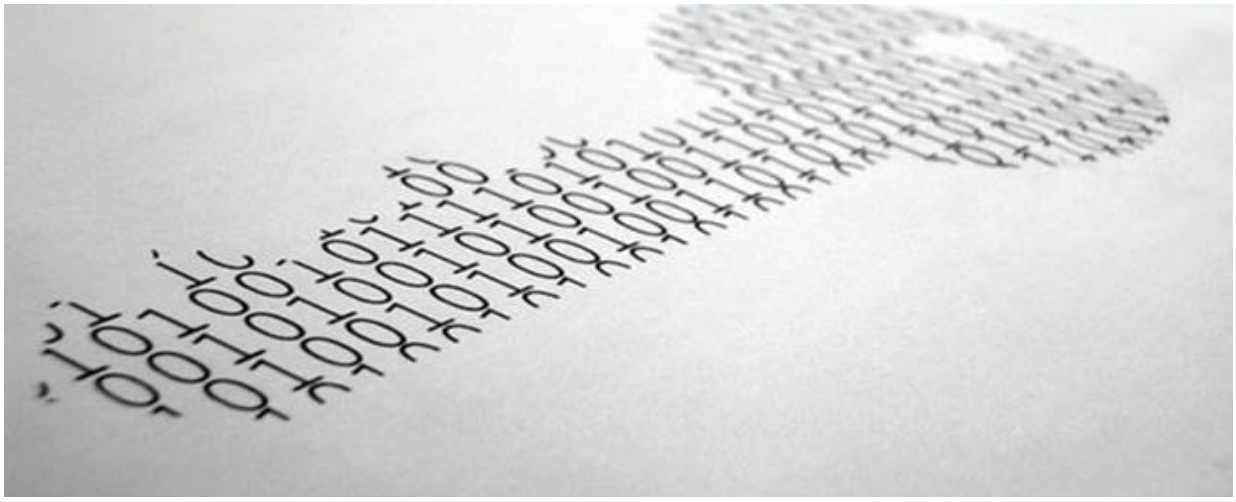
SwissSign

MANAGED PKI SERVICE



Fakten und Technische Details

SwissSign

Inhaltsverzeichnis

1 Einleitung 3
2 Was sind die Vorteile einer Managed PKI Lösung? 3
3 Zertifikatstypen 4
4 Höchste Flexibilität in Abrechnung und Verrechnung 10
5 Schnittstellen, Cockpit und Verwaltung 12
6 Konfiguration und Setup 13
7 Prüfverfahren und Registrierungsstelle 14

SwissSign

1 Einleitung

Mit einer Managed PKI von SwissSign haben Sie die Möglichkeit rund um die Uhr sowohl öffentlich überall vertrauenswürdige aber auch private Zertifikate für seine Organisation zu beziehen, ohne dass die Zertifikatsinhalte noch einzeln von SwissSign überprüft werden müssen. Die Beantragung und Ausstellung kann entweder mit einem Web User Interface oder über eine automatisierte Schnittstelle via dem RFC Standard „CMC“ durchgeführt werden.

2 Was sind die Vorteile einer Managed PKI Lösung?

Durch eine Managed PKI können Sie sofort und zentral für Ihr Unternehmen, ihre Partner und Kunden Zertifikate ausstellen, ohne das die Beantragung der Zertifikate noch einer Einzelprüfung unterliegt. 7 Tage und 24 Stunden steht die Plattform für Sie zur Verfügung. Sie können auch Ihre unternehmensinterne PKI in diese Managed PKI verlagern und damit das gesamte Zertifikatsmanagement im Unternehmen zentralisieren.

Die Managed PKI Lösung verfügt über eine automatische Schnittstelle zum Zertifikatsbezug nach Internet RFC Standard. Hierdurch profitieren Sie automatisch von zahlreichen weiteren getesteten Partnerapplikationen aus dem grossen Partnernetzwerk von SwissSign. Zeitaufreibende Aufgaben wie das manuelle Installieren von Zertifikaten, Signieren von E-Mails und Dokumenten oder Verschlüsselung von Daten können automatisiert durchgeführt werden mit sehr kurzer Projektrealisierungszeit, da die Applikation auf die Managed PKI abgestimmt ist.

Somit haben Sie mit der Managed PKI eine zentrale Stelle für vertrauenswürdige und private Zertifikate für alle Unternehmensbereiche. Damit können Sie auch Applikationen für den Zertifikatsroll-out und -handling zentralisieren und ersparen damit Doppelt- und Mehrfachinvestitionen durch zentrales Management und Automatisierung Ihrer Zertifikatsverteilung und -verwendung.

Die Abrechnung der Zertifikate beschränkt sich nur auf deren Nutzungszeit, technisch wird Ihnen die Zertifikatsausstellung auch über den Bestellrahmen hinaus nicht verwehrt. Damit haben Sie auch in kurzfristigen kritischen Situationen, z.B. Sonntag nachts, die Möglichkeit, Zertifikate auszustellen und ggfs. bei uns dann nachzubestellen.

Die Schweizerische Post und die Schweizerische Bundesbahnen sind nun bereits seit über 100 Jahren erfolgreich am Markt und beweisen diesen Erfolg zusammen mit einer der grössten Schweizer Banken Postfinance heutzutage täglich. SwissSign als 100% Tochter der Schweizerischen Post und der Schweizerischen Bundesbahnen steht auch für beständige und langjährige Partnerschaft. Weltweit gibt es keine Organisation mit öffentlich vertrauenswürdiger Zertifizierungsstelle, die eine so lange Markttradition vorweisen kann. Ein Verschwinden einer Zertifizierungsstelle am Markt bedeutet viel Aufwand und Risiko für alle Anwendungen, Webseiten und Kommunikation Ihres Unternehmens. Hier ist es wichtig auf Kontinuität und Langlebigkeit zu setzen.

SwissSign ist mit seinem Standort im Herzen von Europa auch ein Partner der kurzen Wege. Wir sind schnell vor Ort sofern das notwendig ist und stehen auch im Support mit Ansprechpartnern in Deutsch, Schweizer Mundart. Englisch und Französisch zur Verfügung.

3 Zertifikatstypen

Beinahe alle Zertifikatstypen, die SwissSign auch im Webshop anbietet, können Sie im Rahmen einer Managed PKI beziehen: Webserver und Device Zertifikate (SSL), E-Mail Zertifikate und Code Signing Zertifikate. Neben den unten angeführten Standardzertifikatstypen sind auch Sonderzertifikate optional auf Absprache hin möglich bei grösseren Managed PKI Installationen. Für private Zertifikate bieten wir darüber hinaus auch die Erstellung einer eigenen Root-CA und Issuing CA an. Auch für öffentlich vertrauenswürdige Zertifikate können eigene Issuing CAs bei entsprechendem Volumen erstellt werden. Nachfolgend finden Sie unsere öffentlich vertrauenswürdigen Standardzertifikattypen:

3.1 SSL Silver (DV)

Einsatzzweck:

- Absicherung interner Devices und Server im Netzwerk der Organisation
- Absicherung von Webseiten mit reinem Informationsgehalt ohne Phishingrisiko

Qualitätseigenschaft:

- Gelten als „domänenvalidiert“, d.h. es wird lediglich sichergestellt, dass die Domäne existent ist.

Attribute:

- CN: Domänenname
- SAN-Eintrag: Domänenname (auf Wunsch mit und ohne „www“)

Schlüsselverwendungen und erweiterte Schlüsselverwendungen:

- Digital Signature
- Key Encipherment
- Clientauthentifizierung/ClientAuthentication(1.3.6.1.5.5.7.3.2)
- Serverauthentifizierung/ServerAuthentication(1.3.6.1.5.5.7.3.1)

Technische Laufzeiten:

- 1 Jahr
- 2 Jahre
- 3 Jahre (bis Dez. 2017)

3.2 SSL Silver Wildcard (DV)

Einsatzzweck:

- Absicherung interner Devices und Server im Netzwerk der Organisation
- Absicherung von Webseiten mit reinem Informationsgehalt ohne Phishingrisiko
- Absicherung aller Subdomänen einer Domäne, allerdings nicht die Hauptdomäne
- Ein Zertifikat kann beliebig oft in Kopie eingesetzt werden, immer mit dem gleichen privaten Schlüssel

Qualitätseigenschaft:

- Gelten als „domänenvalidiert“, d.h. es wird lediglich sichergestellt, dass die Domäne existent ist.

Attribute:

- CN: Domänenname mit vorangestelltem Wildcard Zeichen („*“)
- SAN-Eintrag: Domänenname mit vorangestelltem Wildcard Zeichen („*“)

Schlüsselverwendungen und erweiterte Schlüsselverwendungen:

- Digital Signature
- Key Encipherment
- Clientauthentifizierung/ClientAuthentication(1.3.6.1.5.5.7.3.2)
- Serverauthentifizierung/ServerAuthentication(1.3.6.1.5.5.7.3.1)

Technische Laufzeiten:

- 1 Jahr
- 2 Jahre
- 3 Jahre (bis Dez. 2017)

3.3 SSL Gold (OV)

Einsatzzweck:

- Absicherung von Webseiten mit mittlerem Phishingrisiko, ohne relevante Kundendaten

Qualitätseigenschaft:

- Gelten als „organisationsvalidiert“, d.h. es wird sichergestellt, dass die Domäne existent ist, die Organisation diese Domäne kontrolliert und die Organisation existent und überprüft ist.

Attribute:

- CN: Domänennamen
- Organisation, Ort, Staat
- Optional Organisatorische Einheit, Provinz/Bundesland/Kanton
- SAN-Eintrag: Domänenname (auf Wunsch mit und ohne „www“)

Schlüsselverwendungen und erweiterte Schlüsselverwendungen:

- Digital Signature
- Key Encipherment
- Clientauthentifizierung/ClientAuthentication(1.3.6.1.5.5.7.3.2)
- Serverauthentifizierung/ServerAuthentication(1.3.6.1.5.5.7.3.1)

Technische Laufzeiten:

- 1 Jahr
- 2 Jahre
- 3 Jahre (bis Dez. 2017)

3.4 SSL Gold Wildcard (OV)

Einsatzzweck:

- Einsetzbar in speziellen Microsoft Lync und Exchange Umgebungen
- Absicherung von Webseiten mit mittlerem Phishingrisiko, ohne relevante Kundendaten
- Absicherung aller Subdomänen einer Domäne, allerdings nicht die Hauptdomäne
- Ein Zertifikat kann beliebig oft in Kopie eingesetzt werden, immer mit dem gleichen privaten Schlüssel

Qualitätseigenschaft:

- Gelten als „organisationsvalidiert“, d.h. es wird sichergestellt, dass die Domäne existent ist, die Organisation diese Domäne kontrolliert und die Organisation existent und überprüft ist.

Attribute:

- CN: Domänenname mit vorangestelltem Wildcard Zeichen („*“)
- Organisation, Ort, Staat

- Optional Organisatorische Einheit, Provinz/Bundesland/Kanton
- SAN-Eintrag: Domänenname mit vorangestelltem Wildcard Zeichen („*“)

Schlüsselverwendungen und erweiterte Schlüsselverwendungen:

- Digital Signature
- Key Encipherment
- Clientauthentifizierung/ClientAuthentication(1.3.6.1.5.5.7.3.2)
- Serverauthentifizierung/ServerAuthentication(1.3.6.1.5.5.7.3.1)

Technische Laufzeiten:

- 1 Jahr
- 2 Jahre
- 3 Jahre (bis Dez. 2017)

3.5 SSL Gold Multidomain (OV, UCC/SAN)

Einsatzzweck:

- Absicherung von Microsoft Exchange und Lync Umgebungen
- Absicherung von Webseiten mit mittlerem Phishingrisiko, ohne relevante Kundendaten, z.B. mehrsprachige Webseiten auf einem Webserver unter verschiedenen URLs mit Länderkennungen
- Absicherung von bis zu 200 (Wildcard) Domänen in einem Zertifikat
- Ein Zertifikat kann beliebig oft in Kopie eingesetzt werden, immer mit dem gleichen privaten Schlüssel

Qualitätseigenschaft:

- Gelten als „organisationsvalidiert“, d.h. es wird sichergestellt, dass die Domäne existent ist, die Organisation diese Domäne kontrolliert und die Organisation existent und überprüft ist.

Attribute:

- CN: erster Domänenname
- Organisation, Ort, Staat
- Optional Organisatorische Einheit, Provinz/Bundesland/Kanton
- SAN-Eintrag: Bis zu 200 Domänennamen, auch wildcard Einträge

Schlüsselverwendungen und erweiterte Schlüsselverwendungen:

- Digital Signature
- Key Encipherment
- Clientauthentifizierung/ClientAuthentication(1.3.6.1.5.5.7.3.2)
- Serverauthentifizierung/ServerAuthentication(1.3.6.1.5.5.7.3.1)

Technische Laufzeiten:

- 1 Jahr
- 2 Jahre
- 3 Jahre (bis Dez. 2017)

3.6 SSL Gold EV (EV)

Einsatzzweck:

- Absicherung von Webseiten mit relevanten Kundendaten, Webshops, Zahlungsseiten
- Im Browser wird automatisch der grüne Balken mit Sonderinformation angezeigt
- Höchstes Vertrauen

Qualitätseigenschaft:

- Gelten als „extended validated“, d.h. es wird sichergestellt, dass die Domäne existent ist, die Organisation diese Domäne kontrolliert und die Organisation existent ist, geschäftstätig ist und gründlich nach internationalen Standards überprüft ist.

Attribute:

- CN: Domänenname
- Organisation, Ort, Staat, Geschäftskategorie, Land/Provinz/Ort der Registrierung, Registrierungsnummer
- Optional Organisatorische Einheit, Provinz/Bundesland/Kanton, PLZ, Strasse
- SAN-Eintrag: Domänenname (auf Wunsch mit und ohne „www“)

Schlüsselverwendungen und erweiterte Schlüsselverwendungen:

- Digital Signature
- Key Encipherment
- Clientauthentifizierung/ClientAuthentication(1.3.6.1.5.5.7.3.2)
- Serverauthentifizierung/ServerAuthentication(1.3.6.1.5.5.7.3.1)

Technische Laufzeiten:

- 1 Jahr
- 2 Jahre

3.7 SSL Gold EV Multidomain (EV, UCC/SAN)

Einsatzzweck:

- Absicherung von Webseiten mit relevanten Kundendaten, Webshops, Zahlungsseiten insbesondere mit mehreren Domänennamen
- Im Browser wird automatisch der grüne Balken mit Sonderinformation angezeigt
- Höchstes Vertrauen
- Höchste Absicherung von Microsoft Exchange und Lync Umgebungen, auch OWA
- Absicherung von bis zu 200 Domänen in einem Zertifikat
- Ein Zertifikat kann beliebig oft in Kopie eingesetzt werden, immer mit dem gleichen privaten Schlüssel

Qualitätseigenschaft:

- Gelten als „extended validated“, d.h. es wird sichergestellt, dass die Domäne existent ist, die Organisation diese Domäne kontrolliert und die Organisation existent ist, geschäftstätig ist und gründlich nach internationalen Standards überprüft ist.

Attribute:

- CN: Erster Domänenname
- Organisation, Ort, Staat, Geschäftskategorie, Land/Provinz/Ort der Registrierung, Registrierungsnummer
- Optional Organisatorische Einheit, Provinz/Bundesland/Kanton, PLZ, Strasse
- SAN-Eintrag: Bis zu 200 Domänennamen

Schlüsselverwendungen und erweiterte Schlüsselverwendungen:

- Digital Signature
- Key Encipherment
- Clientauthentifizierung/ClientAuthentication(1.3.6.1.5.5.7.3.2)
- Serverauthentifizierung/ServerAuthentication(1.3.6.1.5.5.7.3.1)

Technische Laufzeiten:

- 1 Jahr
- 2 Jahre

3.8 E-Mail ID Gold (S/MIME, entspricht Class 3/2 Standard)

Einsatzzweck:

- E-Mail Verschlüsselung
- E-Mail Signatur insbesondere in der Phishing gefährdeten Kommunikation
- Authentication / Zugriff auf Applikationen und Webseiten

Qualitätseigenschaft:

- Gelten als organisations- und personenvalidiert, d.h. neben der E-Mail Adresse wird sichergestellt, dass das subject (Person, Person hinter einem Pseudonym) existiert und die Organisation die Nutzung des Namens für dieses Zertifikat erlaubt hat und überprüft wurde.

Attribute:

- CN: Vorname, Name oder Pseudonym (z.B. für ein Gruppenpostfach)
- E-Mail, Organisation, Land
- Optional Organisatorische Einheit, Provinz/Bundesland/Kanton
- SAN-Eintrag: E-Mail Adresse

Schlüsselverwendungen und erweiterte Schlüsselverwendungen:

- Digital Signature
- Non Repudiation
- Key Encipherment
- Data Encipherment
- Clientauthentifizierung (1.3.6.1.5.5.7.3.2)
- Sichere E-Mail (1.3.6.1.5.5.7.3.4)
- Verschlüsselndes Dateisystem (1.3.6.1.4.1.311.10.3.4)
- Smartcard-Anmeldung (1.3.6.1.4.1.311.20.2.2)

Technische Laufzeiten:

- 1 Jahr
- 2 Jahre
- 3 Jahre

3.9 E-Mail ID Silver (S/MIME, entspricht Class 1 Standard)

Einsatzzweck:

- E-Mail Verschlüsselung
- E-Mail Signatur in nicht-phishing gefährdeter Kommunikation

Qualitätseigenschaft:

- Gilt als E-Mail validiert, d.h. es wird lediglich sichergestellt, dass die E-Mail existiert.

Attribute:

- CN: E-Mail Adresse (Zertifikate via Web) oder
- CN: Herstellerclient spezifische Zeichenkette (z.B. „Secure Mailgateway Certificate“) bei Nutzung der automatischen Schnittstelle
- OU: Feste Zeichenkette „E-Mail validated only“
- E-Mail Adresse, Organisation, Land

- Optional Organisatorische Einheit, Provinz/Bundesland/Kanton
- SAN-Eintrag: E-Mail Adresse

Schlüsselverwendungen und erweiterte Schlüsselverwendungen:

- Digital Signature
- Non Repudiation
- Key Encipherment
- Data Encipherment
- Sichere E-Mail/Secure Email (1.3.6.1.5.5.7.3.4)

Technische Laufzeiten:

- 1 Jahr
- 2 Jahre
- 3 Jahre

Sollte das Produkt für eine SwissSign Partnerapplikation via automatisierter Schnittstelle benutzt werden, so wird zusätzlich auch die Organisation eingetragen. Das OU Feld kann darüber hinaus noch einen speziellen Eintrag vorweisen, der auf die Partnerapplikation hinweist. Dieser Eintrag wird im Managed PKI Setup Agreement – Anhang angezeigt, nachdem die Partnerapplikation ausgewählt wurde.

Auf der SwissSign Partnerseite werden autorisierte Partnerapplikationen angezeigt.

3.10 Codesigning

Einsatzzweck:

- Signatur von Programmiercode (z.B. Microsoft Makros, Javacode, Applets etc.)
- Nicht einsetzbar, wo EV Standard (z.B. Microsoft Kernel Entwicklung) gefragt ist
- Mit kostenlosem Zeitstempel (10 Stück am Tag) nutzbar.

Qualitätseigenschaft:

- Gilt als Organisations- oder Personenvalidiert. D.h. die Person oder Organisation, auf die das Zertifikat ausgestellt wurde, ist überprüft im Hinblick auf Existenz und Geschäftstätigkeit (Organisation) oder Identität

Attribute:

- CN: Name der Organisation
- Organisation, Ort, Staat
- Optional Organisatorische Einheit, Provinz/Bundesland/Kanton

Schlüsselverwendungen und erweiterte Schlüsselverwendungen:

- Digital Signature
- Codesignatur/Code Signing (1.3.6.1.5.5.7.3.3)
- Microsoft Individual Code Signing (1.3.6.1.4.1.311.2.1.21)
- Microsoft Commercial Code Signing (1.3.6.1.4.1.311.2.1.22)

Technische Laufzeiten:

- 1 Jahr
- 2 Jahre
- 3 Jahre

3.11 Weitere Sonderzertifikate

Auf Wunsch ist auch die Einrichtung weiterer Zertifikatstypen möglich. Die Preise sind im Standardberechnungssheet nicht enthalten und können auf Anfrage hin offeriert werden. Hierzu zählen z.B. 802.1x Zertifikate, d.h. SSL Zertifikate ohne Server Authentication, Zertifikate im Microsoft Umfeld unter Nutzung des User Principal Names (UPN) oder der Templates für Domain und Server Controller.

3.12 Interne Zertifikate, z.B. Device Zertifikate ClientAuth

Die Managed PKI kann kostengünstig erweitert werden mit nicht öffentlich vertrauenswürdigen Zertifikaten, die in der eigenen SwissSign CA oder einer gehosteten CA Ihrer Organisation erzeugt und mit der gleichen Managed PKI verwaltet werden. Nähere Informationen finden Sie hierzu in einem getrennten White Paper. Damit kann im Unternehmen die komplette eigene PKI entfallen.

4 Höchste Flexibilität in Abrechnung und Verrechnung

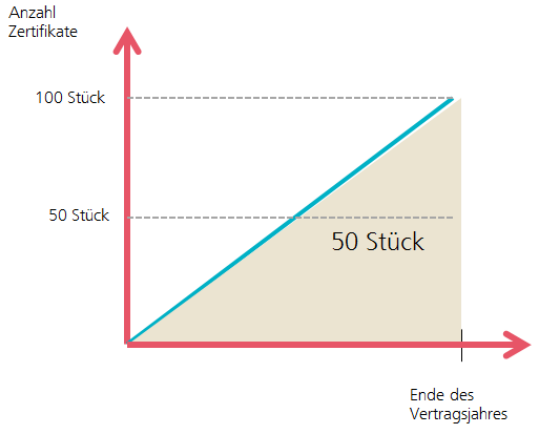
4.1 Leistungsperiode, Zahlung und Flexible Abrechnung

Am Ende des Monats nach der Bestellung beginnt die erste Leistungsperiode für die Managed PKI. Die Vertrags- und Leistungsperiode beträgt ein oder mehrere Jahre und wird automatisch nach Vertragslaufzeit um ein Jahr verlängert, solange nicht 3 Monate vorab gekündigt wird. Zu Beginn jedes Vertragsjahres ist die Vorauszahlung für die Nutzung der Managed PKI fällig, d.h. verrechnet wird auch bei mehrjährigen Verträgen jährlich. Die Höhe richtet sich nach den benötigten Zertifikatstypen und der Anzahl der Zertifikate.

SwissSign unterstützt im Rahmen seines Managed PKI Angebotes ein flexibles Abrechnungsmodell, welches ein allmähliches Anwachsen der Zertifikatsmengen erlaubt. Berechnet werden immer die aktiven Zertifikatstage eines Zertifikates im Jahr.

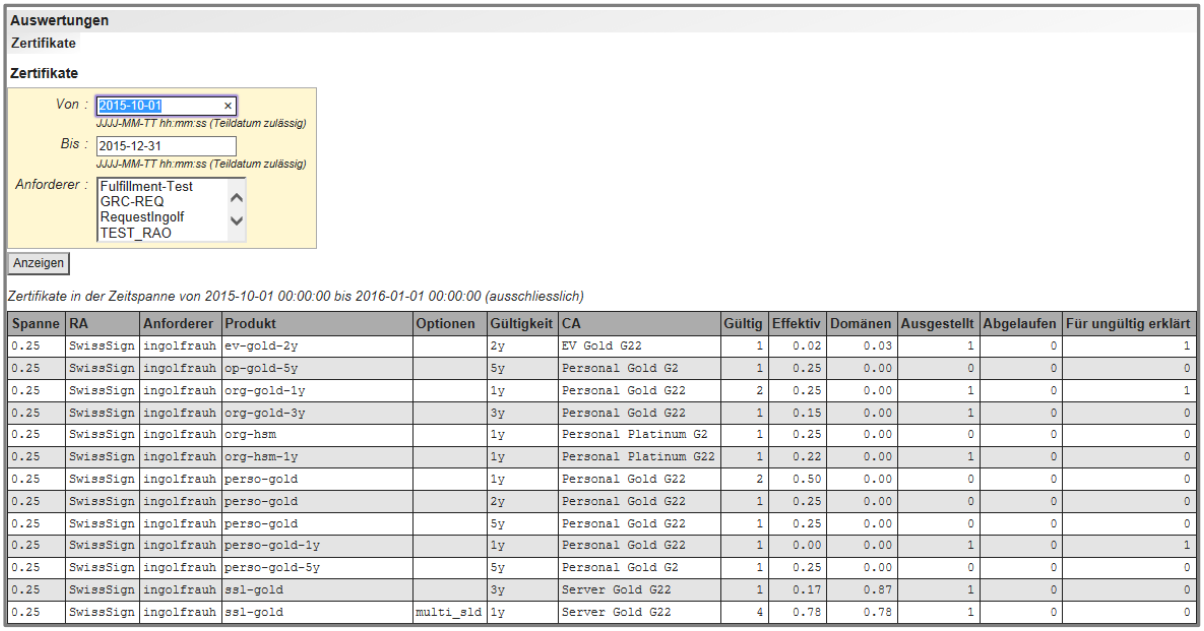
Beispiel: Ein Vertragsjahr dauert von 1. Januar bis zum 31. Dezember. Sollte ein Zertifikat erst am 1. Juli ausgestellt worden sein, wird die Zertifikatsmenge ca. 0.5 berechnet. Sollte ein Zertifikat erst am 1. Oktober ausgestellt werden beträgt es ca. 0.25 und am 1. April ca. 0.75. („circa“ deswegen, weil nicht jeder Monat gleichviele Tage hat).

Umgekehrt ist bei einem linearen Wachstum von 0 auf 100 Zertifikate nur eine Bestellmenge von 50 Zertifikaten in dem Wachstumsvertragsjahr notwendig. Im Folgejahr müssen dann 100 Zertifikate bestellt werden:



4.2 Volumenkontrolle

Ihr Administrator kann jederzeit das bezogene Volumen pro Zertifikatstyp über ein Cockpit überwachen. Grundsätzlich führt eine Überschreitung des bestellten Volumens nicht zu einer technischen Sperre, d.h. es besteht ein Vertrauensvorschuss, so dass technisch beliebig Zertifikate bezogen werden können. SwissSign überwacht regelmässig den Zertifikatsbezug und wird zu Beginn des Folgevertragsjahres mit Ihnen den Mehrverbrauch in Rechnung stellen und den Vertrag anpassen. Ausschlaggebend ist immer die Überschreitung des Gesamtbestellvolumens und nicht die Überschreitung des Volumens eines spezifischen Zertifikatstyps.



Zertifikate in der Zeitspanne von 2015-10-01 00:00:00 bis 2016-01-01 00:00:00 (ausschliesslich)

Spanne	RA	Anforderer	Produkt	Optionen	Gültigkeit	CA	Gültig	Effektiv	Domänen	Ausgestellt	Abgelaufen	Für ungültig erklärt
0.25	SwissSign	ingolfrauh	ev-gold-2y		2y	EV Gold G22	1	0.02	0.03	1	0	1
0.25	SwissSign	ingolfrauh	op-gold-5y		5y	Personal Gold G2	1	0.25	0.00	0	0	0
0.25	SwissSign	ingolfrauh	org-gold-1y		1y	Personal Gold G22	2	0.25	0.00	1	0	1
0.25	SwissSign	ingolfrauh	org-gold-3y		3y	Personal Gold G22	1	0.15	0.00	1	0	0
0.25	SwissSign	ingolfrauh	org-hsm		1y	Personal Platinum G2	1	0.25	0.00	0	0	0
0.25	SwissSign	ingolfrauh	org-hsm-1y		1y	Personal Platinum G22	1	0.22	0.00	1	0	0
0.25	SwissSign	ingolfrauh	perso-gold		1y	Personal Gold G22	2	0.50	0.00	0	0	0
0.25	SwissSign	ingolfrauh	perso-gold		2y	Personal Gold G22	1	0.25	0.00	0	0	0
0.25	SwissSign	ingolfrauh	perso-gold		5y	Personal Gold G22	1	0.25	0.00	0	0	0
0.25	SwissSign	ingolfrauh	perso-gold-1y		1y	Personal Gold G22	1	0.00	0.00	1	0	1
0.25	SwissSign	ingolfrauh	perso-gold-5y		5y	Personal Gold G2	1	0.25	0.00	0	0	0
0.25	SwissSign	ingolfrauh	ssl-gold		3y	Server Gold G22	1	0.17	0.87	1	0	0
0.25	SwissSign	ingolfrauh	ssl-gold	multi_sld	1y	Server Gold G22	4	0.78	0.78	1	0	0

Zertifikate für das gleiche Subject werden nicht gesondert berechnet. So kann für ein E-Mail Konto bereits ein Monat vor Ablauf des alten Zertifikates ein neues Zertifikat bereitgestellt werden, so dass die parallele Nutzung zweier Zertifikate in der Berechnung als ein einziges Zertifikat eingeht.

Wird das lizensierte Volumen binnen einer Leistungsperiode nicht ausgeschöpft, kann es nicht in die nächste Leistungsperiode übertragen werden. Das Volumen kann aber jederzeit erhöht werden durch eine weitere Bestellung von Zertifikaten. Der Unterschiedsbetrag von der Jahreszahlung der neuen Gesamtbestellung zum bisherigen Bestellumfang wird für die verbleibenden Monate der Leistungsperiode anteilig in Rechnung gestellt.

Zertifikate, die nicht mehr im Einsatz sind, können jederzeit revoziert werden. Ab dem Zeitpunkt der Revozierung werden diese bei der Abrechnung nicht mehr mitgezählt..

4.3 Leistungsperiode und technische Laufzeiten der Zertifikate

Auch wenn die Vertragslaufzeit oder Leistungsperiode ein Jahr ist, besteht natürlich die Möglichkeit, die Zertifikate mit einer technischen Laufzeit von mehreren Jahren auszustellen. Sollte der Managed PKI Vertrag einmal nicht verlängert werden, werden die noch gültigen Zertifikate zurückgezogen. Somit ist man auch bei 3- oder 5-jährigen Zertifikaten nicht an die technische Laufzeit dieser Zertifikate finanziell gebunden.

4.4 Flexibilität innerhalb des gewählten Bestellvolumens

Grundsätzlich bietet SwissSign Zertifikate mit einem Volumenrabatt an. Je höher der Bestellwert an Zertifikaten ist, desto höher fällt der Volumenrabatt aus. Innerhalb eines Bestellwertes spielt es im Rahmen der Managed PKI keine Rolle ob dieser Bestellwert durch x-Fache Bestellung eines Typs A von Zertifikaten oder Typ B von Zertifikaten erreicht wurde.

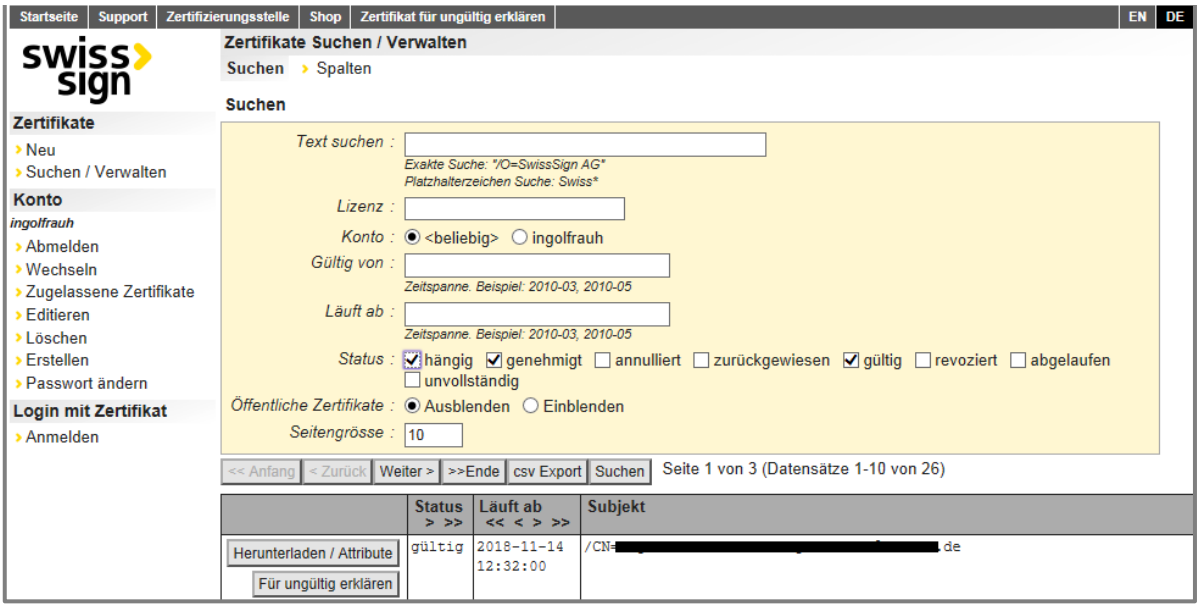
Konkretes Beispiel: Ein SSL EV Zertifikat hat einen Bestellwert von ca. 600 CHF (ohne Volumenrabatt), ein E-Mail Gold ID von ca. 60 CHF. Erfolgt eine Bestellung von Zertifikaten mit einem Bestellwert von 6000 CHF, so können am Ende des Jahres z.B. 100 E-Mail Gold ID Zertifikate genutzt werden oder alternativ auch 10 SSL EV Zertifikate bzw. beliebige Mischungen, die dann den Bestellwert ergeben.

5 Schnittstellen, Cockpit und Verwaltung

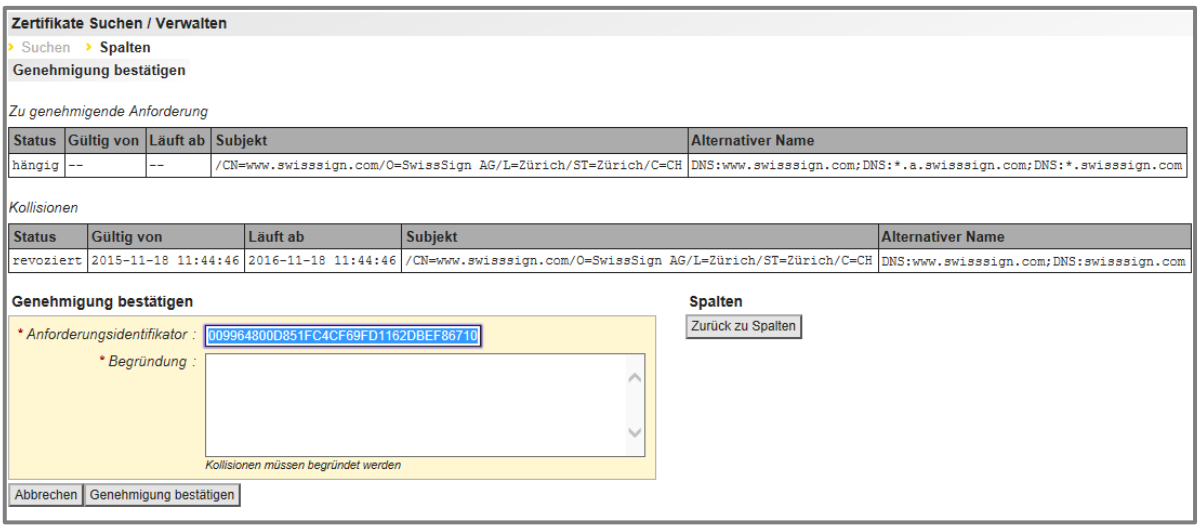
Für die Beantragung und Ausstellung von Zertifikaten werden zwei Standardschnittstellen der Managed PKI angeboten, die in gleicher Weise sowohl für private als auch für öffentlich vertrauenswürdige Zertifikate genutzt werden können: Eine webbasierte Schnittstelle zur manuellen Beantragung, Genehmigung, Revokation und Ausstellung und eine automatisierte Schnittstelle.

Die Webschnittstelle bietet via Browser einen auf Zugangszertifikaten basierten, verschlüsselten TLS Zugang für Ihren Administrator. Der Administrator ist frei, nur zum Zwecke der Beantragung und Revokation (also nicht Ausstellung) weitere Konten z.B. für weitere Mitarbeiter im Unternehmen zu eröffnen. Diese können wahlweise auch mit Zertifikatszugang gesichert werden oder mit Username/Passwort. Über die Webschnittstelle kann die ganze Verwaltung und der Genehmigungsprozess aller Zertifikate, inklusive Reports etc. abgewickelt werden. Bei der Beantragung eines Zertifikates via Webschnittstelle steht es dem Antragsteller frei, ob SwissSign das Schlüsselpaar (öffentlicher/privater Schlüssel) generieren soll oder ob er selber das Schlüsselpaar generiert und im Rahmen des CSR nur den öffentlichen Schlüssel für die Antragstellung übergibt. Über alle Anträge entscheidet der Administrator und Zugangsverantwortliche des Unternehmens. Nach seiner Bewilligung wird das Zertifikat ausgestellt und zum Download via Webbrowser angeboten.

Zusätzlich stellen wir auch eine automatisierte Schnittstelle zur Verfügung. Ihre Organisation beantragt die Zertifikate mit einer Managed PKI Schnittstelle nach RFC 5272 (CMC) Standard und erhält das entsprechende Zertifikat für alle hinterlegten Konfigurationen. Die Konfigurationen können Sie zum Zeitpunkt des Setup bestimmen und setzen im wesentlichen Filter auf Zertifikatsinhalte und Zertifikatstypen. Die Schnittstelle wird ebenfalls mit einem Zugangszertifikat TLS basierend abgesichert. Das Zugangszertifikat kann dann von einer Client Software verwaltet und genutzt werden, die den automatisierten Zugang zur SwissSign internen CA sicherstellt. Im Falle der automatischen Schnittstelle wird das Schlüsselpaar (öffentlicher und privater Schlüssel) in ihrer Organisation erzeugt. Die Schnittstelle erwartet dann einen CSR mit dem von Ihnen generierten öffentlichen Schlüssel. Die Schnittstelle beantwortet einen konformen Antrag sofort mit einem Zertifikat. Sie basiert auf einem http POST Ansatz und ist hier dokumentiert. Eine Revokation kann ebenfalls mit dieser Schnittstelle erfolgen.



Natürlich besteht auch die Möglichkeit, Zertifikate zurückzuziehen (Revozierung) oder auch Anträge zurückzuziehen. Zertifikate können über ein LDAP weltweit verfügbar publiziert werden oder privat gehalten werden.



Im Konto des Administrators wird eine E-Mail Adresse festgelegt, an die sämtliche E-Mails gesendet werden im Zusammenhang mit der Zertifikatsbeantragung und –ausstellung. Diese E-Mail Adresse wird auch von SwissSign im Falle von dringenden Nachrichten oder Meldungen genutzt. Daher wird im Managed PKI Setup Agreement – Anhang nach einem allgemeinen E-Mail Konto gefragt, welches laufend bewirtschaftet wird.

6 Konfiguration und Setup

Die Managed PKI wird von SwissSign so aufgesetzt, dass Fehlbeantragungen und Fehlausstellungen insbesondere von öffentlich vertrauenswürdigen Zertifikaten, so weit möglich, vermieden werden. Dazu werden bestimmte Attributwerte fest vorgegeben und können später bei der Beantragung nicht mehr geändert werden. Hierzu gehören:

- Die überprüften Domänen/E-Mail Domänen

- Die überprüften Organisationen gemäss Registereintrag oder Nachweis
- Adressdaten der jeweiligen Organisation
- EV: Registernummer und Registrierungsstelle
- Bestellte Zertifikatstypen

Im Falle von mehreren Organisationen (z.B. einer XYZ AG und einer XYZ Informationsdienste AG) könnte es technisch möglich sein, dass die Eigenschaften/Domänen der Organisation vermischt werden. Hier muss der Zugangsverantwortliche Sorgfalt walten lassen und schauen, dass z.B. ein Zertifikat einer XYZ AG nicht mit der Domäne einer XYZ Informationsdienste AG ausgestellt wird. Auf Wunsch können auch verschiedene Konten für die verschiedenen Organisationen eingerichtet werden.

7 Prüfverfahren und Registrierungsstelle

Im Falle einer Managed PKI übernimmt Ihre Organisation die Rolle einer Registrierungsstelle. Trotz der bereits vorgegebenen Attributwerte ist sie frei, andere Attributwerte frei zu bestimmen, z.B. die Subdomänen oder Personennamen im Falle eines E-Mail Zertifikates. Ein fehlerhaft ausgestelltes Zertifikat wird häufig aufgespürt, kann sogar missbraucht werden und kann daher auch das Fortbestehen einer Zertifizierungsstelle bedrohen.

Die Annahmeerklärung zur Delegation der Registrierungsstellenaktivitäten regelt daher die notwendige Sorgfalt bei der Ausübung dieser Tätigkeit und regelt auch die Haftungsbedingungen. Es ist wichtig, dass die Organisation auch die Freigabe des Organisationsnamens im Zertifikat gewährt und Zugangsverantwortliche als Zertifikatsverantwortliche mit entsprechender Handlungsvollmacht ausstattet. Die Registrierungsstellentätigkeit wird somit an die Kundenorganisation delegiert. Mehrere Organisationen können dabei den gleichen Zugangsverantwortlichen Handlungsvollmacht geben in Ihren Annahmeerklärungen und damit Zertifikate über eine Schnittstelle beziehen.

SwissSign wird daher sehr genau die Organisationsangaben prüfen: es ist notwendig, dass die Organisation irgendwo registriert ist oder in öffentlichen Datenbanken zu finden ist. Für den Bezug von SSL EV Zertifikaten ist es notwendig, dass die Unternehmung bereits 3 Jahre am Markt aktiv ist. Auch die Zeichnungsbefugnis des Unterzeichners wird überprüft, sowie die Domänen. Für die Domänen besteht die Möglichkeit, dass alle Domänen für öffentlich vertrauenswürdige Zertifikate anhand des korrekten whois Eintrages bereits der Organisation der Managed PKI zugeordnet sind. Sollte das nicht der Fall sein, kann der Kunde in der Selbstkonfiguration der Managed PKI ein vom System angezeigtes „Geheimnis“, z.B. eine Zeichenfolge „XYZ4711“ oder ähnlich, auf eine Seite <Domäne>/.well-known/pki-validation/swisssign-check.htm oder in der Datei swisssign-check.txt im selben Pfad platzieren. Alternativ ist auch ein Eintrag im <TXT> Record des DNS Eintrages möglich. Das SwissSign System ruft dann diese Seite auf und sieht, dass Ihr Team Kontrolle über die Domäne besitzt und trägt diese Domäne in Ihr Setup kostenfrei ein. Auch eine schriftliche Domänenvollmacht ist möglich, hierbei sollte der im whois eingetragene Domäneneigentümer diese unterzeichnen. Es kann der Vertreter des Domäneneigentümers gemäss Handelsregister sein oder eine Person, die whois Eintrag explizit erwähnt wurde. Nachmeldung einer Domäne, die nicht durch Selbstkonfiguration eingetragen werden und anhand einer Domänenvollmacht oder whois Eintrag überprüft werden müssen unterliegen einer Änderungsgebühr. Ebenfalls auch alle nachträglichen Änderungen oder Einfügungen von Organisationen.

Nach diesem Prüfverfahren steht es Ihnen offen, alle von Ihnen bestellten Zertifikate rund um die Uhr auszustellen. Ggfs. werden Daten der Überprüfung nochmals nach einigen Monaten überprüft, häufig geschieht das im Hintergrund.