SwissSign

Bedienungsanleitung Managed PKI

SwissSign

Inhalt

SwissSign

1. Einleitung

1.1 SwissSign und Managed PKI

Die SwissSign AG ist eine international anerkannte Herausgeberin von digitalen Zertifikaten.

Der SwissSign Managed PKI Webservice dient der Ausstellung und Verwaltung von SwissSign Zertifikaten. Der Vorteil bei der Nutzung des Managed PKI Services liegt sowohl im Wegfall des Aufbaues und des Betriebes einer eigenen Zertifizierungsstelle als auch in der Qualität der bezogenen Zertifikate bezüglich der Verbreitung in den Wurzelzertifikatsverzeichnissen (Rootstores) und deren Compliance zu den entsprechenden internationalen Standards.

Im Rahmen dieser Managed PKI Services können Kunden Zertifikate beantragen («Request»), genehmigen («Approve»), ausstellen («Issue») und für ungültig erklären lassen («Revoke»), sowie Zertifikate suchen und verwalten. Dabei unterstützt das Webportal die verschiedenen Rollen (Requestor, Approver, Auditor) innerhalb eines Unternehmens bezüglich Zertifikatsverwaltung. Dabei übernimmt der Kunde die Aufgabe einer Registrierungsstelle (RA), wobei die SwissSign AG den Betrieb der Zertifizierungsstelle (CA=Certification Authority) übernimmt und üblicherweise gegenüber Dritten als der Certificate Service Provider (CSP) auftritt. Selbstverständlich unterstützt der SwissSign Managed PKI Webservice auch den reinen Betrieb einer Kunden CA.

1.2 Ziel und Zweck dieses Dokumentes

SwissSign Managed PKI Service Kunden erhalten ein individuelles Setup auf der SwissSign Infrastruktur um ihre Zertifikate zu verwalten. Dieses Dokument zeigt auf, wie mit dem Managed PKI Service Zertifikate verwaltet werden können: Beantragung, Ausstellung, Verwaltung und Revokation.

1.3 Aufbau dieses Dokumentes

Die Struktur dieses Dokumentes folgt den klassischen Prozessen, die bei privaten Schlüsselverwaltungen (PKI = Private Key Infrastructure) üblich sind. Diese PKI-Prozesse und deren Rollen werden in einem Grundlagenkapitel dargestellt.

Durch den Index am Ende dieser Bedienungsanleitung lassen sich schnell Antworten auf Fragen finden. Die Anleitung verwendet Querverweise, durch Auswahl der Kapitelnummern im Text können Sie schnell verbundene, relevante Inhalte finden. Die Printscreens in dieser Anleitung wurden mit dem Internet Explorer 9 erstellt, in anderen Browsern kann es zu Abweichungen der Darstellung kommen.

1.4 Voraussetzungen für die Nutzung des SwissSign Managed PKI Webservices

Eine beliebige Person, die Empfänger eines signiertes Dokumentes ist oder sich an einer Webseite anmeldet, wird «Relying Party» genannt und muss sich auf den Inhalt des Zertifikates verlassen können. Sie vertraut also dem Certificate Service Provider. Infolge dieser Kette des Vertrauens unterzeichnet der Kunde eines Managed PKI Services die Annahmeerklärung zur Registrierungsstellendelegation, wo er sich den Regeln des Certificate Service Providers unterwirft und seine besondere Verantwortung und Sorgfalt im Umgang und in der Ausstellung von Zertifikaten dokumentiert. Die Regeln des Certificate Service Providers sind in der Zertifizierungspolitik und Zertifizierungspraktiken CP/CPS (www.swisssign.com/cpcps) im Detail beschrieben.

SwissSign führt damit – im Gegensatz zu den Zertifikatprodukten des Webshops – keine Einzelprüfung der Zertifikate im Hinblick auf das Zertifikats-Subject durch, wenn dieses den Richtlinien der Delegation der Registrierungsstelle genügt.In der Annahmeerklärung werden sowohl die Zulässigkeiten und Attribute

der Zertifikatsausstellung festgelegt (z. B. die zugelassenen Domänen, Gültigkeitsdauer der Zertifikate, Sichtbarkeit der Zertifikate im LDAP Verzeichnis) als auch die Pflichten, Prüfprozesse und Sorgfaltsvorschriften, die die Registrierungsstelle (RA) einzuhalten hat.

1.5 Projektspezifische Ausnahmen

Einige Kunden haben angepasste projektspezifische Weboberflächen. Daher können einige Bilder in dieser Anleitung von projektspezifischen Anpassungen abweichen. Die projektspezifischen Abweichungen sind zum Beispiel:

- Login via Smartcard statt via Soft-Zertifikat
- Auswahl von Produkten innerhalb der Managed PKI ohne Möglichkeit der Hinzufügung von Shop-Produkten
- CSR Feld verpflichtet für bestimmte Managed PKI Produkte
- Benutzer-ID im Subject

Auf die projektspezifischen Ausnahmen wird im weiteren nicht eingegangen. Es muss hingegen beachtet werden, dass dadurch einige Printscreens ein anderes Aussehen haben können.

2. PKI – Prozesse und Rollen

Zertifikate haben zwei zentrale Aufgaben, so sind sie einmal ein Container für den öffentlichen Schlüssel und andererseits verbinden sie den öffentlichen Schlüssel mit dem Zertifikatsinhaber/Schlüsselinhaber. Die Aufgabe eines Certificate Service Providers ist es, diese Verbindung als unabhängiger Dritter auf dem Niveau gemäss CP/CPS zu bestätigen und zu garantieren. Damit das gewährleistet werden kann, benötigt er folgende Services, Tätigkeiten und Rollen:

Registration Service (Antragstellungsdienst)

- Zertifikatsantragstellung durch den Antragssteller
- Zertifikatsantragsprüfung durch den Registrierungsstellenverantwortlichen (RAO = Registration Authority Officer) oder nachfolgend Zugangsverantwortlicher genannt.
- Freigabe des Zertifikatsantrags durch den Zugangsverantwortlichen (RAO)

Certificate Generation Service (Generierungsdienst für Zertifikate)

- Erzeugung des Zertifikates

Revocation Service (Dienst zur Ungültigkeitserklärung)

- Online-Ungültigkeitserklärung durch den Zertifikatsinhaber
- Offline-Ungültigkeitserklärung durch den Zugangsverantwortlichen (RAO)

Dissemination Services (Verbreitung der Informationen)

- CP/CPS
- OCSP (Online Certificate Status Protocol) – Online Status über die Gültigkeit von Zertifikaten
- CRL (Certificate Revocation List) – Ungültigkeitslisten (offline) von Zertifikaten
- LDAP (Light Weight Address Directory)

Die folgende Tabelle gibt einen Überblick der Tätigkeiten und deren Abbildung im Managed PKI Service:

Tätigkeit	Rolle/Wer	MPKI-Unterstützung
Zertifikatsantrag	Antragsteller/Systemadministratoren	GUI
Freigabe	Zugangsverantwortlicher	GUI
Ausstellung/Erzeugung	-	CA
Installation	Antragsteller/Systemadministratoren	E-Mail mit Download Link
Ungültig erklären	Antragsteller/Systemadministrator, Zugangsverantwortlicher	GUI
Erneuerung	Antragsteller/Systemadministrator, Zugangsverantwortlicher	Warn-E-Mail 10 Tage und 30 Tage vor Ablauf
Suchen/Verwalten	Antragsteller/Systemadministrator, Zugangsverantwortlicher	GUI
Informieren/Auditieren	Zugangsverantwortlicher, Auditor	GUI

3. Bedienkonzept

Die Benutzeroberfläche ist nativ ohne Nutzung einer speziellen Software für die Benutzeroberfläche geschrieben. Das dient dem Ziel der Sicherheit, da die Nutzung fremder, nicht bekannter Softwarepakte auch immer ein Sicherheitsrisiko bedeutet. Insofern wird die Verwendung von Graphiken und Symbolen in der Benutzeroberfläche minimiert.

3.1 Grundlagen

3.1.1 Rollen innerhalb der Managed PKI von SwissSign

Das System wurde entwickelt um die Ausstellung und Verwaltung der Zertifikate möglichst einfach zu gestalten. Aus diesem Grund arbeitet das System mit unterschiedlichen Rollen, die verschiedene Rechte besitzen:

Anforderer (Requester)	Er ist typischerweise ein Anwender, der ein Zertifikat anfordern kann. Er kann in dieser Rolle die für ihn freigeschalteten Zertifikate beantragen. Ein Anforderer loggt sich mit Benutzernamen /Passwort ein oder es wird ergänzend oder alternativ konfiguriert, dass er sich mit einem Zertifikat einloggen kann.
Zugangsverantwortlicher	Nimmt die Funktionen des Administrators einer Registrierungsstelle (RA) an. Er kann alle Zertifikate einer RA sehen, Zertifikatsanträge freigeben, anfordern, ungültig erklären, anschauen und Konten für Anforderer anlegen. Er ist auch verantwortlich für den Zugang zur Managed PKI und verwaltet die Zugangszertifikate.
RA-Distributor	Dieser wird nur definiert, wenn der Zugangsverantwortliche nicht definiert wird. Er hat keine RA-Funktion. Er sieht alle Zertifikate der RA, kann Zertifikate anfordern, anschauen, revozieren oder Anforderer-Konten anlegen. Dies ist z. B. interessant für SwissSign Partner, die die SwissSign Managed PKI wiederum über Reseller an Endkunden verkaufen und einen Überblick über das gesamte Geschäft haben möchten.
RA-Auditor	Kann alle Zertifikate sehen inklusive Detaildaten von Zertifikaten wie Ausstellungsdatum, Ablaufdatum etc.

3.1.2 Konten

Konten (Accounts) dienen der Verwaltung von Zertifikaten auf Stufe der Anforderer (Requestoren) respektive Anforderer-Gruppe (Requestor-Gruppe) und wurden in früheren Releases der SwissSign Managed PKI auch Profile genannt.

Ein Konto repräsentiert einen Benutzer oder eine Gruppe von Benutzern, die sich durch Benutzername/Passwort oder mittels Zertifikat anmelden können. Konten werden von Zugangsverantwortlicheren innerhalb eines MPKI-Setups angelegt und mit bestimmten Anforderern innerhalb der Managed PKI Setups verbunden. Der Zugangsverantwortliche kann festlegen, ob für dieses Konto ein Zertifikatslogin zwingend notwendig ist und ob der Anforderer auch die Zertifikate revozieren darf.

Ein Konto umfasst Kontaktinformationen, speziell die E-Mail-Adresse für Benachrichtigungen und optional eine Telefonnummer. Die Information kann vom Konteninhaber verändert werden.

Der Anforderer kann Zertifikatsanforderungen im Rahmen der für die RA zugelassenen Zertifikatstypen stellen. Jede Zertifikatsanforderung unter Benutzung dieses Kontos wird diesem Konto zugeordnet. Damit müssen die Kontoinformationen nicht jeder Zertifikatsanforderung einzeln zugeordnet werden. Jede einzelne Zertifikatsanforderung wird über einen Workflow zu den entsprechenden Zugangsverantwortlicheren weitergeleitet, welche diese Anforderung prüfen und bewilligen müssen.

Achtung: Das Konto im Rahmen der Managed PKI auf swisssign.net hat nichts mit den Benutzerkonten zu tun, die ggfs. im Webshop www.swisssign.com angelegt wurden.

3.1.3 Zugangsverantwortlicher

Zugangsverantwortlicheren verwalten eine RA (siehe Kapitel 3.1.4). Ihnen stehen dazu typische Grundfunktionen wie Anzeigen, Suchen oder Exportieren von Zertifikaten zur Verfügung. Nur Zugangsverantwortlicheren können Zertifikate ausstellen, Anforderungen für Zertifikate (durch Benutzerkonten mit Anforderer-Erlaubnis) genehmigen oder die Rechte von Benutzern modifizieren. Auch das Überschreiben von Passwörtern von Anforderer-Konten ist Zugangsverantwortlicheren möglich. Alle Zugangsverantwortlicheren haben gegenseitig Zugriff auf die Konten, die mit entsprechenden RAs verbunden sind.

Hinweis: Der Login als Zugangsverantwortlicher erfolgt zwingend mit dem zuvor von SwissSign eingerichteten Zugangsverantwortlicher-Zertifikat.

3.1.4 Registrierungsstelle (RA)

Ein Managed PKI Kunde kann von SwissSign mehrere Registrierungsstellen eingerichtet erhalten, wie es im entsprechenden Managed PKI Setup Agreement festgelegt wurde. So macht es ggfs. Sinn aufgrund unterschiedlicher Prozesse eine RA nur für Gold Zertifikate zu nutzen und eine andere nur für Silver Zertifikate, oder eine für Personenzertifikate und die andere für SSL Zertifikate. Aber auch grosse Abteilungen können für sich eine RA haben, die getrennt ist von der RA einer anderen Abteilung.

Die Vorteile liegen im organisatorischen Prozessablauf: In der Rollenvergabe kann z. B. die Rolle «Anforderer» vom Zugangsverantwortlichen dann später nur einer spezifischen RA zugewiesen werden und somit organisatorisch getrennt werden. Auch die Prüfung der Zertifikate kann für die Registrierungsstellen getrennt erfolgen.

3.1.5 Zertifikatsgutschein

Ein Zertifikatsgutschein (manchmal auch Zertifikatslizenz benannt) ist ein Code, der es dem Benutzer erlaubt, ein entsprechendes Zertifikat anzufordern. Im Rahmen der Managed PKI wird der Gutscheincode nicht eingesetzt oder nur dann, wenn von einem bestimmten Zertifikatstyp sehr geringe Mengen von vielen Anforderern benötigt werden. Der Gutscheincode kann typischerweise im SwissSign Webshop erworben werden.

3.2 Aufbau der Benutzeroberfläche

Die Benutzeroberfläche ist in folgende Bereiche unterteilt:

- Header-Bereich: Allgemeine Informationen und Sprachauswahl
- Hauptmenü
- Menüzeile
- Arbeitsbereich

Die Benutzeroberfläche ist in folgende Bereiche unterteilt, auf die im nachfolgenden Text referenziert wird:

Oben links gibt es mehrere Schaltflächen, die mit Links verbunden sind:

- Startseite: Durch Betätigen dieser Schaltfläche kommt man immer wieder auf die Startseite der Benutzeroberfläche zurück.
- Support: Ein Link zum Helpdesk
- Zertifizierungsstelle: Hier gelangt man zu allgemeinen Informationen über SwissSign und zu weiteren Links z. B. zur CP/CPS und den Zertifikaten der Root und Issuing (Intermediate) CA.
- Shop: Hier gelangt man zum Webshop von SwissSign.
- Zertifikat für ungültig erklären: Verlinkung zu einer Informationsseite über Möglichkeiten einer Ungültigkeitserklärung eines Zertifikates.
- Help: Diese Bedienungsanleitung

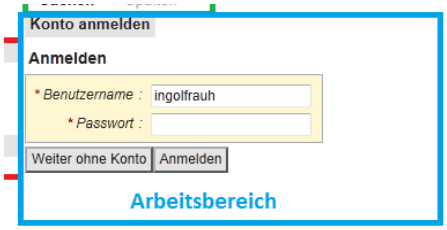
Besonderheit: Der Anwender kann durch eine Schaltfläche ganz oben rechts diese Leiste komplett (inklusive Logo) ausblenden, um eine grössere Arbeitsfläche zu haben.

Oben rechts kann jederzeit die Sprache geändert werden.

- DE: Benutzeroberfläche in Deutsch
- EN: Benutzeroberfläche in Englisch

Links befindet sich das Hauptmenü. Unterhalb der einzelnen Untermenü-Überschriften sind Aktionen anwählbar.

Über die Menüpunkte im Hauptmenü wird der Applikationsablauf im Arbeitsbereich gesteuert.



Je nach gewähltem Menü im Hauptmenü gibt es einen Workflow oder Ablauf bzw. mehrere Aktionen, die möglich sind. Um den Arbeitsbereich entsprechend anzusteuern, kann auf die Schaltflächen der Menüzeile oberhalb des Arbeitsbe-

reichs geklickt werden.

3.3 Start und Login auf ra.swisssign.net

Vor dem ersten Anmelden erhält der Kunde von SwissSign die nötige Konfiguration, um mit der MPKI Infrastruktur zu arbeiten. Diese Konfiguration wurde zuvor in der Annahmeerklärung zur Delegation der Registrierungsstellentätigkeit festgelegt. Dazu erhält der Kunde je nach Wunsch eines oder mehrere – regulär drei – Zugangsverantwortlicher-Zertifikate, mit denen er sich gegenüber SwissSign als Zugangsverantwortlicher authentisiert und auf die SwissSign CA unter www.swisssign.net als Zugangsverantwortlicher zugreifen kann.

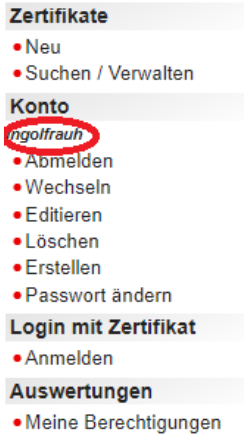
Das Zertifikat muss im Betriebssystem bzw. Browser eingerichtet werden oder auf Smartcard verfügbar sein, um es für den Login verwenden zu können.

Generell gibt zwei Optionen um sich anzumelden:

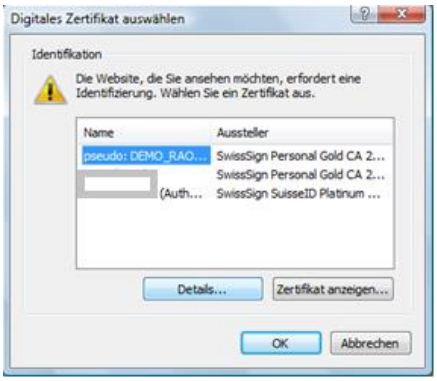
- Login mit Zertifikat: Als Zugangsverantwortlicher ausschliesslich mit Zertifikat möglich via den Link oben oder über den Menüpunkt in https://www.swisssign.net
- Login mit Konto, welches z.B. der Rolle Anforderer zugeordnet ist. Die Anforderer-Konten werden in der Regel vom Zugangsverantwortlicher angelegt. Das ist nur über https://www.swisssign.net möglich.

Es ist immer möglich, als bereits eingeloggter Benutzer eine andere Rolle einzunehmen und sich mit einem dementsprechenden Konto einzuloggen.

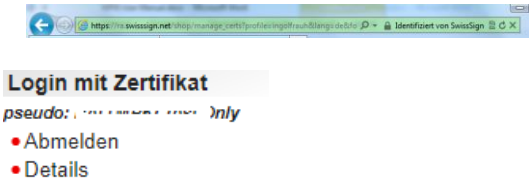
Sobald man im Konto eingeloggt ist, wird der Kontoname unterhalb der Menüzeile «Konto» kursiv und fett gedruckt angezeigt.



Wenn man sich als Zugangsverantwortlicher mit Zertifikat anmelden will, so muss SwissSign ein Zertifikat für den Zugangsverantwortlicher einrichten. Der Zugangsverantwortlicher kann auch für andere Benutzer später ein Login mittels Zertifikat einrichten über «Zugelassene Zertifikate».



Man wird zunächst über ein Fenster des Betriebssystems gebeten, das Zertifikat für das Login auszuwählen. Es ist immer eine SuisseID Platinum oder ein spezielles RAO Zertifikat für den Zugangsverantwortlicher konfiguriert.



Eine erfolgreiche Anmeldung als Zugangsverantwortlicher wird in der Adresszeile des Browsers angezeigt: Die Adresse: ra.swisssign.net ist gewählt. Auch im Hauptmenü ist nun ersichtlich, dass man mit Zertifikat eingeloggt ist. Der eingeloggte Benutzer erscheint nun unter der Menüzeile «Login mit Zertifikat».

Hinweise:

- Es ist darauf zu achten, dass man nur mit einem Konto angemeldet ist. Mit «Abmelden» können Sie sich aus dem entsprechenden Konto ausloggen.
- Beim Login wird ein Konto-Session-Cookie (signiert) gesetzt. Dieser ist <30 Minuten gültig.
- Ein Anforderer-Konto wird kundenseitig durch den Zugangsverantwortlicher angelegt. Der Zugangsverantwortlicher hat auch die Möglichkeit, ein neues Passwort zu vergeben, wenn der Anforderer sein Passwort vergessen hat.

3.4 Umgang mit Benutzerkonten

Ein Benutzer kann sich auf einem Benutzerkonto einloggen. Dieses Konto ist grundsätzlich mit verschiedenen Rollen verbunden.

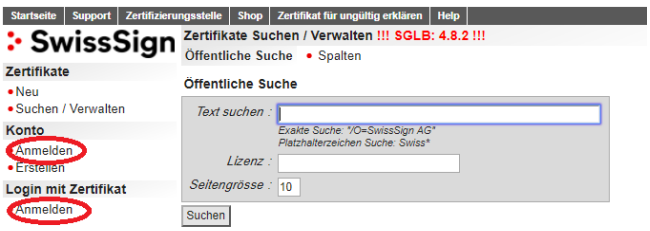
3.4.1 Anlegen eines Kontos

Kunden einer Managed PKI mit eigener Registrierungsstelle sollten nur Konten nutzen, die der Zugangsverantwortlicher für sie angelegt hat. Alle anderen Konten sind Webshop-Benutzern vorbehalten. Die Zertifikate, die über ein Konto beantragt werden, dass nicht vom Zugangsverantwortlicher eingerichtet wurde, sind in der Verwaltung der RA nicht sichtbar.

Auf die Erstellung von Konten für Webshop-Kunden wird hier nicht eingegangen.

3.4.2 Anmelden am Konto

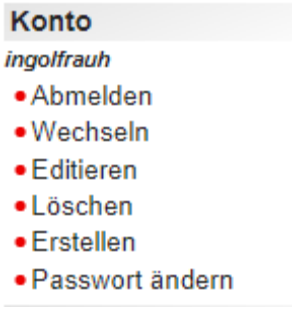
Ein Zertifikatsanforderer kann sich in seinem zuvor von dem Zugangsverantwortlicher eingerichteten Konto anmelden. Der Zugangsverantwortlicher hat festgelegt, ob die Anmeldung zwingend mit Benutzername/Passwort oder Zertifikat erfolgen muss. Entsprechend hat die Anmeldung unter Menüpunkt «Anmelden» im Menü «Login mit Zertifikat» oder Menü «Konto» zu erfolgen.



3.5 Kontoverwaltung

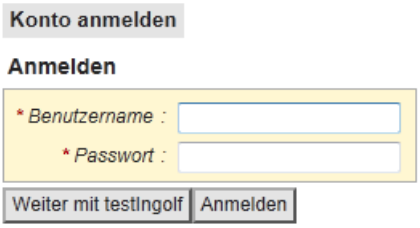
Als normaler Benutzer hat man die Möglichkeit im Nachhinein sein Konto zu verwalten.

Im Hauptmenü hat man unter dem Menüpunkt «Konto» folgende Möglichkeiten, sein Konto zu verwalten:



Mit «Abmelden» kann man sich komplett aus der Anwendung abmelden und ist praktisch ein Benutzer ohne Konto der Webseite. Benutzer ohne Konto können z. B. immer noch öffentlich publizierte Zertifikate suchen und anzeigen lassen.

Mit «Wechseln» kann man in ein anderes Konto wechseln, indem man sich an diesem anmeldet.



Mit «Editieren» kann man die Attribute des Kontos verändern, z. B. die E-Mail-Adresse oder Telefonnummer.

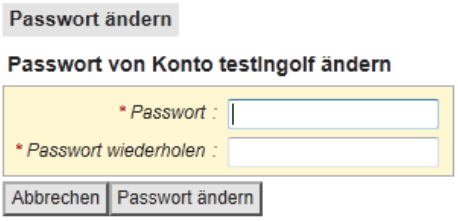
Mit «Löschen» kann das bereits vorhandene Konto wieder gelöscht werden. Achtung: Das jeweilige Konto wird sofort gelöscht.

Mit «Erstellen» kann ein weiteres Konto erstellt werden. Es läuft analog zum erstmaligen Erstellen des Kontos. In diesem Falle muss der Benutzername, das Passwort und eine E-Mail Adresse eingegeben werden, die für alle Benachrichtigungen zu den Zertifikaten genutzt wird, die unter diesem Konto beantragt wurden, unabhängig von der E-Mail Adresse, die in einem Zertifikat selber enthalten ist. Die bevorzugte Sprache legt die Sprache für die E-Mail Benachrichtigungen und die Sprache der Benutzeroberfläche nach dem Login fest.

Passwörter können bis zu 49 Zeichen lang sein und dürfen folgende Zeichen beinhalten:

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

Mit «Passwort ändern» ändert man das Passwort zu einem vorhandene Konto.



3.6 Anforderer (Requester) Konti-Erstellen und Verwalten

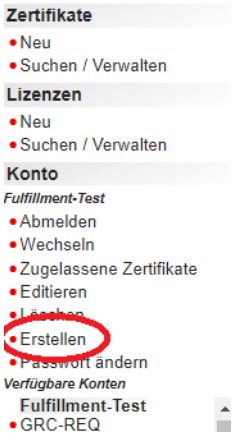
3.6.1 Neues Anforderer-Konto als Zugagangsverantwortlicher erstellen

Der Zugangsverantwortliche hat die Möglichkeit, bestimmten Benutzern die Rolle «Anforderer» (Requester) zuzuweisen. Er kann auch festlegen, dass diese Personen sich auf der Managed PKI Plattform nur mit Zertifikat einloggen dürfen und nicht mehr mit Benutzername/Passwort. Hierzu ist ein Zertifikat mit einem Konto zu verbinden. Im Falle von SwissSign Zertifikaten muss hierfür mindestens ein Gold Zertifikat gewählt werden. Der Zugangsverantwortliche kann auch für einen Benutzer zwingend vorschreiben, zukünftige Logins nur noch mit Zertifikat durchzuführen oder kann beide Möglichkeiten (Benutzername/Passwort und Zertifikat) zulassen.

Der Zugangsverantwortliche kann sich alle «zugelassenen Zertifikate» anzeigen lassen, diese natürlich auch revozieren und verwalten. Zunächst wird beschrieben, wie ein neuer Benutzer (z. B. als Anforderer) angelegt wird.

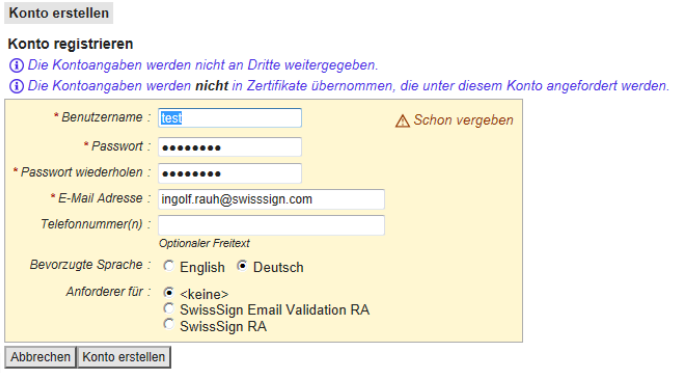
Der Zugangsverantwortliche loggt sich zunächst als Zugangsverantwortlicher in der RA ein.

Im Hauptmenü wählt er unter dem Menüpunkt «Konto» die Aktion «Erstellen».



Im Arbeitsbereich füllt er nun die Kontoangaben für das neue Konto aus. Hierzu zählen:

- Benutzername, unter dem sich der neue Benutzer demnächst anmeldet.
- Passwort
- E-Mail-Adresse des Benutzers
- Optional die Telefonnummer
- Bevorzugte Sprache der Benutzerführung und für die E-Mail-Kommunikation (Deutsch/Englisch)
- «Anforderer für»: Hier kann festgelegt werden, ob der Benutzer auch innerhalb einer markierten RA-Zertifikate anfordern darf.



Sobald der Benutzer Zertifikate anfordern darf, kann der Zugangsverantwortliche hier noch weitere Optionen festlegen, die bei Anwahl der Auswahlknöpfe «Anforderer für» automatisch aufklappen:

- Nur Zertifikats-Login: Sicherheitseinstellung, die verhindert, dass sich der Benutzer ausser mit dem Zertifikat noch mit Benutzername/Passwort einloggen kann.

Ungültigkeitserklärung deaktiviert: Der Benutzer darf die angeforderten Zertifikate nicht revozieren (für ungültig erklären). Das darf in diesem Falle nur der Zugangsverantwortliche.

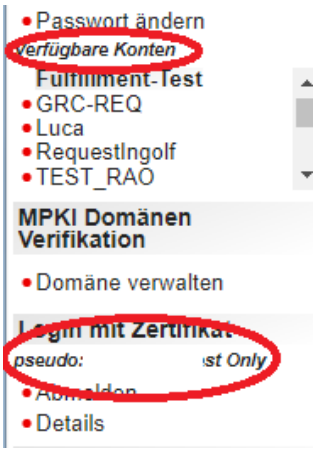
Hinweis: Bei Beantragung von Zertifikaten werden die Angaben aus dem Kontofür Benachrichtigungen zu dem jeweiligen Request verwendet. Das heisst die E-Mail-Adresse und das Zertifikat werden automatisch mit dem Kontoverknüpft, sofern der Beantragende das nicht explizit ändert.

3.6.2 Vorhandenes Konto die Anforderer-Rolle übergeben

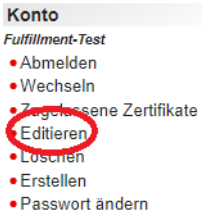
Der Zugangsverantwortliche loggt sich zunächst als Zugangsverantwortlicher in der RA ein.

Er meldet sich nun unter einem Konto mit Benutzername/Passwort ein oder wählt ein vorhandenes Konto aus der ihm angezeigten Übersicht unter «Verfügbare Konten».

Das gewählte Konto ist dann aktiv, wenn es fett und kursiv gedruckt unterhalb des Menüpunktes «Konto» steht. Im nebenstehenden Beispiel ist es das Konto «CE».



Unter dem Hauptmenüpunkt «Konto» den Menüpunkt «Editieren» anwählen.



In dem Arbeitsbereich werden nun die Attribute dieses Kontos angezeigt. Das Attribut «Anforderer für» ist anzupassen, indem die entsprechende RA (falls mehrere vorhanden sind) markiert wird. Bei den Optionen sind folgende Checkboxen optional auszuwählen:

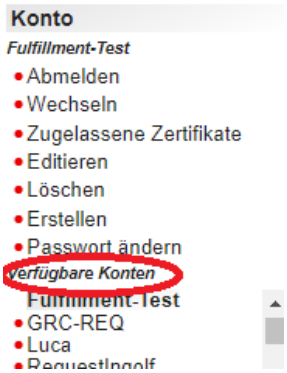
- Nur Zertifikats-Logon: Sicherheitseinstellung, die verhindert, dass sich der Benutzer ausser mit dem Zertifikat noch mit Benutzername/Passwort einloggen kann.
- Ungültigkeitserklärung deaktiviert: Der Benutzer darf die angeforderten Zertifikate nicht revozieren (für ungültig erklären). Das darf in diesem Falle nur der Zugangsverantwortliche.

3.6.3 Ein Konto mit Zertifikat verbinden (für Login)

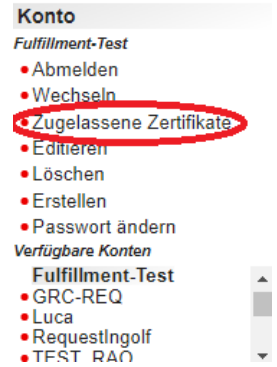
Gerade für die Anforderung von Zertifikaten kann der Zugangsverantwortliche für die Personen, die Zertifikate anfordern dürfen, festlegen, dass diese sich nur mit Zertifikat (speziell konfiguriertes RA Operator Zertifikat oder Stufe Gold oder Platinum – SuisseID) an der MPKI Applikation anmelden dürfen. Der Zugangsverantwortliche kann ein MPKI Konto auch mit mehreren Zertifikaten verknüpfen, so dass Ferienvertretungen etc. möglich sind.

Hierzu muss er ein Konto mit einem Zertifikat für das Einloggen verbinden.

Zunächst wird der Benutzer vom Zugangsverantwortlichen entweder unter «Verfügbare Konten» angewählt oder man loggt sich als Zugangsverantwortlicher in dieses Konto ein.



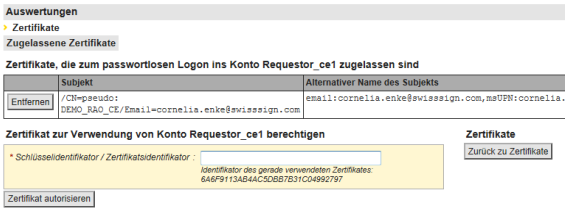
Hierzu gibt es in der RA-Administration-sverwaltung den Punkt «Zugelassene Zertifikate», der sich im Hauptmenü links unter «Konto» befindet.



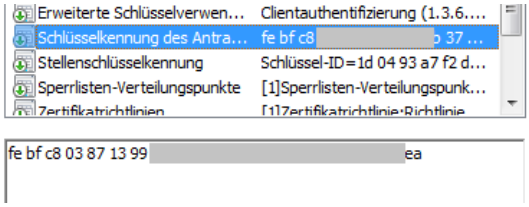
Der Tab «Zugelassene Zertifikate» zeigt alle Zertifikate an, sofern diese schon mit einem Konto verbunden sind.

Ein neues Zertifikat kann über das Eingabefeld «Schlüsselidentifikator» eingegeben werden. Hier ist die ID des Zertifikates einzugeben.

Mit der Schaltfläche «Entfernen» kann auch ein Zertifikat wieder einem Konto entzogen werden. Der Benutzer muss sich dann wieder mit Benutzername/Passwort einloggen.



Den Schlüsselidentifikator können Sie aus der Standardzertifikatsanzeige Ihres Betriebssystems entnehmen.



Hinweis: Grundsätzlich hat der Zugangsverantwortliche Zugriff auf alle Konten innerhalb der Managed PKI. Möchte auch ein anderer Benutzer Zugriff auf andere Konten haben, so hat er diese einzeln über die Funktion «Zugelassene Zertifikate» einzubinden.

4. PKI Prozesse und deren Abbildung in der Software

4.1 Antrags-Prozess/Anfordern von Zertifikaten

Jede Zertifikatsanforderung gehört zu einer RA. Eine Zertifikatsanforderung ist nur möglich mit den für diese RA hinterlegten und konfigurierten Zertifikatstypen.

Ein MPKI Kunde von SwissSign kann mehrere eigene RAs besitzen, unter denen unterschiedliche Zertifikatstypen oder unterschiedliche Domänen definiert sind.

Benutzer müssen eine der folgenden Bedingungen erfüllen, damit Sie Zertifikatsanforderungen stellen können:

- Besitz eines Zertifikatsgutscheincodes (dieser wird historisch noch an einigen Stellen im GUI mit dem englischen Wort „Lizenz“ oder „Lizenzcode“ belegt): Eingabe eines gültigen Codes. Zertifikatsgutscheine können im SwissSign Webshop gekauft werden, können aber auch vom Zugangsverantwortlichen erzeugt werden im Rahmen einer Managed PKI. Ein Zertifikatsgutschein berechtigt einen Benutzer dazu, eine bestimmte Anzahl Zertifikate anzufordern – in der Regel ein einziges Zertifikat. Ein Zertifikatsgutschein bestimmt ein Produkt und damit eine RA, worüber eine Anforderung gestellt werden kann. Zertifikatsgutscheine lohnen sich bei Nutzung durch unterschiedliche Zertifikatsanforderer, die aber nur ein oder wenige Zertifikate wünschen und für die man nicht jedes Mal ein eigenes Konto anlegen möchte.
- Der Benutzer ist Zugangsverantwortlicher (über Zertifikat-Authentisierung)
- Der Benutzer ist MPKI-Anforderer (über ein MPKI-Anforderer-Konto)

Bei Beantragung als Administrator oder Benutzer mit Konto ist ein Login mit Passwort oder Zertifikat, wie oben beschrieben, notwendig.

Sollte ein Zertifikat im Shop erworben sein, welches in der Verwaltung der Zertifikate der Managed PKI mit auftauchen soll, so ist darauf zu achten, dass dieses Zertifikat auf jeden Fall mit einem Benutzer beantragt wird, der vom Zugangsverantwortlicher angelegt wurde.

Sofern man bereits mit einem anderen Konto (z. B. Zugangsverantwortlicher) eingeloggt ist, kann es Sinn machen, sich zunächst über das Hauptmenü abzumelden und dann an einem Konto anzumelden, mit dem man Zertifikate beantragen kann. Oder man erstellt eine neues Konto über den Menüpunkt «Erstellen».

Einfache Benutzer mit Anforderer-Konto müssen die Rechte besitzen, um Zertifikate zu beantragen.

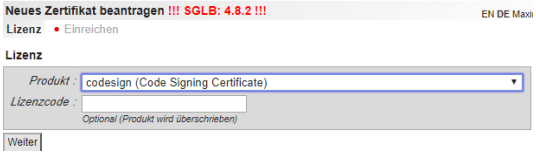
Administratoren können für die Anforderung eines Zertifikates zusätzlich ein separates Konto verwenden. Dies ist aber nicht zwingend notwendig. Ein separates Konto bietet folgende Vorteile:

- Kontodaten (E-Mail-Adresse, Spracheinstellung) werden direkt übernommen und bei der Erstellung eines Zertifikates als Attribute dem Zertifikat beigefügt. Dabei handelt es sich nicht um Daten, die im Zertifikat enthalten sind, aber z. B. zugeordnete Daten, wie z. B. die E-Mail-Adresse, an die Ablaufnotifikationen bezüglich dieses Zertifikates gehen.

Nach denen mit einem Konto angeforderten Zertifikaten kann gezielt durch Anwendung eines Filters (Anforderer) gesucht werden.

Um Zertifikate neu zu beantragen ist im Hauptmenü links unter Oberpunkt «Zertifikate» der Unterpunkt «Neu» zu wählen.

Im Rahmen der Managed PKI können Sie im Arbeitsbereich unter «Lizenz» das passende Zertifikat mit dem Attribut «Produkt» auswählen. Wenn Sie einen Zertifikatguscheinim Webshop erworben haben, geben Sie diese unter «Lizenzcode» ein.

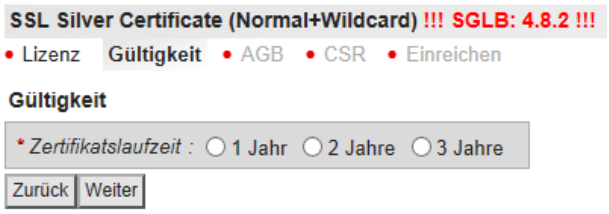


Achtung: Für Benutzer mit Anforderer-Konto kön-

nen nur die Produkte ausgewählt werden, die für dieses Konto freigeschaltet sind.

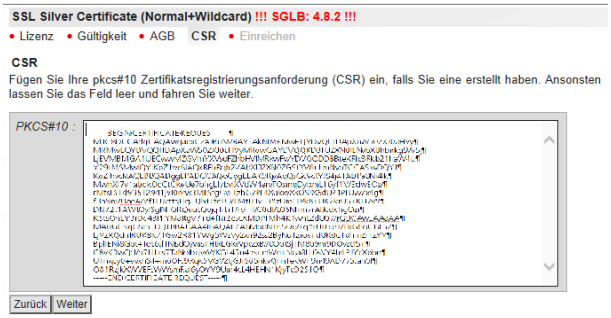
Je nach Einstellung der Managed PKI oder Zertifikatguschein kann das Produkt entweder noch für die Laufzeit konfiguriert werden oder es ist bereits vorkonfiguriert.

Im Falle, dass das Zertifikat nicht für eine Laufzeit vorkonfiguriert ist kann nun die Konfiguration der Laufzeit stattfinden. Ansonsten wird diese Auswahl nicht angezeigt.



Im Arbeitsbereich müssen nun die Teilnehmerbedingungen („Subscriber Agreement“) gelesen und bestätigt werden. Hierzu die Schaltfläche «Ich akzeptiere diese Bedingungen» wählen. Durch Anwahl des Wortes «Aufklappen» kann der gesamte Text der Bedingungen gelesen werden.

Optional: Zertifikatsregistrierungsanforderung (CSR = Certificate Signing Request) eingeben. Für den Benutzer besteht die Möglichkeit, dass er sich extern mit eigenen Tools (z. B. certtool.exe oder OpenSSL) ein Schlüsselpaar erzeugt und nur für den öffentlichen Schlüssel ein Zertifikat anfordert. Diese Anforderung geschieht mittels eines sogenannten CSR, den diese Tools automatisch generieren. Der vom externen Tool generierte CSR Text im PKCS#10 Format ist in das nachfolgende Feld einzugeben und die Schaltfläche «Weiter» zu wählen. Ein typischer Signing Request ist nebenstehend zu sehen.



Sollte der Benutzer sich dafür entscheiden, von SwissSign die Schlüssel generieren zu lassen, so ist das Feld unter PKCS#10 leer zu lassen und nur die Schaltfläche «Weiter» zu betätigen.

Hinweis: Alternativ kann der Benutzer auch SwissSign damit beauftragen für Ihn den privaten und öffentlichen Schlüssel zu generieren. Bei der Generierung des privaten Schlüssels wird dieser sofort mit einem Passwort, welches der Benutzer eingibt, verschlüsselt. SwissSign kennt dieses Passwort nicht und kann dieses auch nicht wieder herstellen. Es ist daher sorgfältig aufzubewahren. Im Falle eines Verlustes sind alle mit diesem Schlüssel verschlüsselten Daten nicht mehr lesbar und können nicht mehr weiterverwendet werden.

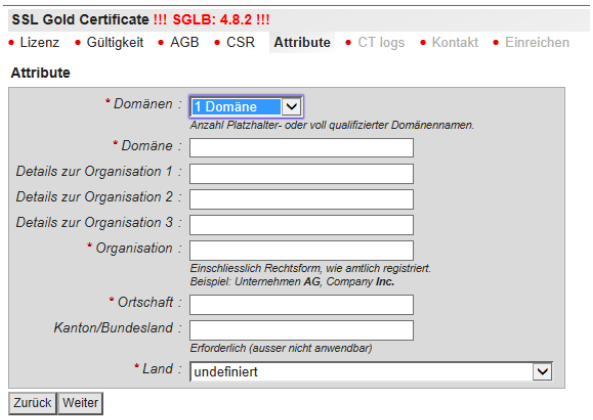
Das von SwissSign generierte SSL Schlüsselpaar bleibt für kurze Zeit (3 Monate) auf der Plattform. Schlüsselpaare für S/MIME Personenzertifikate bleiben während ihrer Laufzeit auf der Plattform und können jederzeit neu unter Verwendung des Passwortes heruntergeladen werden.

Die nachfolgenden Schritte unterscheiden sich jetzt von Zertifikat zu Zertifikat. Daher werden nach den Zertifikatstypen die Unterkapitel getrennt.

4.1.1 Anfordern von SSL Zertifikaten

Nachfolgend ist der typische Ablauf bei der Bestellung von SSL Zertifikaten beschrieben.

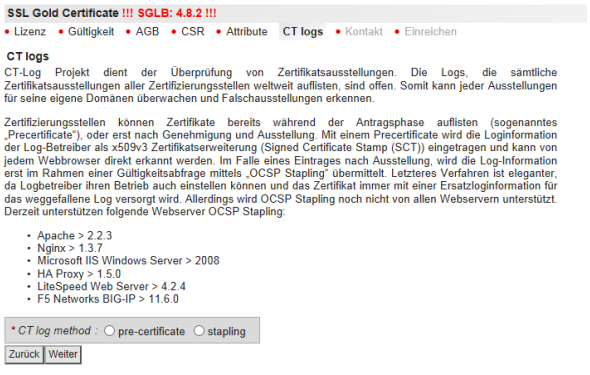
Im Arbeitsbereich ist zunächst die Identität auszufüllen: Zunächst muss dem Zertifikat ein Domänenname vergeben werden, der später auch im Subject des Zertifikates steht. Die Organisation ist im Falle einer Managed PKI vorbelegt, anderweitig kann sie bei z. B. Webshop Nutzern eingegeben werden. Ort, ggfs. Kanton/Bundesland und Staat mit dem Hauptsitz der Organisation sind in den nachfolgenden Feldern einzugeben. Bei Silver Zertifikaten ist nur der Eintrag des Domänennamens verpflichtend. Danach ist die Schaltfläche «Weiter» zu betätigen.



Hinweis: Wurde ein SSL Wildcard Zertifikat angewählt, ist bei der Domäne als erste Subdomäne das Wildcardzeichen („*“) einzugeben, z.B. *.swisssign.com.

Alle Pflichtfelder sind immer mit einem (*) gekennzeichnet.

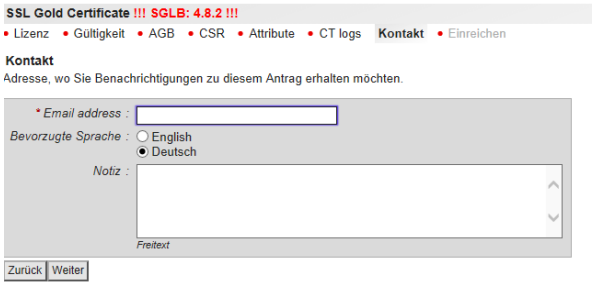
Alle SSL Zertifikate werden in einem Certificate Transparency Log (CT Log) abgespeichert. Das ist eine Anforderung insbesondere von Google Chrome, um Zertifikate als „vertrauenswürdig“ darzustellen. Hintegrund ist die Möglichkeit, über Monitorwerkzeuge immer sich informieren zu lassen, sofern ein Zertifikat (auch durch Betrug oder unabsichtlich) für eine eigene Domäne ausgestellt wird. Der Betrug und die Fehlausstellung soll damit vermieden werden. Für eine CT Log Überprüfung eines Zertifikates gibt es für den Browser zwei Möglichkeiten: Die Logs werden vorab mit einem sogenannten „pre-certificate“ informiert über den Inhalt des auszustellenden Zertifikates und geben hierzu als Bestätigung eine Signatur ab. Diese Signatur wird in das Zertifikat übernommen. Vorteil: Das Zertifikat ist sofort auf jedem Webserver gebrauchsfertig. Nachteil: Das Zertifikat ist sehr umfangreich (mehrere Logs unterzeichnen) und sofern Logs vom Markt verschwinden und weniger als 3 gültige Überschriften übrig bleiben, wird das Zerti-



fikat als gesamtes ungültig. Die zweite Methode trägt das Zertifikat parallel zur Ausstellung in die CT Logs ein und auf dem Webserver wird „OCSP stapling“ aktiviert. Dadurch erhält der Webserver regelmässig eine signierte Gültigkeit von SwissSign. In dieser signierten Gültigkeit werden die signierten Bestätigungen der CT Logs eingepflegt. Das Zertifikat bleibt damit schlanker und erhält immer mindestens 3 CT Log Rückmeldungen, da die CA das Log Handling mit den vorhandenen Logs administriert.

Unsere Empfehlung ist daher, wenn möglich, „stapling“ zu wählen.

Sofern Sie via Konto eingeloggt sind, erhalten Sie nicht mehr die gezeigte Kontakt-Ansicht. In diesem Fall wird als Kontakt der in den Kontoeinstellungen hinterlegte Kontaktdatensatz genommen. Wollen Sie dennoch diesen explizit anpassen, müssen Sie in der Menüzeile oben den Punkt «Kontakt» wählen. Die hier eingegebenen Kontaktdaten überschreiben dann die im Konto hinterlegten Daten – aber nur für das hier angeforderte Zertifikat.



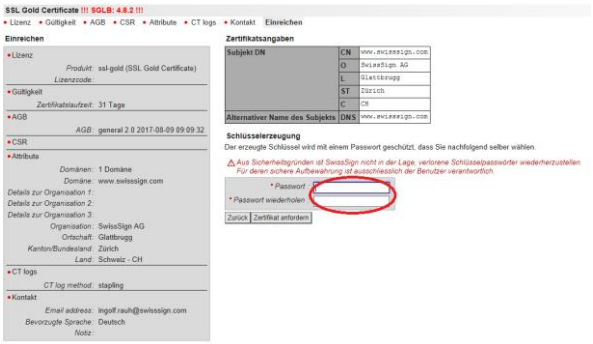
Benutzer ohne Kontologin kommen automatisch auf diese Kontaktseite und füllen die Daten E-Mail-Adresse und bevorzugte Sprache aus. Die E-Mail-Einstellungen wirken sich z. B. auf Hinweis-E-Mails zum baldigen Ablauf von Zertifikaten aus.

Im Feld „Notiz“ können Sie weitere administrative Informationen zu Ihrem Zertifikatsantrag hinterlegen, z.B. das interne Abrechnungskonto oder den Gerätenamen, Ansprechpartner, etc. Diese Informationen fliessen nicht in das Zertifikat, werden aber bei Reports angezeigt.

Anschliessend ist die Schaltfläche «Weiter» zu betätigen.

Jetzt kann das Zertifikat angefordert werden. Alle Zertifikatsdaten werden nochmals angezeigt. Sind eventuell Fehler vorhanden, können die vorherigen Menüs in der Menüzeile oben nochmals angewählt werden und die Daten können angepasst werden. Auch wenn Sie Ihre Daten mittels CSR eingegeben haben können Sie hiermit nochmals Ihre Daten anpassen. Im Falle einer Schlüsselgenerierung durch SwissSign (kein CSR wurde eingegeben) ist im Passwortfeld ein sicherer Schlüssel für den Transfer des Passwortes einzugeben. Anschliessend ist die Schaltfläche «Zertifikat anfordern»

anzuwählen.



Falls Ihr Zertifikat nicht in der MPKI freigeschaltet war, sondern Sie einen Zertifikatsgutschein im Webshop erhalten haben, werden Sie im Falle von Gold und Gold EV Zertifikaten gebeten, ein Antragsformular auszudrucken und unterzeichnen zu lassen. Hierin sind die Organisation und die Domänenzugehörigkeit zu bestätigen.

Sollten Sie Ihr Zertifikat mit Hilfe eines CSR beantragt haben und die dort verwendeten Namen enthalten einen Umlaut, so können Sie im orangen Feld unter «Einreichen» sehen, ob der Umlaut richtig interpretiert wurde. Sollte das nicht der Fall sein, können Sie den Umlautwert korrigieren:

Gehen Sie wieder in der Menüleiste zurück auf das Menü «Attribute».

Die von Ihnen im CSR dargestellten Attribute wurden den Feldern zugeordnet und können editiert werden. Mit «Weiter» kommen Sie dann wieder zu der zuletzt angezeigten «Einreichen» Anzeige.

Hintergrundinformation hierzu: Umlaute werden in Zertifikaten nach UTF-8 Codierung behandelt (http://www.utf8-zeichentabelle.de/unicode-utf8-table.pl?start=128&number=128&names=-&utf8=string-literal). So wird z. B. ein Firmenname «Test und Söhne» wie folgt im Hintergrund codiert: «Test und S\\xc3\\xb6hne». Die Weboberfläche macht das bequem im Hintergrund, bei CSR Eingaben kann es aber immer wieder zu Fehler kommen, je nach Qualität des CSR Tools.

Ein SSL Silver Zertifikat wird ähnlich wie oben beantragt:

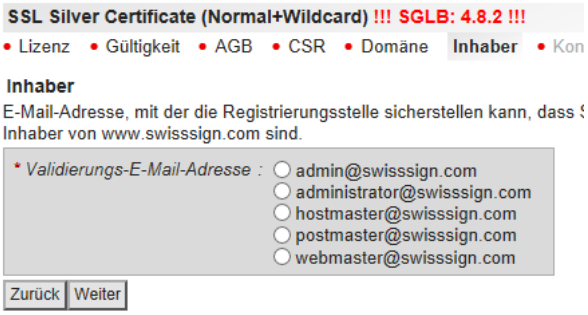
Im Arbeitsbereich ist nur der Domänenname einzugeben. Es muss ein voll qualifizierter Domänenname sein und kein interner Domänenname oder eine IP-Adresse.

Alle Pflichtfelder sind immer mit einem (*) gekenn-

zeichnet.

Sofern Sie eine Domäne eingeben, die mit „www“ beginnt, werden Sie gefragt, ob Sie (kostenfrei) auch die Basisdomäne (ohne „www“) mit in das Zertifikat aufnehmen wollen.

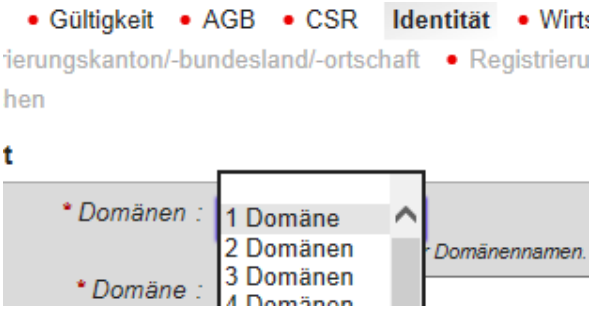
Im Falle, dass Sie nicht ein im Rahmen der MPKI vorgesehenes Silver SSL Zertifikat beantragt haben, sondern eine Zertifikatslizenz aus dem Webshop genutzt haben, müssen Sie die Inhaberschaft bzw. die Zugriffskontrolle auf diese Domäne zeigen. Hierzu wird Ihnen eine E-Mail an ein von Ihnen wahlweise angegebenes E-Mail-Konto, das mit dieser Domäne verbunden ist, versendet.



Der weitere Ablauf ist dann wie beim SSL Gold Zertifikat oben.

Ein Multi-Domain Zertifikat erlaubt den Eintrag von bis zu zweihundert zusätzlichen Domänen zu einer Hauptdomäne:

Die Anzahl der Domänen, die zusätzlich zur Hauptdomäne in das Zertifikat aufgenommen werden soll, muss gewählt werden.

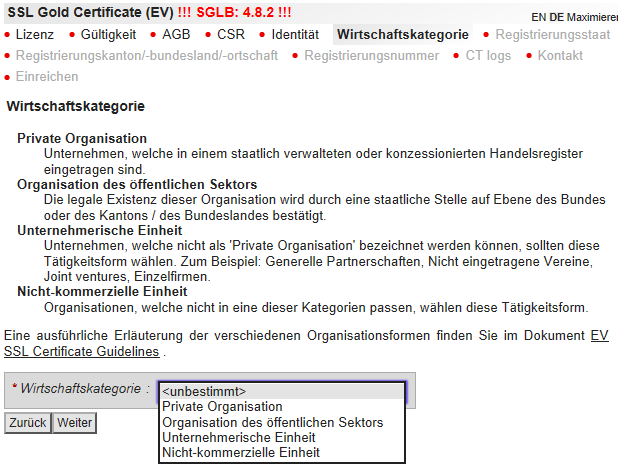


Nach der Auswahl werden die Eingabefelder sofort angezeigt und können entsprechend ausgefüllt werden. Hinweis: Es ist absolut notwendig, dass die Organisation auch im Besitz dieser Domänen ist oder eine Vollmacht des Besitzers vorliegt.

Der weitere Ablauf ist dann wie oben beschrieben.

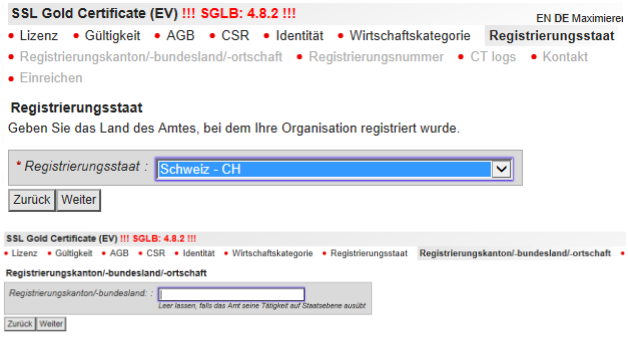
Bei einem SSL EV Gold Zertifikat gilt es noch einige Besonderheiten zu beachten. Im Rahmen der Zertifikatsantragstellung werden noch besondere Angaben abgefragt:

Nach Angabe der Zertifikatsdaten wird noch die Wirtschaftskategorie überprüft. Diese muss mit den Einträgen im Handelsregister oder sonstigem Register übereinstimmen. Bitte orientieren Sie sich auch an den Erläuterungen auf www.swisssign.com (Produkt SSL EV) – Identität.



Auch der Staat und ggfs. Kanton (Bundesland)/Ortschaft, bei der die Organisation registriert wurde, muss angegeben werden.

Hinweis: Es ist zwingend notwendig, dass die zugehörige Registrierungsstelle und Registrierungsnummer unverwechselbar ist. Agiert ein Handelsregister auf Ortsebene, muss hier der Ort, Bundesland und Staat angegeben werden (wie z.B. in Deutschland). Agiert ein Handelsregister auf Kantonalebene (wie z.B. in der Schweiz) ist nur der Kanton und das Land anzugeben.



Die entsprechende Registrierungsnummer ist ebenfalls einzutragen. Bitte beachten Sie, dass hier in der Schweiz die neue UID einzutragen ist.

Der weitere Ablauf ist dann wie oben beschrieben.

Hinweis: Es sind für die von SwissSign generierten Schlüssel sichere Passwörter zu verwenden. Unsichere Passwörter (z. B. zu geringe Länge) müssen explizit bestätigt werden. Passwörter sind sicher aufzubewahren und dürfen nicht verloren gehen. SwissSign kennt diese Passwörter nicht und kann diese im Falle

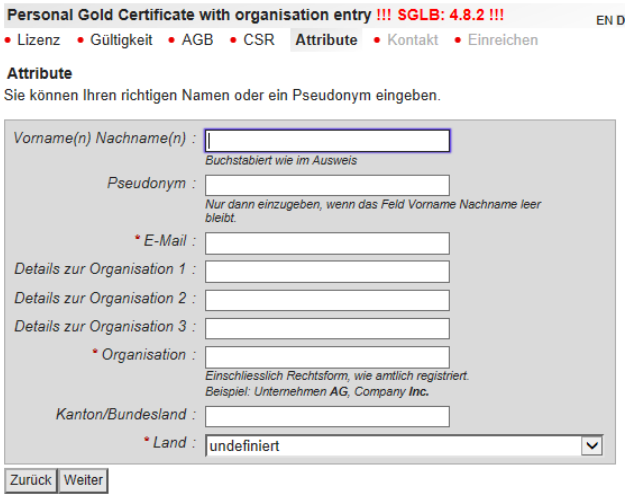
eines Verlustes auch nicht wiederherstellen. Das Zertifikat und die damit verschlüsselten Daten sind dann verloren. Private Schlüssel von SSL Zertifikaten werden nach kurzer Zeit ebenfalls gelöscht, diese sind rechtzeitig vom SwissSign System herunterzuladen.

Bei einer Managed PKI sind nach dem Setup bereits zahlreiche Felder vorbelegt und können nicht verändert werden. Das dient der Sicherheit der regulierungskonformen Ausstellung.

4.1.2 E-Mail Zertifikate (S/MIME)

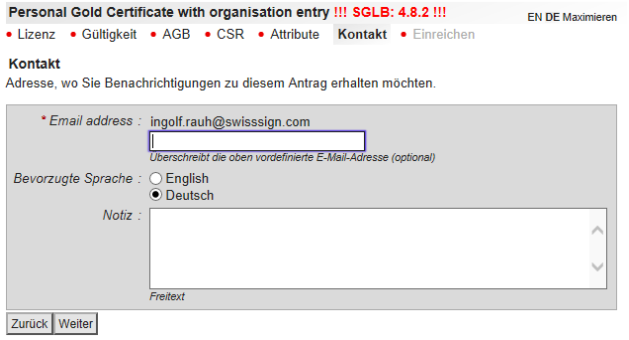
Nachfolgend wird die Vorgehensweise bei E-Mail Zertifikaten beschrieben:

Im Arbeitsbereich sind die Attribute für das E-Mail Zertifikat einzugeben. Alle erforderlichen Felder sind mit einem Stern (*) gekennzeichnet. Im Falle eines Gold Zertifikates werden Vornamen und Nachnamen eingegeben. Auch die Verwendung eines Pseudonyms ist gestattet, dann muss das Feld Vorname/Nachname freigelassen werden. Es ist darauf zu achten, die Namen so zu verwenden, wie sie auch in der eigenen ID/Reisepass geschrieben werden. Im Falle von Silver Zertifikaten ist nur die Eingabe der E-Mail-Adresse notwendig, die Namenseingabe entfällt. Diese muss allerdings bei Anforderung des Zertifikates bereits existent sein. Gold Zertifikate mit Organisationseintrag werden hier mit der Organisation spezifiziert. Danach ist die Schaltfläche «Weiter» zu betätigen.



Pseudonyme können für anonyme Mailboxen oder Gruppenaccounts genutzt werden. Wichtig ist, dass es einen Verantwortlichen für dieses Zertifikat gibt. Namen, die in das Pseudonym Feld eingegeben werden, werden mit dem String „pseudo:“ im Zertifikat dargestellt, z.B. wird das Pseudonym „Sales-Mailbox“ als „pseudo: Sales-Mailbox“ dargestellt.

Sofern Sie mit einem Konto eingeloggt sind, erhalten Sie nicht mehr die gezeigte Kontaktansicht. In diesem Fall wird als Kontakt die in den Kontoeinstellungen hinterlegten Daten genommen. Wollen Sie dennoch diese explizit anpassen, müssen Sie in der Menüzeile oben den Punkt «Kontakt» wählen. Die hier eingegebenen Kontaktdaten überschreiben dann die im Konto hinterlegten Daten – aber nur für das hier angeforderte Zertifikat.



Benutzer ohne Kontologin kommen automatisch auf diese Kontaktseite und füllen die Daten E-Mail-Adresse und bevorzugte Sprache aus. Die E-Mail-Konfiguration wirkt sich z. B. auf Hinweis-E-Mails zum Ablauf von Zertifikaten aus.

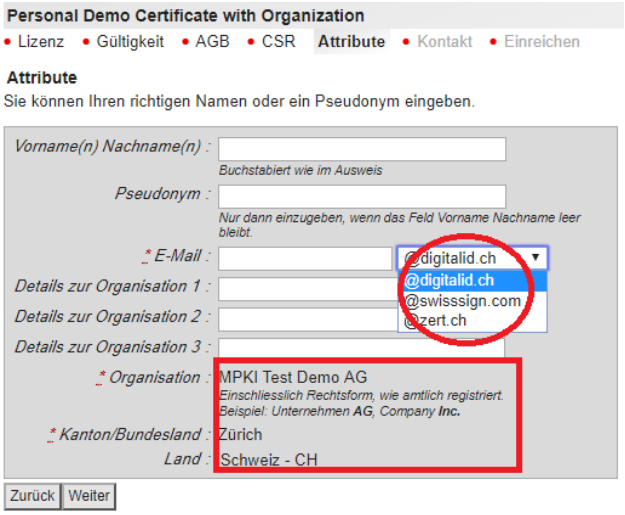
Anschliessend ist die Schaltfläche «Weiter» zu betätigen.

Jetzt kann das Zertifikat angefordert werden. Alle Zertifikatsdaten werden nochmals angezeigt. Sind eventuell Fehler vorhanden, können die vorherigen Menüs in der Menüzeile oben nochmals angewählt und die Daten können angepasst werden. Andernfalls ist im Falle einer Schlüsselgenerierung durch SwissSign im Passwortfeld ein sicherer Schlüssel für den Transfer des Passwortes einzugeben. Anschliessend ist die Schaltfläche «Zertifikat anfordern» anzuwählen.

Im Falle von Gold Zertifikaten, die nicht über die MPKI sondern über eine zusätzliche Webshop-Lizenz erworben wurden, werden die Benutzer gebeten, ein Antragsformular auszudrucken und unterzeichnen zu lassen. Hierin sind die Organisation und die Domänenzugehörigkeit zu bestätigen.

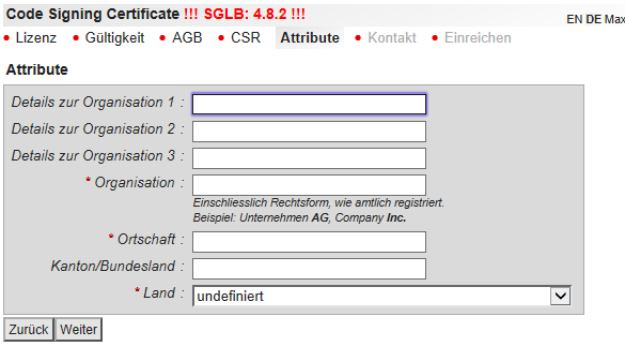
Hinweis: Es sind für die von SwissSign generierten Schlüssel sichere Passwörter zu verwenden. Unsichere Passwörter (z. B. zu geringe Länge) müssen explizit bestätigt werden. Passwörter sind gehörig aufzubewahren und dürfen nicht verloren gehen. SwissSign kennt diese Passwörter nicht und kann diese im Falle eines Verlustes auch nicht wiederherstellen. Das Zertifikat und die damit verschlüsselten Daten sind dann verloren.

Im Rahmen einer Managed PKI können einige Felder bereits vorbelegt sein, z.B. die E-Mail Domäne. Das dient der Sicherheit der regulierungskonformen Ausstellung



4.1.3 Weitere Zertifikatstypen: z. B. Code Signing Zertifikat

Das Ausfüllen erfolgt analog zu den obigen Beispielen. Beim CodeSigning Zertifikat muss mindestens die Organisationsbezeichnung und das Land angegeben werden.



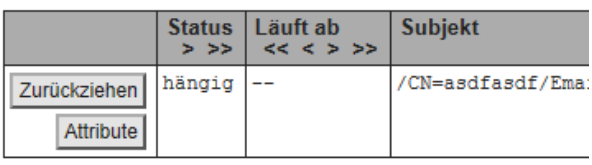
4.2 Zurückziehen von Zertifikatsanträgen

Zertifikatsanträge, die z. B. versehentlich gestellt wurden, können – solange sie nicht genehmigt wurden – zurückgezogen werden. Hierfür ist der zurückzuziehende Antrag zunächst einmal zu suchen.

Im Hauptmenü wird der Menüpunkt «Suchen/Verwalten» angewählt.

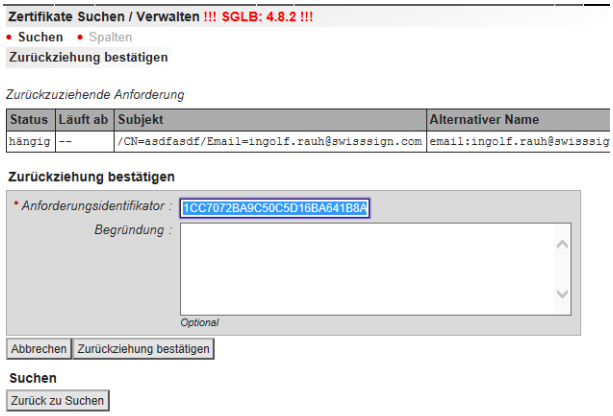
Gibt man im Suchfeld keine weiteren Suchkriterien an, so werden alle eigenen beantragten Zertifikate angezeigt. Anwender, die kein Konto haben und ihr Zertifikat über einen Zertifikatsgutscheincode beantragt haben, geben diesen im Feld „Lizenz“ ein. Damit ist die Berechtigung zum Ändern des Antrages (oder auch später des Zertifikats) freigeschaltet.

Nun kann man den Antrag heraussuchen und den Schaltknopf «Zurückziehen» drücken.

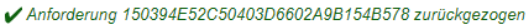


Im nachfolgenden Fenster müssen die Gründe für eine Zurückziehung eingegeben werden (als Freitext).

Danach ist die Zurückziehung zu bestätigen.



Sie erhalten daraufhin eine Bestätigung (auch per E-Mail).



Anwender, die kein Konto haben und den Antrag mittels Gutscheincode gestellt haben, können nun den Gutscheincode wieder für einen neuen Antrag basierend auf demselben Zertifikatstyp nutzen.

4.3 Genehmigungs-Prozess

Die Zertifikatsanträge werden anschliessend vom Zugangsverantwortlichen (Administrator) genehmigt. Das Genehmigungsverfahren ist weiter unten beschrieben.

4.4 Erneuerungs-Prozess

Sobald ein Zertifikat abläuft, muss dieses erneuert werden. Hierzu ist ein neuer Zertifikatsantrag nach oben beschriebenen Ablauf zu stellen. Es gibt (noch) keine Erneuerungsfunktion, die die Werte bereits ausgestellter Zertifikate übernimmt. Es empfiehlt sich das neue Zertifikat bereits 1-2 Wochen zuvor auszustellen und mit dem auslaufenden Zertifikat parallel laufen zu lassen. Im Rahmen der Managed PKI wird eine Überschreitung der Zertifikatsanzahl um 10% geduldet, insofern ist diese parallele Nutzung von zwei Zertifikaten binnen dieser Zeit nicht relevant für die Abrechnung.

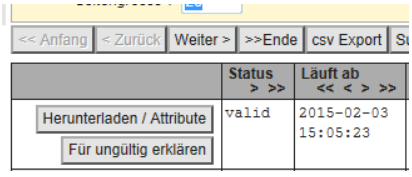
4.5 Ungültigkeitsprozess (Revokation)

Der Anforderer kann selber Zertifikate für ungültig erklären, sogenannt «revozieren». Hierfür loggt er sich unter seinem Login ein und sucht das entsprechende Zertifikat. Bitte beachten Sie, dass ein RAO ein Anfordererkonto so konfigurieren kann, dass Revokationen nicht möglich sind.

Im Hauptmenü wird der Menüpunkt «Suchen/Verwalten» angewählt.

Gibt man im Suchfeld keine weiteren Suchkriterien an, so werden alle eigenen beantragten Zertifikate angezeigt. Anwender, die kein Konto haben und ihr Zertifikat über einen Zertifikatsgutscheincode beantragt haben, geben diesen im Feld „Lizenz“ ein. Damit ist die Berechtigung zum Ändern des Zertifikats freigeschaltet

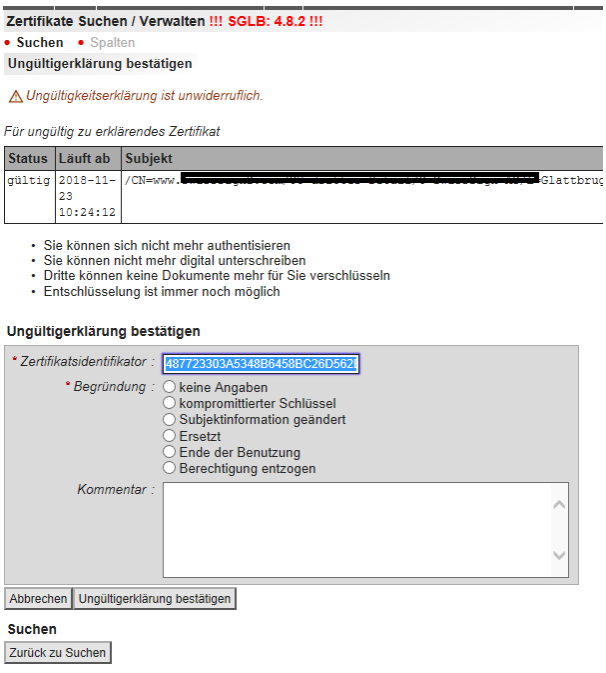
Nun kann man das Zertifikat heraussuchen und den Schaltknopf «Für ungültig erklären» drücken.



Im nachfolgenden Fenster müssen die Gründe für eine Ungültigkeitserklärung eingegeben werden:

- Keine Angaben
- Kompromittierter Schlüssel: Der private Schlüssel wurde gestohlen bzw. es besteht die Gefahr, dass er gestohlen wurde.
- Subject-Information geändert, z. B. Änderung des Firmennamens, oder Nachnamens.
- Ersetzt: Das Zertifikat wurde durch ein anderes ersetzt.
- Ende der Benutzung: Das Zertifikat wird nicht mehr weiter benötigt, z. B. Austritt eines Mitarbeitenden aus dem Unternehmen.
- Berechtigung entzogen, z. B. aufgrund von nicht bezahlten Zertifikatslizenzen.

Optional kann auch ein Kommentar abgegeben werden.



Ein Zertifikatsgutschein gilt als verbraucht und wird durch das Zurückziehen eines Zertifikates nicht wieder freigegeben.

Hinweis: Eine abgegebene Ungültigkeitserklärung kann nicht mehr revidiert werden. Das Zertifikat wird als ungültig markiert in allen Listen (CRL) oder Diensten (OCSP), die bei einer Zertifikatsgültigkeitsanfrage herangezogen werden.

5. Management der Zertifikatsgutscheine

5.1 Ausstellen von Zertifikatsgutscheinen

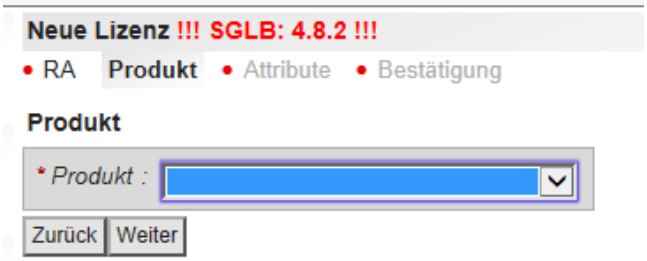
Ein Zugangsverantwortlicher hat die Möglichkeit, insbesondere für Benutzergruppen, die über kein Anforderkonto verfügen, Lizenzen für einen Zertifikatsbezug zu übermitteln. Damit kann dieser Nutzer entweder ohne Konto auf swisssign.net oder mit einem selbst erstellten Konto ein Zertifikat beziehen.

Hinweis: Die Software nutzte historisch das angelsächsische Wort license (zunächst mit Lizenz übersetzt) für die Gutscheine bzw. Gutscheincodes. Es handelt sich hierbei aber nicht um den juristischen Begriff einer Lizenze (z.B. für ein künstlerisches Werk oder eine Softwarenutzung). Im Laufe der Releases wird die Benutzerführung überarbeitet und das Wort „Lizenz“ durch „Zertifikatsgutschein“ ersetzt.

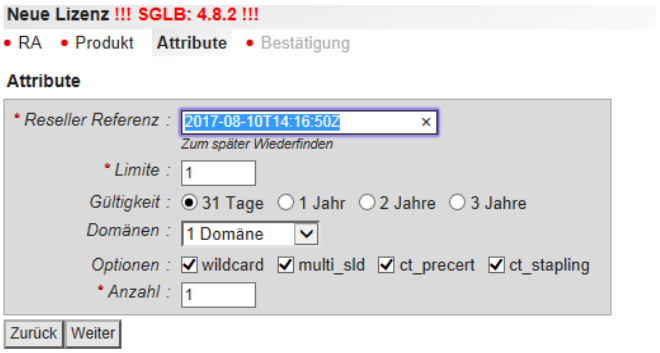
Zunächst wählt der RAO im Hauptmenü den Punkt „Neu“ im Submenü „Lizenzen“ an.

Sofern für die Managed PKI mehrere RAs konfiguriert sind, muss zunächst die für das Gutscheinprodukt verantwortliche RA ausgewählt werden.

Danach muss das Produkt ausgewählt werden.

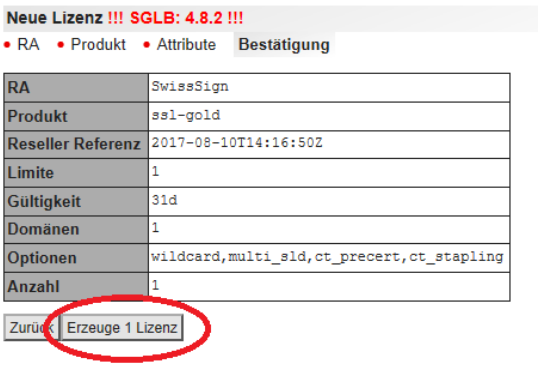


Nun müssen Daten zum Gutscheincodeeingegeben werden:

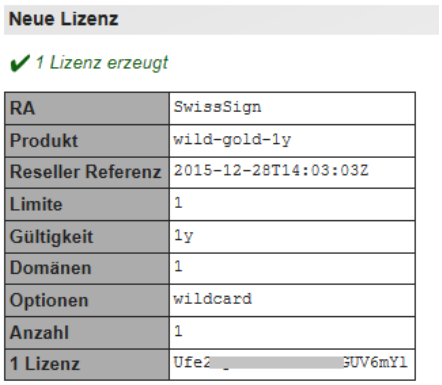


- Reseller Referenz: Ein selbstgewählter String, unter dem man später den Gutschein für Verwaltungs- oder Abrechnungszwecke wiederfinden kann.
- Limite: Nutzungslimit, gibt an wie häufig ein- und derselbe Code eingesetzt werden darf. Damit lässt sich eine Dauerlizenz erzeugen, die z.B. 50x eingesetzt werden kann.
- Gültigkeit: Laufzeitdauer des Zertifikats (sofern nicht im Produkt vorkonfiguriert)
- Domänen: Kann nur bei einem Multi-Domänenzertifikat konfiguriert werden. Anzahl der Domänen bis 200.
- Optionen: DIESE SOLLTEN NICHT VERÄNDERT WERDEN! Die Optionen sind:
  multi_sld: Für Multidomänenzertifikate, eine Deaktivierung lässt dann nur Subdomänen einer Hauptdomäne zu.
  self_validation: ermöglicht die Selbstvalidierung bei Personenzertifikaten Silver
  wildcard: ermöglicht Wildcardeinträge im SSL Gold oder SSL Silver Zertifikat
  ct_precert: Ermöglichen der Ausstellung eines Precertificates für CT Log
  ct_stapling: Ermöglichen einer OCSP Stapling Antwort mit CT Log Signaturen
- Anzahl: Anzahl der zu erzeugenden Zertifikatgutscheine

Mit „Weiter“ und „Erzeuge 1 Lizenz“ werden nun die Zertifikatgutscheincodes erzeugt.



Der Gutscheincode unter „1 Lizenz“ kann nun weitergegeben werden an den Benutzer, der diesen Gutschein gegen einen Zertifikatsantrag einlösen möchte.



5.2 Einlösen von Zertifikatsgutscheinen

Ein beliebiger Nutzer hat nun die Möglichkeit, den erzeugten Gutscheincod entweder mit oder ohne Konto auf swisssign.net einzulösen.

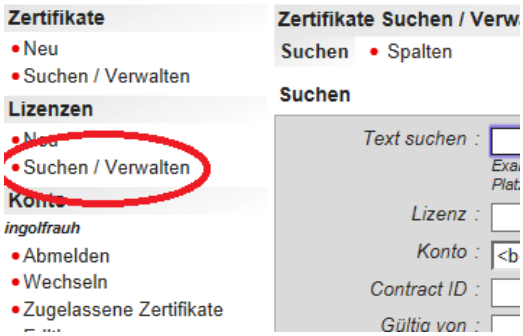
Ohne Login kann ein Nutzer direkt im Hauptmenü den Punkt „Neu“ wählen und den Zertifikatsgutscheincode eingeben. Für alle Operationen, die im Nachhinein einen bestehenden Zertifikatsantrag oder ein bestehendes Zertifikat ändern sollen, muss dann der Antrag oder das Zertifikat über „Suchen/Verwalten“ durch Eingabe dieses Codes gesucht werden.

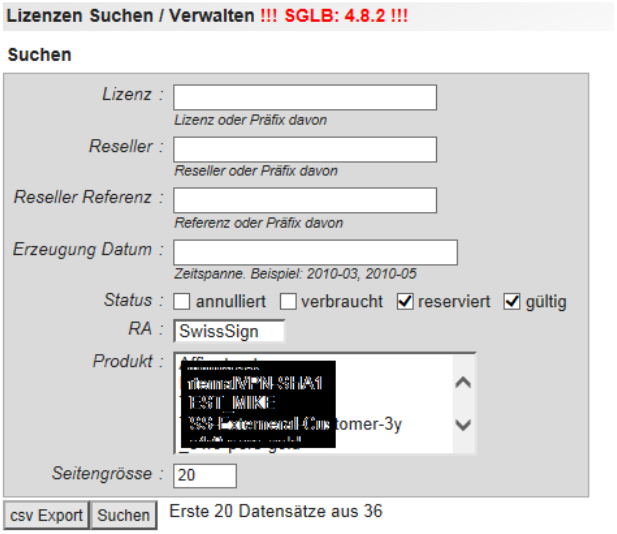
Auch als Nutzer mit einem Konto oder eines Kontos innerhalb einer Managed PKI kann der Zertifikatsgutscheincode mit „Neu“ genutzt werden.

5.3 Gutscheincodesuche und Verwaltung

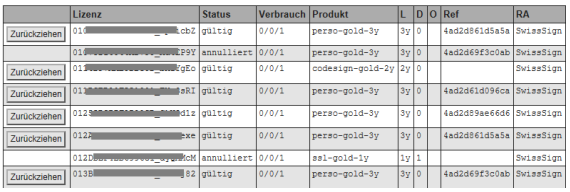
Der Zugangsverantwortliche und Auditor hat die Möglichkeit die ausgestellen Lizenzen zu verwalten oder nach Ihnen zu suchen.

Die Verwaltung/Suche wird im Hauptmenü unter „Suchen/Verwalten“ im Submenüpunkt „Lizenzen“ ausgewählt. Es kann nun eine Suche und Anzeige nach mehreren Suchkriterien erfolgen:





- Lizenz: Suche nach einem Gutscheincode. Es können auch nur die ersten Zeichen des Gutscheincodes eingegeben werden, ein Wildcardzeichen ist in diesem Falle nicht einzufügen.
- Reseller: Code eines Resellers (der von SwissSign vergeben wurde)
- Reseller Referenz: Suche nach einer Referenz, die bei Bestellung durch den Aussteller gegeben wurde. Auch hier reichen die ersten Zeichen.
- Erzeugung Datum: Datum der Erzeugung.
- Status: Status des Gutscheincodes:
  annulliert: Gutscheincode, der zurückgezogen wurde und nicht mehr gültig ist.
  verbraucht: Gutscheincode, der bereits für ein Zertifikat eingesetzt wurde und wo das Zertifikat ausgestellt wurde.
  reserviert: Gutscheincode, der bereits für einen Zertifikatsantrag verwendet wurde. Das Zertifikat wurde aber noch nicht ausgestellt.
  gültig: gültige, nicht eingesetzter Gutscheincode.
- Produkt: betreffendes Zertifikatsprodukt



Die Auswertetabelle zeigt nun alle ausgestellten Zertifikate an. Hierbei können noch nicht zurückgezogene (annulierte) Gutscheincodes zurückgezogen werden.

Die Überschriften, bedeuten folgendes:

- Lizenz: erzeugter Code
- Status (wie oben)
- Verbrauch: Die letzte Ziffer gibt an, wie häufig dieser Gutscheincode zum Einsatz gelangen darf. Die erste Ziffer zeigt die Anzahl der Einsätze die zum Status „reserviert“ geführt haben, die zweite (mittlere) Zahl die Anzahl der bereits eingesetzten Zertifikate.
- Produkt: Produkt, welches mit dem Gutscheincode gekoppelt ist
- L: Laufzeit in Jahren(y), Monaten (m) oder Tagen (d).
- D: Anzahl der Domänen
- O: herangezogene Optionen, siehe 5.1
- Reseller: die von SwissSign vergebene Resel-

leridentifikation
- Ref: Der von Ihnen gewählte Referenzstring bei der Erzeugung des Zertifikates
- RA: Die Registrierungsstelle, unter der das Produkt ausgestellt wird.
- Erzeugt: Wann der Gutschein angelegt wurde
- Zuletzt geändert: Letzte Änderung am Gutscheindatensatz

6. Management von Zertifikaten

6.1 Wahl der Rechte

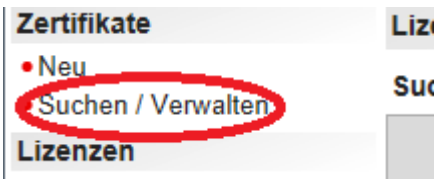
Je nach gewählter Benutzerrolle können Zertifikate verwaltet werden. Auch ein Benutzer ohne Login hat z. B. Möglichkeiten, öffentliche Zertifikate zu suchen. Die folgende Übersicht zeigt die Möglichkeiten:

Rechte	Möglichkeiten
Ohne Login	• Suche öffentlicher E-Mail Zertifikate • Anzeige der Ergebnisse • Zertifikatsattribute anzeigen • Herunterladen bestimmter Zertifikate für die verschlüsselte E-Mail Kommunikation
Login als Benutzer, der kein Administrator ist	• Suche von eigenen Zertifikaten • Anzeige der Ergebnisse • Zertifikatsattribute anzeigen • Herunterladen seiner Zertifikate, sofern er Anforderer-Rolle hat. • Änderung von Attributen eigener Zertifikate • Herunterladen der für einen selbst generierten Schlüssel mit Passwort
Login als Zugangsverantwortlicher	Alle Funktionen, die in den nachfolgenden Unterkapiteln beschrieben sind.

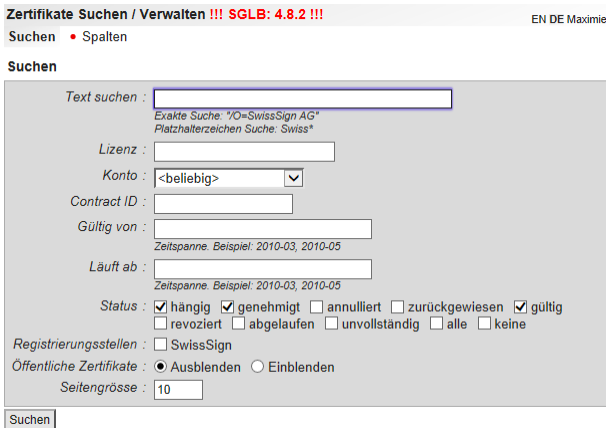
Hinweis: Möchte ein Zugagnsverantwortlicher ein anderes Konto ausführen, so hat er sich explizit zunächst auszuloggen und dann mit dem Konto (inklusive Login) fortzufahren.

6.2 Suche von Zertifikaten

Im Hauptmenü wird unter dem Label «Zertifikate» der Menüpunkt «Suchen/Verwalten» gewählt.



In dem Arbeitsbereich kann jetzt nach einem Gutscheincode (Lizenz) oder alternativ nach einem Text gesucht werden, der ein Zertifikat enthält. Das Platzhalterzeichen «*» kann im letzten Fallverwendet werden.



Je nach Rolle können auch mehr Suchattribute zur Verfügung gestellt werden, z. B. der Status der Zertifikate oder Zertifikatsanträge (z. B. «pending»).

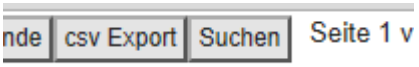
Die Anzahl der Ergebnisse ist auf die unter «Seitengrösse» eingestellte Anzahl von Zertifikaten begrenzt. Die Anzahl kann angepasst werden.

Ohne Eingabe von Suchkriterien werden die eigenen Zertifikate angezeigt.

Hinweise:

- Die Anpassung der Anzahl der Ergebnisse (Seitengrösse) auf grosse Zahlenwerte kann zu langen Abfragezeiten führen. Will man die Ergebnisse später exportieren (z. B. in Excel), werden immer nur die angezeigten Ergebnisse exportiert. Gegebenenfalls empfiehlt es sich dann, die Anzahl der angezeigten Ergebnisse so hochzusetzen, dass alle Ergebnisdatensätze angezeigt werden. Diese können dann alle in Excel exportiert werden.
- Die Suche nach öffentlichen Zertifikaten ist immer auf die Anzeige des betreffenden E-Mail Zertifikates beschränkt und kann nur mit einem Filter (z. B. Eingabe der E-Mail Adresse) durchgeführt werden.

Ausgegebene Datensätze können unter «csv Export» exportiert werden und z. B. nach Excel importiert werden.

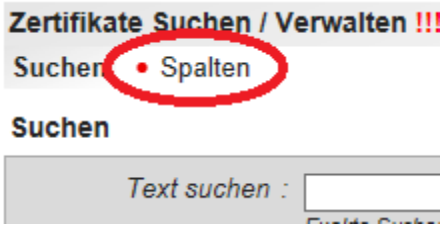


6.3 Anzeige der Ergebnisse

Die Anzeige einzelner Attribute zu einem Zertifikat kann bequem gesteuert und festgelegt werden:

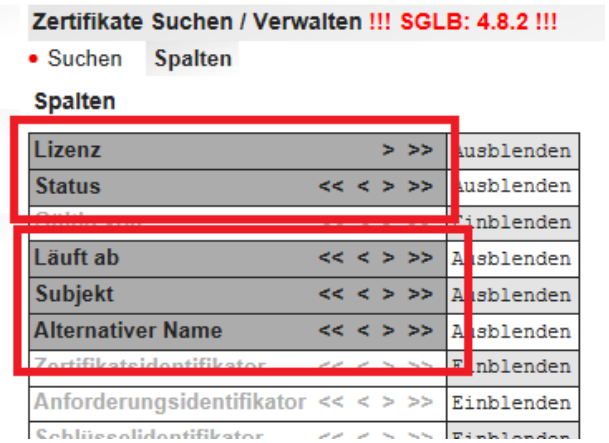
Sofern Sie nicht bereits im «Suchen/Verwalten» Menü sind, wählen Sie dieses im Hauptmenü unter «Zertifikate», Menüpunkt «Suchen/Verwalten».

In der Menüleiste oben wählen Sie den Menü Tab «Spalten».

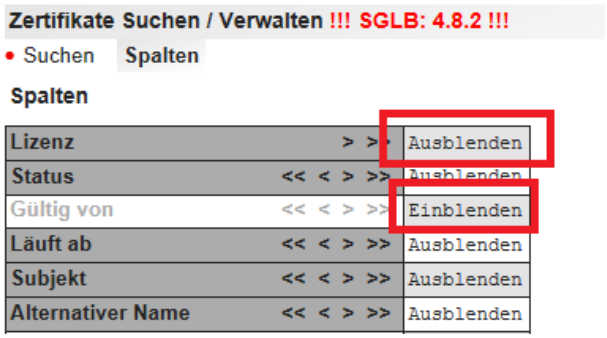


Sie sehen nun eine Tabelle von Attributen jeweils rechts versehen mit einer Schaltfläche «Einblenden» oder «Ausblenden».

Diejenigen Attribute, die derzeit in der Ergebnistabelle der Suche angezeigt werden, sind grau hinterlegt und markiert. Die anderen möglichen Attributwerte sind weiss hinterlegt und nicht markiert.

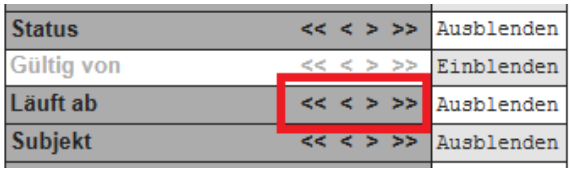


Attributspalten in der Ergebnisliste können nun durch die Betätigung des Schalters «Einblenden» oder «Ausblenden» ein- bzw. ausgeschaltet werden.



Über die Pfeiltasten «<» oder «>» können Spalten in der Ergebnistabelle um eine Position nach links oder rechts verrückt werden, analog auch in der Attributs Liste oben.

Mit den Doppelpfeiltasten «<<» bzw. «>>» kann gezielt eine Spalte an das linke oder rechte Ende der Tabelle bewegt werden.

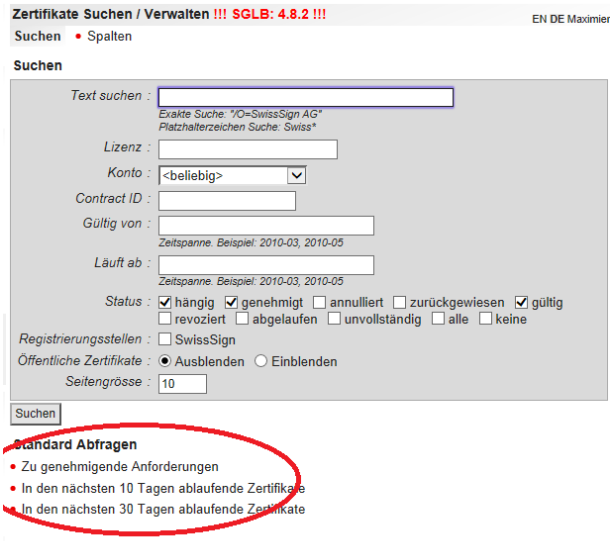


Durch die Zusammenstellung der wesentlichen Attributdaten kann flexibel ein individueller Report über alle Zertifikate oder Zertifikatsanträge erstellt werden.

6.4 Genehmigung, Ausstellung, Zurückweisung und Revokation

Ein Zugangsverantwortlicher hat die Aufgabe, Zertifikatsanträge zu genehmigen oder zurückzuweisen. Er folgt hierbei den mit SwissSign im Managed PKI Setup Agreement festgelegten Regeln, z. B. bei der Überprüfung der Person, auf die das Zertifikat ausgestellt werden soll. Ist der Zertifikatsantrag genehmigt, so kann das Zertifikat ausgestellt werden. Ist das Zertifikat nicht mehr gültig oder wurde kompromittiert, so muss es wiederrufen werden («Revokation»).

Zunächst sind die Zertifikate zu suchen, für die entsprechende Aktionen auszulösen sind.

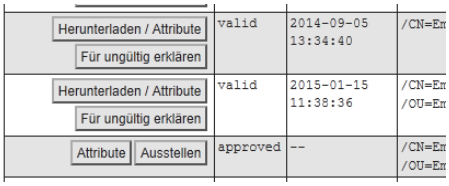


Beispielsweise können für den Prozess der Genehmigung oder Zurückweisung alle hängigen Zertifikatsanträge ausgewählt werden. Hier ist dann z. B. die Checkbox «pending» zu wählen. Alternativ sind häufige Standard Abfragen für Administratoren auch als Hyperlink neben der Suchmaske angezeigt:

- Zu genehmigende Anforderungen: Alle Anforderungen, die anstehen für eine Anforderung
- In den nächsten 10 Tagen ablaufende Zertifikate
- In den nächsten 30 Tagen ablaufende Zertifikate

Für die Revozierung können bestimmte Zertifikate mit einer bestimmten Subject-Bezeichnung gesucht werden.

Neben den Zertifikaten in der Ergebnisliste werden jetzt die einzelnen Aktionsknöpfe angezeigt. Im nebenstehenden Beispiel kann z. B. ein Zertifikat für ungültig erklärt werden. Es werden nur die Aktionen zugelassen, die für das Zertifikat möglich sind. So kann z. B. nur ein Zertifikatsantrag genehmigt werden. Zertifikate für bereits genehmigte Zertifikatsanträge können ausgestellt werden, so dass der Benutzer sie herunterladen kann. Grundsätzlich können auch Zertifikate heruntergeladen werden oder man kann die Attribute eines Zertifikates ansehen.

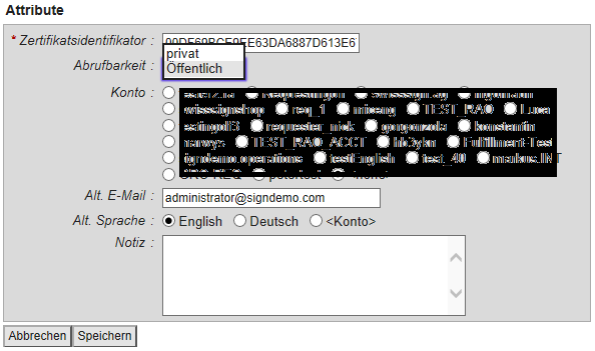


Alle Zertifikate mit Abrufbarkeit «Public download» können von beliebigen Benutzern angezeigt und ohne privaten Schlüssel heruntergeladen werden (z.B. E-Mail Zertifikate). Andere Zertifikate sind für unberechtigte Benutzer nicht sichtbar.

6.5 Attribute/Abrufbarkeit anzeigen/ändern, Download, Übertragung von Zertifikaten

Man kann im Nachhinein einige Attribute, die mit dem Zertifikat verknüpft sind, ändern. Hierfür ist in der Ergebnisliste zunächst die Schaltfläche «Attribute» anzuwählen.

Anschliessend können im Arbeitsbereich unter «Attribute» Einstellungen vorgenommen werden:

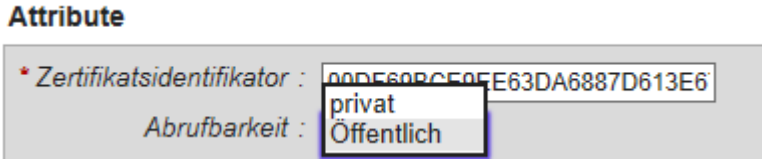


- Die E-Mail für die Notifikation 10 oder 30 Tage vor dem Zertifikatsablauf kann für dieses Zertifikat unter «Alt. E-Mail» angepasst werden, auch die dazugehörige Sprache unter «Alt. Sprache» (Alternative Sprache).
- Im Notizfeld kann eine beliebige Notizzuordnung zu diesem Zertifikat verändert werden (z.B. die Beschreibung des Gerätes, des Geräteverantwortlichen oder der Kostenstelle.

- Die Abrufbarkeit des Zertifikates auf dem swisssign.net Zertifikatsverzeichnis kann über eine Auswahlliste geändert werden.
- Sind mehrere Konten vorhanden, so kann das Zertifikat auch einem anderen Konto hierüber zugeordnet werden. Die entsprechende Checkbox für das Konto ist dann anzuwählen.

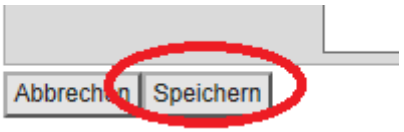
Die Abrufbarkeit kann auf zwei Werte angepasst werden:

- Privat
- Öffentlich



Im Falle von «privat» wird auf swisssign.net Ihr Zertifikat nicht für aussenstehende Benutzer angezeigt. Im Falle von «öffentlich » kann Ihr Zertifikat nur für andere auf Gültigkeit geprüft werden und alle Details Ihres Zertifikats sind für jedermann im Falle über die Suche oder LDAP sichtbar.

Alle Änderungen sind mit der Betätigung der Schaltfläche «Speichern» abzuschliessen.



7. CAA (Certificate Authority Authorization (RFC 6844)

SwissSign unterstützt den CAA Standard. D.h. sofern Sie in Ihrem Domänennamensservice (DNS) festgelegt haben, dass nur Zertifikate einer anderen Zertifizierungsstelle ausgestellt werden dürfen, verweigert das SwissSign CA System die Ausstellung der Zertifikate. Zur richtigen Konfiguration von CAA wenden Sie sich an unser FAQ auf www.swisssign.com

8. LDAP Einstellungen

SwissSign bietet auch die Auskunft über die Zertifikate über den Dienst „LDAP“ an. Die LDAP Schnittstelle wird von vielen Programmen (z.B. Outlook) genutzt und ermöglich so eine automatisierte Signatur oder Verschlüsselung, sofern der Kommunikationspartner bei SwissSign ein Zertifikat hat und wie im vorherigen Abschnitt gezeigt, dieses für die öffentliche Suche freigeschaltet hat.

Bei der Konfiguration von LDAP wenden Sie sich an die Anleitungen Ihrer E-Mail Software. Folgende Einstellungsparameter sind einzugeben:

Servername: directory.swisssign.net

Port:389

Suchbasis: o=SwissSign,c=CH

9. Domänenverwaltung

Als Zugangsverantwortlicher haben Sie die Möglichkeit im Rahmen des vom CA Browser Forums zugelassenen Verfahrens neue Hauptdomänen für die Managed PKI zu beantragen und automatisch prüfen zu lassen.

Folgende Verfahren sind dabei zulässig, um Ihren Zugriff auf die genannten Hauptdomänen zu prüfen:

a. TXT Check
In einer Textdatei unter dem Pfad:
<domain>/.well-known/pki-validation/swisssign-check.txt

Der Inhalt des Texts Datei muss wie folgt formatiert sein: <random value>
Es sind keine Weiterleitungen zugelassen!

b. HTML META TAG Check
Als <meta> Tag einer HTML Datei unter dem Pfad:
<domain>/.well-known/pki-validation/swisssign-check.htm

Der Inhalt des Meta Tags muss wie folgt formatiert sein:
<meta name="swisssign-check" content="<random value>" />
Es sind keine Weiterleitungen zugelassen!

c. DNS Eintrag
Als TXT Eintrag im DNS der Domäne.
Der Inhalt muss wie folgt formatiert sein:
"swisssign-check=<random value>"

Die spitzen Klammern <> beim <random value> dienen nur zur Illustration und müssen weggelassen werden.

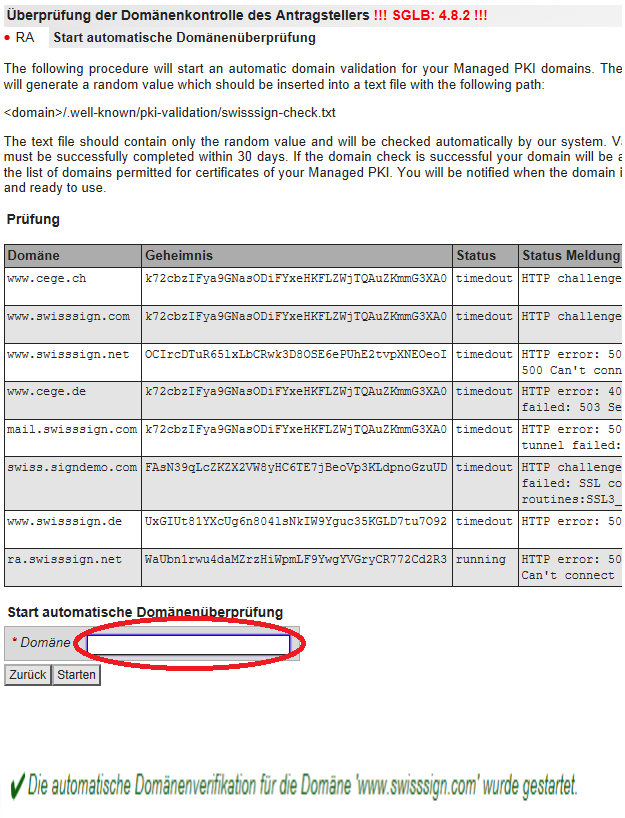
Im Rahmen der beschriebenen automatischen Verfahren prüft das System 30 Tage lang, ob Sie das Geheimnis an einer der 3 Stellen hinterlegt haben. Sobald eine der drei Prüfungen Erfolg zeigt, wird unser Fulfillment automatisch angewiesen, die Domäne Ihrer Managed PKI hinzuzufügen. Sie können dann für diese Domäne und deren Subdomänen E-Mail Zertifikate und SSL Zertifikate ausstellen.

Melden Sie sich als Zugangsverantwortlicher an.

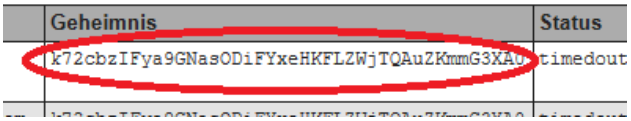
Rufen Sie im Hauptmenü die den Menüpunkt „Domäne verwalten“ im Rahmen des Menübereichs „MPKI Domänen Verifikation“ auf.

Der Ablauf der Domänenüberprüfung wird nochmals kurz beschrieben. Mit Aktivierung des „Weiter“ Knopfes gelangen Sie zur Eingabe Ihrer Domäne.

Geben Sie nun Ihre zu überprüfende Hauptdomäne ein. Sofern die Hauptdomänen zugelassen sind, sind auch die Subdomänen dieser Hauptdomäne in der Managed PKI zugelassen.



Sie erhalten ein Geheimnis angezeigt welches Sie ohne weitere Zusätze in eine swisssign-check.txt Datei einsetzen, oder welches Sie in Form eines

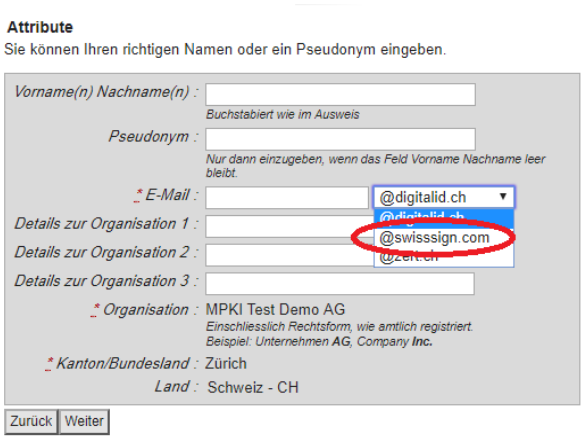


<meta> Tags in eine Seite swisssign-check.htm einsetzen können. Die Datei oder Seite muss unter <Domäne>/.well-known/pki-validation auffindbar und von aussen durch SwissSign zugänglich sein. Alternativ kann das Geheimnis auch in einen TXT record Ihrer Domain Name Services (DNS) eingesetzt werden. Hierbei ist die Form „swisssign-check=<Geheimnis>“ zu wählen.

Der Statusmeldung können Sie entnehmen, ob die automatische Überprüfung erfolgreich war, oder ob es z.B. mit der Firewall und Erreichbarkeit Probleme gegeben hat. Eventuelle Problemmeldungen und Zeiten der letzten Überprüfung helfen ggfs. Ihrem und dem SwissSign Support bei Erreichbarkeitsproblemen.

Status Meldung	Letzte Überprüfung
HTTP challenge file is redirection. HTTPS error: 404 Not Found	2017-07-28 08:00:00.000000 UTC
HTTP challenge file is redirection. HTTPS error: 404 Not Found	2017-07-28 08:00:00.000000 UTC
HTTP error: 500 Can't connect to www.swisssign.net:80. HTTPS error: 500 Can't connect to www.swisssign.net:443	2017-07-28 08:00:01.000000 UTC
HTTP error: 404 Not Found. HTTPS error: 500 establishing SSL tunnel failed: 503 Service Unavailable	2017-07-28 08:00:01.000000 UTC
HTTP error: 503 Service Unavailable. HTTPS error: 500 establishing SSL tunnel failed: 503 Service Unavailable	2017-07-28 08:00:01.000000 UTC
HTTP challenge file is redirection. HTTPS error: 500 SSL upgrade failed: SSL connect attempt failed error:14090086:SSL routines:SSL3_GET_SERVER_CERTIFICATE:certificate verify failed	2017-07-31 14:00:00.000000 UTC
HTTP error: 500 read timeout. HTTPS error: 500 read timeout	2017-08-05 09:00:00.000000 UTC
HTTP error: 500 Can't connect to ra.swisssign.net:80. HTTPS error: 500 Can't connect to ra.swisssign.net:443	2017-08-10 14:00:00.000000 UTC

Sobald die Domäne vom SwissSign Fulfillment einem letzten Check unterworfen und für Ihre Managed PKI freigeschaltet wurde, erhalten Sie ein E-Mail. Die Domäne kann nun im Rahmen der Managed PKI bei der Bestellung eines Zertifikates ausgewählt werden.



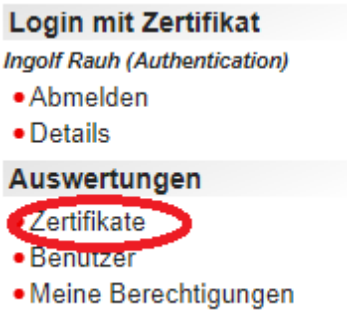
10. Auswertungen

Diese Auswertungen kann nur der Zugangsverantwortliche oder Auditor aufrufen.

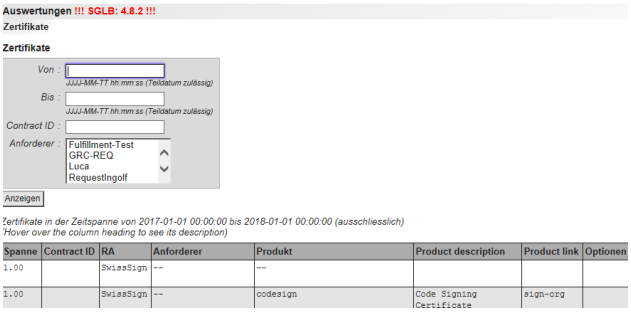
10.1 Zertifikate

Melden Sie sich als Zugangsverantwortlicher oder Auditor an.

Rufen Sie im Hauptmenü die Auswertung «Zertifikate» auf.



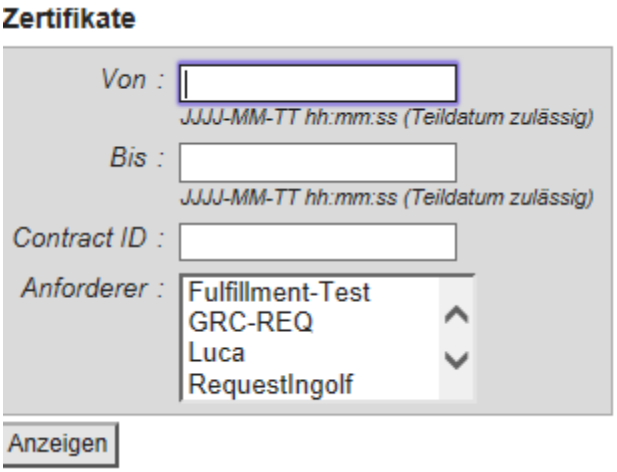
Die Auswertung wird nun angezeigt. Sie kann über das Suchfenster parametrisiert werden.



Folgende Parameter können eingegeben werden:

- Von: Betrachtungszeitraumbeginn, es ist auch nur das Datum (ohne Uhrzeit) zulässig.
- Bis: Betrachtungszeitraum Ende
- Contract ID: Vertragskundennummer (wird von SwissSign vergeben)
- Betroffene RA

Anforderer: Zertifikate eines Anforderers werden angezeigt.



Der Menüpunkt «Zertifikate» im Hauptmenü gibt eine Ansicht über folgende Parameter:

- Jahre: Betrachtungszeitraum der Auswertung. Eine Auswertung über ein halbes Jahr zeigt hier 0.5 an, eine Auswertung über ein Jahr 1.0. Standardmässig wird ohne Parametrisierung immer die Auswer-

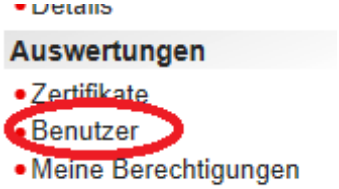
tung vom ersten Tag des laufenden Monats im vergangenen Jahr bis zum ersten Tag des Monats im laufenden Jahr angezeigt.

- Contract ID: Vertragskundennummer (wird von SwissSign vergeben)
- RA: Registrierungsstelle
- Anforderer: Diese Spalte zeigt den Anforderer an. Wurden die Zertifikate durch den Zugangsverantwortlichen an-gefordert, bleibt der Eintrag leer.
- Produkt: Hier wird das Zertifikatsprodukt inklusive Laufzeit angezeigt, z. B. personal-silver-1y für ein Personal Silver ID Zertifikat mit einjähriger Laufzeit.
- Produkt Beschreibung: Hier wird das Zertifikatsprodukt beschrieben gemäss der kommerziellen Bestellung des Managed PKI Vertrages.
- Optionen: Produktoptionen, die gesetzt werden (z.B. Multidomänenfähigkeit, Eintrag in das CT Log, Wildcardfähigkeit, etc.)
- Gültigkeit: Dauer der Gültigkeit des konfigurierten Produktes
- CA: Das ist die ausgebende CA, die das Zertifikat ausgegeben hat.
- Gültig: Am Endtag der Betrachtungsperiode Anzahl der gültigen Zertifikate.
- Effektiv: Es werden alle Zertifikate multipliziert mit der Zeitperiode, in denen sie innerhalb des Betrachtungszeitraumes gültig waren, und dividiert durch den Betrachtungszeitraum. Beispiel: Hatte man 10 Zertifikate zum 1. Januar eines Jahres und 10 weitere ein halbes Jahr später, so ergibt sich die effektive Anzahl von 15 Zertifikaten über den Betrachtungszeitraum 1.1. bis 31.12 des Jahres. Diese Berechnung wird als Grundlage für etwaige Nachverrechnungen genommen. Insofern werden unterjährig ausgestellt Zertifikate nicht voll in eine Nachverrechnung hineingenommen.
- Domänen: Anzahl der beantragten Domänen
- Ausgestellt: Anzahl der im Betrachtungszeitraum ausgestellten Zertifikate.
- Abgelaufen: Anzahl der im Betrachtungszeitraum abgelaufenen Zertifikate.
- Für ungültig erklärt: Anzahl der im Betrachtungszeitraum für ungültig erklärte Zertifikate.

10.2 Benutzer

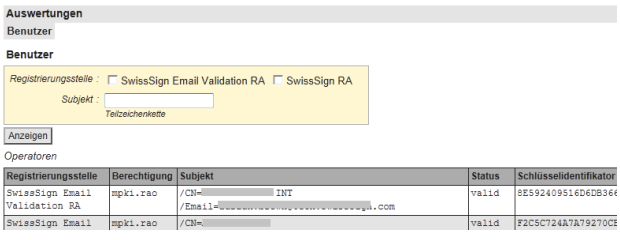
Unter dem Menüpunkt «Auswertungen/Benutzer» werden Benutzer auf gleichem Berechtigungslevel und niedrigeren Berechtigungslevels angezeigt mit den jeweiligen Rechten. Der Punkt ist nur für eingeloggte Zugangsverantwortliche sichtbar.

Diese Auswertung kann über den Hauptmenüpunkt «Benutzer» unterhalb von «Auswertungen» gestartet werden



Die Auswertung zeigt alle Benutzer der gleichen oder niedrigeren Hierarchiestufe einer RA an. Sie sehen,

- für welche «Registrierungsstelle» (RA) dieser Benutzer eingetragen ist.
- wie seine Berechtigungen sind.
- wie der Status ist.



und das für den Zertifikatslogin notwendige Zertifikat wird mit Schlüsselidentifikator und Zertifikats-Identifikator angezeigt.

Unter Operatoren werden die Zugangsverantwort-

lichen und Auditoren geführt. Unter Anforderer die Zertifikatsanforderer.

11. E-Mail-Benachrichtigungen

11.1 E-Mail-Verkehr bei Zertifikatsanforderung durch Requester

Das System erzeugt zu bestimmten Ereignissen E-Mails, die an bestimmte Personen versendet werden. Mit der Anforderung des Zertifikates hat man festgelegt, wer der Empfänger der E-Mail eines Zertifikates ist:

- Das Zertifikat wurde unter einem bestimmten Konto angefordert: Die E-Mail, die diesem Konto zugeordnet ist, wird für alle Benachrichtigungen bezüglich dieses Zertifikates genutzt.
- Das Zertifikat wurde ohne Konto angefordert: Es wurde während der Anforderung die Kontaktdaten und damit auch die E-Mail-Adresse für Benachrichtigungen über dieses Zertifikat festgelegt.
- Das Zertifikat wurde als Zugangsverantwortlicher angefordert: Das Zertifikat wird dann immer mit der Rolle des Zugangsverantwortlichen als Anforderer verbunden, auch wenn der Zugangsverantwortliche ein Anforderer-Konto genutzt hat. Somit wird die Zugangsverantwortlichen-E-Mail für Benachrichtigungen genutzt. Ist das nicht gewünscht, muss sich ein Zugangsverantwortlicher explizit ausloggen und mit Benutzername/Passwort oder Zertifikat eines speziellen Anforderers einloggen.

Von diesen Regeln ausgenommen sind sogenannte «Proof of Posession» E-Mails – also E-Mails, die überprüfen, ob der Benutzer Zugriff und Kontrolle über eine bestimmte E-Mail-Adresse hat. Das geschieht bei Zertifikaten der Stufe Silver, die nicht im Rahmen einer Managed PKI freigeschaltet wurden, sondern deren Lizenz im Webshop gekauft wurde. Bei einem Personal Silver ID Zertifikat wird direkt diejenige E-Mail-Adresse adressiert, die im Zertifikat aufgenommen werden soll. Bei einem Silver SSL Zertifikat wird die bei Antragstellung angegebene E-Mail-Adresse adressiert.

Hinweis: Auch bei einer Anforderung aus einem Konto heraus, in dem man eingeloggt ist, kann man die Kontaktdaten, die mit dieser Anforderung verknüpft sind, explizit ändern. Das ist weiter oben beschrieben. Siehe Kapitel 4.1

Achtung: Zu unterscheiden sind die Benachrichtigungs-E-Mail von den E-Mails, die zur Verifikation einer E-Mail oder Domäne z. B. an die E-Mail-Adresse des Zertifikatinhabers versendet werden. Hierbei wird abweichend von allen Kontoeinstellungen oder Kontakteinstellungen immer die E-Mail-Adresse des Zertifikates genommen, bzw. der Zugangsverantworltiche einer Domäne angeschrieben, falls es sich um ein SSL Zertifikat handelt. Es ist unbedingt darauf zu achten, dass diese E-Mail-Adresse bereits existent ist, wenn das Zertifikat beantragt wird.

Alle E-Mail-Nachrichten unterscheiden sich nach Zertifikatstyp.

Typischerweise gibt es folgende Ereignisse, die E-Mails auslösen. Alle E-Mails werden auch zusätzlich an den Zugangsverantwortlichen versendet.

- Anforderung eines Zertifikates: Der Empfänger gemäss Kontoeinstellung oder Kontakteinstellung zum Zertifikat bekommt eine Bestätigungs-E-Mail. Er hat die Möglichkeit bei einem Webshop-Bezug des Zertifikates ggfs. ein notwendiges Antragsdokument herunterzuladen, welches ihm per Link angeboten wird. Er hat zusätzlich die Möglichkeit, die Anforderung wieder zurückzuziehen.
- Nach Genehmigung oder Zurückweisung des Zertifikates durch die Registrierungsstelle: Der Empfänger erhält an dieselbe Adresse wie bei der Anforderung eines Zertifikates ein E-Mail zugesendet. Ein Link in der E-Mail verweist direkt auf die Downloadseite des Zertifikates.
- 30 Tage vor Ablauf eines Zertifikates: 30 Tage vor Ablauf eines Zertifikates erhält der Empfänger an dieselbe Adresse wie bei der Anforderung eines Zertifikates eine E-Mail zugesendet, die ihn auf den Ablauf des Zertifikates hinweist.

- 10 Tage vor Ablauf eines Zertifikates: 10 Tage vor Ablauf eines Zertifikates wird der Benutzer erneut auf den Ablauf hingewiesen.
- Ungültigkeitserklärung: Bei einer Revozierung (Ungültigkeitserklärung) eines Zertifikates wird ebenfalls eine E-Mail ausgelöst, auch wenn der Benutzer selber diese Ungültigkeitserklärung durchgeführt hat.
- Zurückziehung eines Antrages: Wurde ein Zertifikatsantrag zurückgezogen, wird dieser Vorgang mit einer E-Mail bestätigt.

Hinweis: Hat sich die E-Mail-Adresse geändert und möchte man diese dem bereits ausgegebenen Zertifikat zuordnen, so ist das über eine Attributsänderung zum Zertifikat möglich. Siehe Kapitel 5.5.

11.2 Kundenspezifische E-Mail-Benachrichtigungen

E-Mail-Benachrichtigungen können kundenspezifisch eingestellt werden. Hierzu gibt es Template-Texte, die gemeinsam mit dem SwissSign Support angepasst werden können.

12. Support Kontakt

Bei allen Fragen ist der Support über helpdesk@swisssign.com erreichbar oder kann über die Menüleiste oben angewählt werden:

SwissSign

13. Index