@testcompany.com

#### Key generation

The generated key will be encrypted with the following password.

*⚠ For security reasons, SwissSign is unable to recover lost key passwords. Their secure storage is in the sole responsibility of the user.*

\* Password :

\* Repeat password :

**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.

### 5.3 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.

**1-year Code Signing Certificate** EN

[License](#) > [EUA](#) > [CSR](#) > **Attributes** > [Contact](#) > [Submission](#)

**Attributes**

*Email :*   
*Organizational unit :*   
 \* *Organization :* Testcompany AG  
Including legal form, as officially registered.  
 Example: Unternehmen AG, Company Inc.  
*Locality :*   
*Canton/State :*   
 \* *Country :* Switzerland - CH

#### 5.4 Organization certificate HSM

In case of an organization certificate (HSM) you must obligatory enter a CSR..

**1-year Organisation Platinum Certificate for HSM**

[> License](#)
[> EUA](#)
CSR
[> Submission](#)

**CSR**

Paste your pkcs#10 Certificate Signing Request (CSR).

\* PKCS#10 :

Back
Proceed

The further process is as described above..

#### 5.5 Organization certificate on smart card with USB reader

In case of an organization certificate on smart card with USB reader you will remain on the platform swissign.com and directly fill in all attributes of the certificate.

After clicking on your license link you will be redirected to the form. You have to fill your title, first name, last name, name of the organisation (please use the same spelling and organization form as used in the trade registry excerpt), the country of the organization (main site), the canton or province and the location (place). Please note that the details highlighted in yellow are used in the certificate later.

Please fill in an email address. Please note that this email address will also be used for all notifications for this certificate in contrast to the email address of the swissign.net account. The email of the swissign.net account is not used.

If you perform a signature service as a

✓ Type of certificate	1-Jahr Organisationszertifikat
✓ Period of validity	1 Year(s)
✓ Reader	With USB Reader

Please complete the fields below correctly and then, click "Next".

The fields marked with a \* must be filled in.

The information entered in the certificate and checked by us is highlighted in yellow.

Check the help by moving the mouse over the blue information mark for the fields first name and surname in particular.

**Application data**

Title*	Mister
First name*	Hans
Surname*	Mustermann
Name of the organisation*	SwissSign AG
Organisation details, part 1	
Organisation details, part 2	
Country*	Switzerland
Canton*	Zürich
Place*	Zürich
E-mail address*	hans.mustermann@swissign.com
E-mail address confirmation*	hans.mustermann@swissign.com

Third Party Services  Yes

third party for the organization announced in the certificate please tick the checkbox at third party services.

The delivery address is used for all communication concerning your purchased certificate. It could differ, e.g. in case of a third party, from the address details entered in the certificate area above.

Delivery address	
Company	SwissSign AG
First name*	Hans
Surname*	Mustermann
Address 1*	Sägereistrasse 25
Address 2	
Postcode and town*	8152 Glattbrugg
Country	Switzerland
Phone*	044 8383683
Korrespondenzsprache	Englisch

## 5.6 CSR entry and check

If you use a CSR the entries made are automatically checked against the rules of SwissSign concerning the certificate type, license type or regulations of the CP/CPS.

If the CSR does not match these rules the proposed change to the CSR is shown and must be acknowledged. Please note that the certificate will be requested based on these changes and the final displayed certificate attributes.

CSR  
⚠ Some attributes cannot be considered

```
*PKCS#10
MIICCAACCAQwIExpc2Aub29yYDAITAA9IHR1eEA1YVQ01DA1w#PcyRSpY2xk
CjAGbGVVRAcMCY9d9Rk5.cam1j=DEPMA0GA1UECgwGQ00JDIjPFRIRmRlPwFyVWQ0DAak
ZmZkdka0Vnfa+dMkEDASBghVBAhMCC3d3dy5hbnRlbnR5cHM3YVJAYj0kZllycCA0aG
PnduY9sLm13c3Rlcm1haW50aW50aW50aW50aW50aW50aW50aW50aW50aW50aW50aW50
A0CCA0Cg9kRAK493ya990ka/kkZnJh8B803/3Wd8BENT3c44/3De2G0Lh+33/y
#RdumR1ka206Lh1RKO7F006g33TOY3mcam9/kN5p5Fnnm23u4N0Mx108n4e33f
d8eE88emtA5-2IHUYRgA+V88GJoa.yeB3Zks0PKa+20vY1KFRZQCRm0p/5AMd8F
2C788R99/420QpR8DuxJ0EF8899V2X3L1ed1KEM120RkshpPmT1AM00p50
13XzSDheK0GTZK5116x9480n+88pw021POQRk8E3BakKL09yaW0L8YtZ2ZV/
11h8U02j48R5M4773eW8RdxR55-yQ0FzE8CwEAAsAAMA0GCSqS1b3QERBBAGA
AA4TBACJTKK+4m10x5n002u8G5-oQePy0rEn/1ck3V9u0Hvtp0a/Loh#NA5My1wVVb
hAo2M9WLL8omax8qR8xk53buR1rccM49aIC7/G1EKd12OM/9RAC080d+Z8dLxw
```

Skipped attributes:  Not acknowledged  Acknowledged

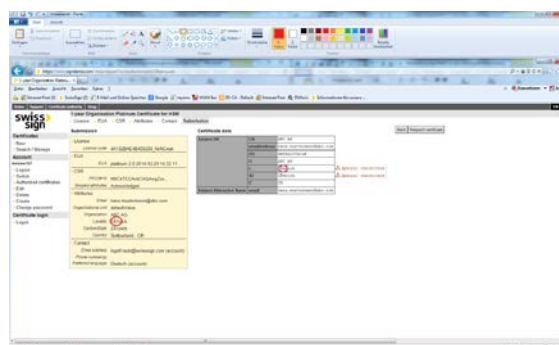
Back Proceed

Skipped attributes

Subject DN [cn] [www.abc.com]

Please tick “Acknowledged” to accept the changes and click afterwards “Proceed”.

It happens that in case of a CSR entry special characters are not shown in the right way.



In this case select the menu item “Attributes” in the menu line above.

You can now correct/edit the misspelling.

**1-year Organisation Platinum Certificate for HSM**

[License](#) > [EUA](#) > [CSR](#) **Attributes** > [Contact](#) > [Submission](#)

**Attributes**

Email : hans.mustermann@abc.com  
 Organizational unit : defaultValue  
 \* Organization : ABC AG  
Including legal form, as officially registered.  
 Example: Unternehmen AG, Company Inc.  
 Locality : Zürich  
 Canton/State : Zürich  
 \* Country : Switzerland - CH

Back Proceed

The page below “Submission” now shows the final certificate details which will be part of the certificate request.

**1-year Organisation Platinum Certificate for HSM**

[License](#) > [EUA](#) > [CSR](#) > [Attributes](#) > [Contact](#) **Submission**

**Submission**

> License  
 License code: 4A182BAE4B450250\_NrNCruk  
 > EUA  
 EUA: platinum 2.0 2014-12-29 14:32:11  
 > CSR  
 PKCS#10: MIIc4TCCAckCAQAwgZsx...  
 Skipped attributes: Acknowledged  
 > Attributes  
 Email: hans.mustermann@abc.com  
 Organizational unit: defaultValue  
 Organization: ABC AG  
 Locality: Zürich  
 Canton/State: Zürich  
 Country: Switzerland - CH  
 > Contact  
 Email address: [redacted] (account)  
 Phone number(s):  
 Preferred language: Deutsch (account)

Back Request certificate

**Certificate data**

Subject DN	CN	ABC AG
	emailAddress	hans.mustermann@abc.com
	OU	defaultValue
	O	ABC AG
	L	Zürich
	ST	Zürich
Subject Alternative Name	C	CH
	email	hans.mustermann@abc.com

## 5.7 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 first of all or to enter the used license again in order to be forwarded to the search mask.

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

### Certificates

- > New
- > Search / Manage



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

**Search / Manage** EN DE Maximize  
Search > Columns

**Search**

Search text :   
Exact search: \*O=SwissSign AG\*  
 Wildcard search: Swiss\*

License :

Account :

Valid from :   
Time span. Example: 2010-03, 2010-05

Expires :   
Time span. Example: 2010-03, 2010-05

Status :  pending  approved  rejected  cancelled  valid  
 revoked  expired

Registration authorities :  SwissSign

Public certificates :  Hide  Show

Page size :

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

<input type="button" value="Withdraw"/>	pending	--	/C=
<input type="button" value="Attributes"/>			/E=
			/O=
			/j=
			/b=
			/o=

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

Then the withdrawal has to be confirmed.

**Search / Manage** EN DE Maximize  
Search > Columns

**Confirm withdraw**

Request to be withdrawn

Status	Expires	Subject	Alternative name
pending	--	/CN=... /Email=...@tech.swissign.com /O=SwissSign Test/L=Zürich/ST=ZH/C=CH /j=... /businessCategory=Private Organization /serialNumber=123	email:...@tec DNS:a.test.swissign.c DNS:b.test.swissign.c

**Confirm withdraw**

\*Request identifier : 5CA09CD722 36A0E584

Reason :

Optional

**Search**

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

**Search / Manage**  
Search > Columns

✓ request 5CA09CD72297...6846C9F withdrawn

## 5.8 Approval process

The certificate requests are then approved by the RA operator of SwissSign. The requirements for the approval process are described further below.

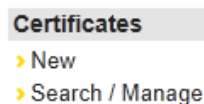
## 5.9 Renewal process

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 into the new certificate request. It is recommended to issue the new certificate 2-3 weeks beforehand and to have it running alongside the expiring certificate.

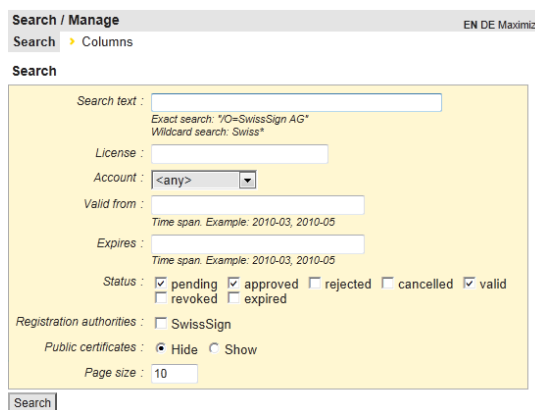
### 5.10 Revocation process

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.



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

	Status > >>	Expires << < > >>	Sub
Download / Attributes	valid	2015-02-27 16:52:14	/CN= /Em: /OU=
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.

**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.

**Confirm revoke**

⚠ Revocation is irreversible.

*Certificate to be revoked*

Status	Expires	Subject	Alternative name
valid	2015-05-28 14:25:11	/CN=... /Email=...@tech.swissign.com	email: ...@te...

- authentication is no longer possible
- digital signature is no longer possible
- encryption is no longer possible
- decryption is still possible

**Confirm revoke**

\* Certificate identifier : 00A09C04BC...28F497?

\* Reason :

- Unspecified
- Key compromise
- Affiliation changed
- Superseded
- Cessation of operation
- Privilege Withdrawn

Comment :

Cancel | Confirm revoke

## 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

Without login

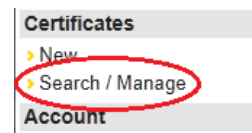
Login as a user who is not an administrator

#### Options

- Search for public certificates
  - Display results
  - Display certificate attributes
  - Download certain certificates
- 
- Search for certificates
  - Display results
  - Display certificate attributes
  - Download certain certificates if the person has the requester role.
  - Change attributes of own certificates
  - Download keys generated for oneself with password

### 6.2 Search for certificates

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

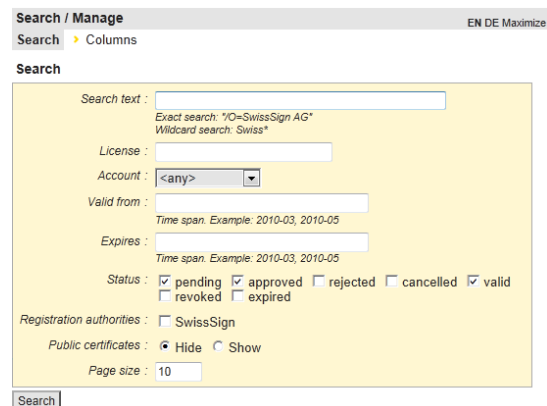


In the work area it is now possible to search for a licence key or alternatively for a text which contains a certificate. The wild card character «\*» can be used. The search string should always contain “ characters as first and last character.

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



Search / Manage EN DE Maximize

Search > Columns

Search

Search text :

Exact search: \*O=SwissSign AG\*  
 Wildcard search: Swiss\*

License :

Account :

Valid from :

Time span: Example: 2010-03, 2010-05

Expires :

Time span: Example: 2010-03, 2010-05

Status :  pending  approved  rejected  cancelled  valid  
 revoked  expired

Registration authorities :  SwissSign

Public certificates :  Hide  Show

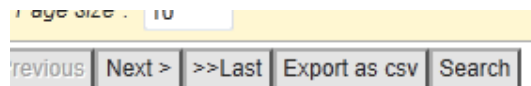
Page size :

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 20 certificates and can be made only with a filter (e.g. text input).

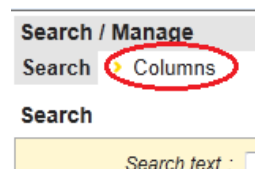
Issued data sets can be exported under «Export as csv» and imported to Excel, for example.



### 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».

**Columns**

Status	> >>	Hide
Valid from	<< < > >>	Show
Expires	<< < > >>	Hide
Subject	<< < > >>	Hide
Alternative name	<< < > >>	Hide
Certificate identifier	<< < > >>	Show

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».

**Columns**

Status	> >>	Hide
Valid from	<< < > >>	Show
Expires	<< < > >>	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.

### Columns

Status	> >>	Hide
Valid from	<< < > >>	Show
Expires	<<< < > >>>	Hide
Subject	<< < > >>	Hide
Alternative name	<< < > >>	Hide
Certificate identifier	<< < > >>	Show

**Please note:** All certificates with the availability «Public download» can be displayed by any users (even without account) and downloaded without a private key. Other certificates are not visible for unauthorised users.

## 6.4 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.

Revoke		
Download / Attributes	valid	2011
Revoke		
Download / Attributes	valid	2011

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 availability of the certificate in the swissign.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 three values:

- Private
- Public lookup
- Public download

In the case of «Private», your certificate will not be displayed for outside users on swissign.net. In the case of «Public lookup»,

### Attributes

\* Request identifier : 87ABC3211BA7CA192F224579E2A

Availability : Private

Account : testuser123

Alt. email :

Account: ingolf.rauh@swissign.com

Alt. language :  English  Deutsch  <account>

Account: Deutsch

Alt. phone :

Cancel Update

Availability : Public download

Account : Private

Alt. email : Public lookup

your certificate can only be checked for validity by others. With «Public download» all details of your certificate are visible for everyone via the search.

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

A screenshot of a form with a yellow background. It contains two input fields: 'Alt. language' with a radio button and 'Alt. phone' with a text box. Below the fields are two buttons: 'Cancel' and 'Update'.

## 6.5 Create Request Form / Registration Form Again

As far as you did request a Gold certificate the last step of the request was the download and print-out of the request form. If you lost this form it is possible to recreate this form by searching the pending certificate request as described above.

Please look for your pending certificate request as described above and click on „Attributes“.

A screenshot of a table with a grey background. The table has three rows. The first row has a button labeled 'Attributes'. The second row has a button labeled 'Withdraw' and a text field containing 'DNS:www.swissign.com'. The third row has a button labeled 'Attributes', which is circled in red.

In case of a Gold certificate request you can download the form again by a click on the link:

A screenshot of an 'Approval' section with a yellow background. It contains a text field with the text 'Registration form : gold\_multi\_ucc\_new'.

## 6.6 Resend of proof of possession emails

In case of SSL Silver certificates or Personal ID Silver certificates an email will be send to your mentioned email address in order to check if you possess or if you can control the mentioned domain.

It happens that this email does not arrive at your account, e.g. in case you have set up the email account after the certificate request. It may be necessary to resend the email for proof of possession again:

Please look for your pending certificate request as described above and click on „Attributes“. You will see the Approval section.

A screenshot of a table with a grey background. The table has three rows. The first row has a button labeled 'Attributes'. The second row has a button labeled 'Withdraw' and a text field containing 'DNS:www.swissign.com'. The third row has a button labeled 'Attributes', which is circled in red.

In case of a SSL certificate you can select the email address again and resend the email by click on the button below.

### Approval

\* Email :  admin@swissign.com  
 administrator@swissign.com  
 hostmaster@swissign.com  
 postmaster@swissign.com  
 webmaster@swissign.com

Send proof of possession email

In case of a Personal ID certificate you can resend the email by click on the button below.

### Approval

Email : ingolf.rauh@swissign.com

Send proof of possession email

## 6.7 Proof of Possession Email

In case of Silver SSL or Personal Silver ID certificates you obtained an email with link which should be activated to show that you can control the specified (email-)domain.

Von:  ca@signdemo.com Gesendet: Mo 29.12.2014 10:00:00  
 An:  [redacted]  
 Cc:  
 Betreff: New SwissSign Silver Certificate Request 13450AEA11[redacted]  
 Signiert von: ca@signdemo.com

Dear customer

The following certificate request has just been submitted to SwissSign:

**/CN=Email: [ingolf.rauh@swissign.com](mailto:ingolf.rauh@swissign.com)/OU=Email Validated Only (email:ingolf.rauh@swissign.com)**

As the legitimate owner of the email '[ingolf.rauh@swissign.com](mailto:ingolf.rauh@swissign.com)', you can approve this request yourself. To approve the request now, please open the following link in your browser:

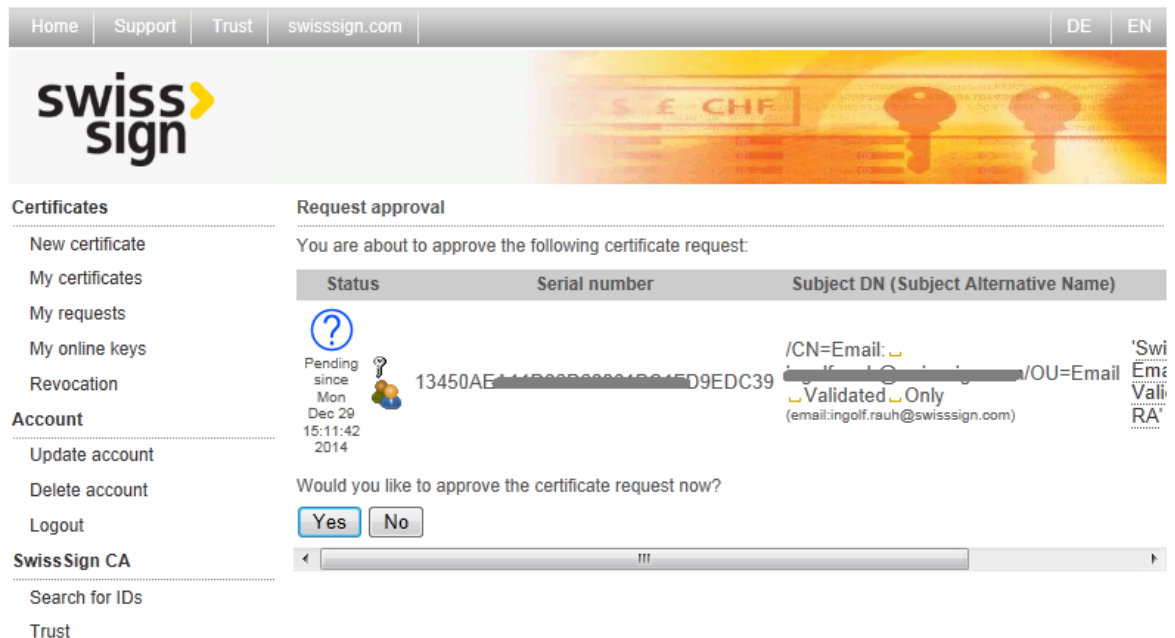
[https://swiss.signdemo.com/cgi-bin/request/approve?auth=65647A1BF5466D32\[redacted\]&id=13450AEA11\[redacted\]](https://swiss.signdemo.com/cgi-bin/request/approve?auth=65647A1BF5466D32[redacted]&id=13450AEA11[redacted])

To cancel the certificate request, use the following link:

This email allows you with 2 different links

- To withdraw your certificate request. In this case the license can be reused for the next certificate request or
- To show that you can control the specified domain or email address:





Please confirm the request approval by clicking on “Yes”.

## 7. Authorization of the Certificate Request – File in the form

Silver SSL or Personal ID Silver certificates are normally authorized immediately after confirming the access control to the specified domain or email address. In case of Gold, Gold EV and Organization certificates you can download and print a PDF or http form document which has to be signed accordingly. The document is already prepared with all your certificate request data you entered before.

You have to fill in the following information:

- Authorization of the requester: please fill in the name, signing date and signing place. The person who entered the certificate data before has to sign here.
- Authorization of the organization (applicant): please fill in the name, signing date and signing place of the responsible of your organization according to the trade registry excerpt or other organizational document. If a joint signature by at least 2 persons is required the certificate request must be signed by 2 responsible persons.
- Authorization of the domain: If the certificate mentions a domain name, the domain owner has to sign here. Please fill in the name of the domain owner, the signing date and signing place. In case you or your organization owns also the domain the signees from the point before have to sign here again. Otherwise please look up at <http://whois.com> or <https://gwhois.org>: who is the owner of your domain? Let him sign the document.

If your organization is listed in the trade registry you have no longer to attach a trade registry excerpt for your request. In case your organization is not listed in the trade registry you have at least to show the existence of your organization. Please contact in doubt our helpdesk for more information. It could be helpful to send us in this case:

- A copy of an official letter from your tax office showing the company tax ID number of your organization.
- Any official registry which show your business.
- In case of state organizations: a confirmation letter of the upper organizational unit.

In case of SSL EV certificates we have to find your organization in an official phone book or yellow page book in order to check your address. If your company exists no longer than 3 years we need a statement of your bank about the existence of your business with starting point of your exercised business.

SwissSign needs furthermore copies of the passport (or EU/Swiss/Liechtenstein IDs) of all persons who signed the request. The copy should show the photo, the complete name and signature of the signee.

Requests should be sent by regular mail to the following address:

SwissSign AG  
Fulfillmentcenter

Sternmatt 6  
Postfach 2259  
CH 6010 KRIENS 2

In case you want to use a courier parcel express service you need some additional address lines:

Swiss Post Solutions AG  
SwissSign  
4. Obergeschoss

Sternmatt 6  
Postfach 2259 / 6010 Kriens 2

CH-6010 Kriens

In urgent cases you can send the documents and form also electronically in parallel to the regular mail. Please use the email address [registration@swissign.com](mailto:registration@swissign.com). If the documents do not arrive at least 10 days after the email an eventual issued certificate based on the electronic sent documents will be revoked.

## 8. Authorizations

In special if you want to request multiple certificates you can ease the process with authorizations to prevent multiple signatures from all responsible.

A general authorization document can be found on this page: <https://www.swissign.com/en/support/order-and-request-procedure>. The document itself is [Subscriber Agreement For Gold Certificates With Organization Entry](#) (PDF, 116 KB) - including all authorizations.

You can choose within the document if this authorization is e.g. limited only for the domain authorization or both domain and organization.

Please give a hint on the request form that a authorization was already filled in. The best way would be to include always a copy of this authorization to all requests.

## 9. Download of the issued certificate

If the certificate was authorized you will get an email showing you the download link of your certificate. By click on the download link you will be redirected to the swissign.net download page. Here you can download the certificate with different certificate file types.

**Search / Manage**

> Search > Columns

**Download / Attributes**

*(i) Authentication cookie is no longer valid*

**Certificate**

Alternative name	Certificate identifier	Expires
email: [redacted]	EC2FD[redacted]1534	2015-12-29 16:31:19

**Download certificate and private key (.p12, PKCS#12)**

\* Display name :

\* Key password :

\* Download code : 9EQ7000100E4700E10010001150011B5261!

**Details**

Version	v3
Serial number	00:ec:2f:db:7b:24:c1:85:71:10:2c:ed:fa:32:e5:34

By default the download is offered as p12 file format. Other formats can be downloaded if you search the certificate in your account and download it again. You are also able to download:

**Download certificate (without private key)**

Format :

- .cer
- .crt
- .pem
- .p7c (certificate chain)
- .pem (certificate chain)

The cer, crt or pem format (all without private key) or the p7c or pem format which includes not only the requested certificate but also the complete certificate chain like the issuing certificate and the root certificate of SwissSign.

If you install a web browser it is necessary to install also the issuing certificate and the root certificate of SwissSign otherwise the worldwide web browsers will not show properly that the certificate is trusted.

In case SwissSign did generate the private/public key pair the SSL certificate file p12 based on this key should be downloaded within short term since SwissSign will delete this key (within at latest 3 months). Personal IDs are not target of this deletion.

**10. E-mail notifications**

## 10.1 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 was determined.

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 as described above.

**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 administrator 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 administrator.

- 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.

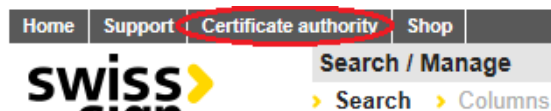
**Please note:** If the e-mail address has changed and you want to allocate this to the already issued certificate, this is possible by making an attribute change for the certificate. See chapter 5.5.

## 11. Import Root and Intermediate certificates

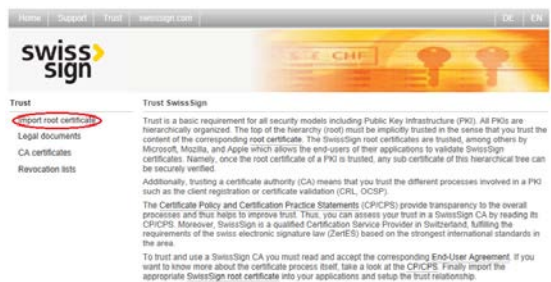
All major browsers and operation systems contain SwissSign root and intermediate certificates. Nevertheless you have to install these root and intermediate certificates if you want to setup web servers or appliances additionally to your certificate. The easiest way is described in chapter 9 “download certificate chain”.

But it is also possible via the direct link to all root certificates of SwissSign:

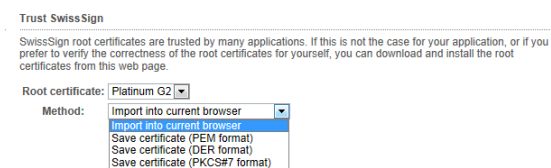
Please select in the menu in the left upper corner the menu item „Certificate authority“



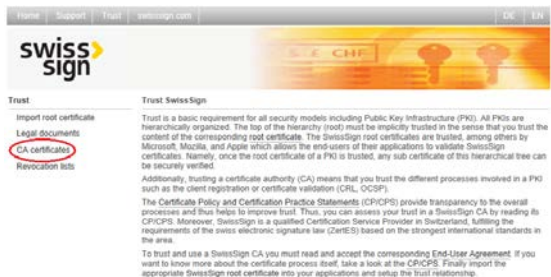
A new window will open and you will see a main menu on the left hand side. First you can select the menu item “Import root certificate”.



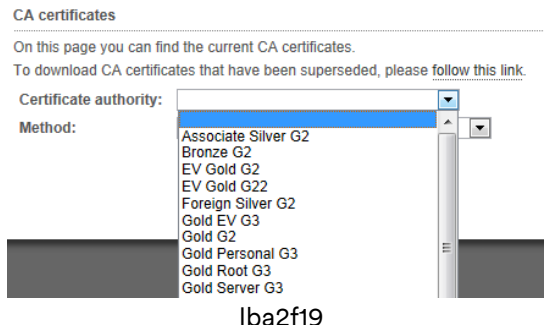
The corresponding root certificate can be downloaded in different file formats or directly imported to your browser.



Concerning the issuing or intermediate certificates please select the menu item „CA certificates“



First you have to select the corresponding issuing CA and then you can download the certificate in different file formats..



## 12. Support contact

For all questions the support team can be reached via <https://www.swissign.com/en/support/supportform> or [helpdesk@swissign.com](mailto:helpdesk@swissign.com) or can be selected via the menu bar at the top:



## 13. Typical Problems

The following problems occur sometimes. Please find also more information in our FAQ area: <https://www.swissign.com/en/swissign-faq>

<p>I want to have other key usages.</p>	<p>You can only edit those certificate attributes which are explicitly allowed to change by the input fields, like domain, organization, locality, province/state, country, email, name, first name, etc.). All other attributes are fix according to the selected product, e.g. Personal Silver ID. The attributes are described in the shop. By this a change of these attributes is not possible, any changes in a CSR will be ignored.</p>
<p>My SwissSign certificate is not shown as „trustful“</p>	<p>Normally this i hint of a missing intermediate or issuing certificate and/or missing root certificate. See description above. Please mind that PDF Adobe readers will show only hardware linked certificates (SwissSign</p>

	Platinum) als trustful.
My certificate should not be publicly visible.	Please call again the attributes of your certificate and select the „availability“ as „private“.
My private key is lost or is stolen.	You shall immediately revoke your certificate. Please search your certificate and press “Revoke”.
There is a difference between my certificate attributes and the certificate request.	As described above there can be differences between a CSR and the content of a certificate since some attributes of the CSR are ignored (like key usage) and fix for the selected product. If there is furthermore any difference please contact the support.
My certificate validity ends	You cannot extend the validity of your certificate. You have to order a new certificate with the same certificate content.
I want to return my certificate	Basically the T&Cs do not permit any return of your certificate. As goodwill SwissSign accepts a return of a certificate up to one month after issuance and pay back the cost. Afterwards you can get a voucher/coupon for the remaining time of the certificate. You have always to revoke the returned certificate since a real “return” is not possible.
Search functionality shows certificates of third parties	Each search will also show certificate from others in the same way a phone book shows phone numbers of other people. The certificates are needed for encrypted communication between people and systems. Only those certificates will be shown which are marked in the attributes of a certificate as publically downloadable.
I need the pfx format	The PFX file format is the same as the p12 file format. Please download the p12 format and rename the file afterwards.
I have to change my certificate details	As far as the certificate is not yet approved and issued the pending certificate request can be found in the search functionality. You can withdraw the pending request and renew it. When the certificate is already issued you



	<p>have to request a new certificate, unfortunately. As goodwill SwissSign will credit your cost for the previous certificate within one month after issuance. Afterwards it will be credited with a coupon for the remaining lifetime of the certificate.</p>
<p>I did not get the proof of possession email.</p>	<p>Please look for the pending certificate request and resend the email again by clicking on the „Attributes“ of the request and the „Send“ button as described above.</p>
<p>I have to create and print out the registration form again</p>	<p>Please look for the pending certificate request and recreate the form again by clicking on „Attributes“ and the link of the form as described above.</p>

## 14. Index

- account 10, 11, 12, 13, 15, 19, 21, 31
- Account 7, 12, 16
- Affiliation changed 28
- Alt. email 31
- Alt. language 31
- anonymous mailbox 21
- applicant 34
- approval 5
- Approval 27, 33
- attribute 39
- attributes 15, 30, 31
- Attributes 12, 18, 21, 25, 31
- Authorisation revoked 28
- Authorization 34, 36
- Authorized certificates 13
- availability 31
- business category 20
- CA certificates 39
- canton/federal state 16
- cer 37
- Certificate authority* 8, 39
- certificate expiry 31
- certificate licence 7
- Certificate login 9
- certificate request 5
- certificate signing request 15
- certificates.csv 14
- Cessation of operation 28
- Change password 13
- CodeSigning 22
- Columns 30
- Contact 16, 21
- CP/CPS 4
- crt 37
- CSR 15, 17, 18, 24
  - certificate signing request 15
- csv 14
- DE 8
- Delete 12
- domain 18, 35
- Domains 19
- Download 36
- Edit 12
- E-mail 38
- e-mail address 12, 15, 16
- EN 8
- EUA 15
- Excel 14, 30
- Expand 15
- expiry 15
- Export as csv 30
- extend the validity 41
- First name 21
- General Terms and Conditions 4
- German 8
- group account 21
- helpdesk* 8
- Hide 30
- Import root certificate 39
- intermediate certificate 39
- issuing certificate 37
- jurisdiction country 20
- Key compromise 28
- key identifier 14
- Key identifier 13
- key usages 40
- language 31
- LDAP 5
- licence 15
- Licence 29
- license 9
- login 29
- Logon 11
- Logout 12
- main menu 9
- Main menu 7
- Manage 29
- menu line 9
- Menu line 7
- multi-domain certificate 19
- New 15
- OCSP 5, 28
- organization 34
- organization certificate 23
- p12 37
- p7c 37
- Page size 29
- password 16, 20
- pem 37
- personal certificates 21
- pfx 41
- PKCS#10 15
- PKI 4
- preferred language 12, 16
- Private 31
- private key infrastructure
  - PKI 4
- profile 7
- proof of possession email 32
- pseudonym 21

Public download 31  
public key 15  
Public lookup 31  
RA administrator 5, 6  
registration form 17  
Registration Form 32  
Registration number 20  
relaying party 4  
Remove 13  
renewal 6  
Renewal process 27  
request approval 34  
Request certificate 17, 22  
requester 29, 34  
Requester 5  
Revocation 27  
Revoke 6, 27  
root certificate 37, 39  
Search 29  
Search text 29  
Search/Manage 6, 27, 30  
*Shop* 8  
Show 30  
SSL EV certificates 35  
SSL Gold 16  
SSL Silver certificate 18  
Submission 18  
*Support* 8, 40  
Switch 12  
telephone number 12  
third party services 24  
trade registry 35  
Umlauts 18  
UTF-8 18  
Withdraw 26  
Withdrawing certificate requests 26  
work area 9  
Work area 7