Digitale Zertifikate

SwissSign, eine Datensicherheits-spezialistin der Schweizerischen Post

Managed Public Key Infrastructure (MPKI)
Automatisierte Zertifikatsverwaltung zur Absicherung Ihrer IT-Infrastruktur

Täglich kommen neue Datenverbindungen zwischen Anwendungen, Apps und unterschiedlichen Geräten dazu. Diese eröffnen Chancen, mit jedem neuen Netzwerk steigt aber auch das potenzielle Risiko. Cyberkriminelle nutzen mögliche Sicherheitslücken aus. Die Managed Public Key Infrastructure der Datensicherheitsspezialistin SwissSign schützt Ihre Anwendungen mit Schweizer Zertifikaten für SSL und Secure E-Mail basierend auf den höchsten Sicherheitsstandards. Noch dazu stellt die SwissSign-MPKI eine moderne State-of-the-Art-Lösung für eine einfache Zertifikatsverwaltung rund um die Uhr dar. Betrieb und Datenhaltung erfolgen zu 100 Prozent in der Schweiz.

Was ist die MPKI?

Über die Managed Public Key Infrastructure (MPKI) der Datensicherheitsspezialistin SwissSign können Sie im Abo-Modell rund um die Uhr unbegrenzt Public-Key-Zertifikate für

- SSL und
- Secure E-Mail

beziehen. Dabei profitieren Sie bei höheren Bezugsvolumen von attraktiven Volumenrabatten.

Ihre Vorteile

- Garantieren Sie die Privatsphäre und den Datenschutz Ihrer Kundschaft und Partner.
- Verschlüsseln und authentisieren Sie Ihren E-Mail-Verkehr.
- Erhöhen Sie das Vertrauen von Kundinnen und Kunden in Ihre Webanwendung und bezeugen Sie die Echtheit Ihres Auftritts.
- Schützen Sie sich vor Phishing und Man-in-the-Middle-Angriffen.
- Profitieren Sie von einer besseren Sichtbarkeit im Google-Ranking.
- SwissSign – Swiss Made Software – Swiss Quality

So funktioniert die MPKI

Zertifikate für Ihre Mitarbeitenden, Kundschaft und Partner verwalten Sie rund um die Uhr eigenständig. Über eine automatisierte Schnittstelle oder über das Web-Administrationstool stellen Sie jederzeit jeden Zertifikatstyp sofort aus. Und dank der Schnittstellenstandards ACME und OpenAPI führen Sie ausserdem ein komplettes Autoenrollment mit den Partnerprodukten durch. Die Hauptfunktionen auf einen Blick:

- Übersichtliches Webportal für Bewirtschaftung der MPKI
- Automatisiertes Zertifikats-Lifecycle-Management (REST-API, ACME oder CMC)
- Reports nach Zertifikatstypen, Gruppen oder Ablaufdaten
- Elektronische Abwicklung von Vertragsunterlagen

Vertrauensstufen

Wählen Sie die Vertrauensstufe Ihres SSL-Zertifikats aus. Als zertifizierte Certificate Authority (CA) orientiert sich die Datensicherheitsspezialistin SwissSign an den bekannten Standards:

- **Domain Validation (DV):** für Webseiten mit einem einfachen Schutzbedürfnis, z. B. Blogs, Mailserver o. Ä.
- **Organisation Validation (OV):** für Unternehmen, die ihren Kunden hohen Schutz bieten möchten, z. B. Webshops o. Ä.
- **Extended Validation (EV):** für Unternehmen, welche die höchste Vertrauensstufe ausweisen möchten, z. B. Banken, grosse Webshops o. Ä.

E-Mail-Zertifikate

Entsprechend finden Sie hier auch die Auswahl an E-Mail-Zertifikaten für die Authentisierung bzw. Signatur und Verschlüsselung von E-Mails:

- **E-Mail ID Silver (Personal):** Zertifikate für E-Mail-Adressen *(E-Mail only, auch «Mailbox Validated» genannt)*
- **E-Mail ID Gold (Pro):** Die Zertifikate enthalten neben der E-Mail-Adresse auch die Organisation und den Namen (oder ein Pseudonym) einer Person *(für Mitarbeitende, auch «Sponsor Validated» genannt).*

Das spricht für die MPKI

- Die Datensicherheitsspezialistin SwissSign ist ein vom Bund anerkannter Schweizer Trust Service Provider (TSP).
- Die Daten werden zu 100 Prozent in der Schweiz gehalten – basierend auf den höchsten, jährlich auditierten Sicherheitsstandards.
- Es kommt nur Schweizer Recht zum Tragen.
- Die Datensicherheitsspezialistin SwissSign erfüllt nationale und internationale Normen und gesetzliche Anforderungen.

Schnittstellen

Neben der manuellen Ausstellung über ein aufgeräumtes Web-GUI unterstützt MPKI auch moderne Protokolle für den automatisierten Zertifikats-Lifecycle:

- Für die Ausstellung von SSL-Zertifikaten wird ACME (Automatic Certificate Management Environment) bereitgestellt.
- Das REST-API basierend auf OpenAPI V3 erlaubt die automatisierte Verwaltung von E-Mail- und SSL-Zertifikaten (inklusive Wildcard).
- Genauso erlaubt die Schnittstelle CMC (Certificate Management over CMS) gemäss Internetstandard RFC 5272 die Automatisierung des Lifecycle für alle Zertifikate.

Für die Automatisierung bietet Ihnen die Datensicherheitsspezialistin SwissSign ein grosses Partnernetzwerk für Zertifikats-Lifecycle-Management-Systeme und E-Mail-Gateway-Lösungen.

Post CH Kommunikation AG
Digital Business
Wankdorfallee 4
3030 Bern

E-Mail digital-business@post.ch
post.ch/zertifikate

Private Managed Public Key Infrastructure (MPKI)
Outsourcing der MPKI in die zertifizierte SwissSign-Umgebung

Der Betrieb einer internen Public Key Infrastructure (PKI) verursacht oftmals hohen finanziellen und personellen Aufwand. Die Lösung dafür ist das Cloud-Outsourcing der internen, privaten PKI in die zertifizierte Umgebung der Datensicherheitsspezialistin SwissSign (in Kombination mit einer Partner-Anwendung). Damit können Sie sich auf Ihr Kerngeschäft fokussieren. Beispiele für eine private MPKI sind Zertifikate für die Microsoft-Umgebung, Mobile Device Management (MDM) oder Internet of Things (IoT). Profitieren Sie bei der Automatisierung der Zertifikatsverwaltung ausserdem vom umfangreichen SwissSign-Partnernetzwerk.

Was ist die Private MPKI?

Innerhalb der Managed PKI betreibt die Datensicherheitsspezialistin SwissSign auf Wunsch Ihre Public Key Infrastructure (PKI) nach Ihren Vorgaben und unter Ihrem Wurzelzertifikat (Root CA).

Die Private Managed PKI richtet sich dabei insbesondere an die Kundschaft, die eine Cloud-Lösung benötigt und von der sicheren, zertifizierten SwissSign-Umgebung profitieren will.

Den Umfang und die Parameter legen Sie dabei gemäss Ihren Bedürfnissen fest. Das Angebot umfasst auf jeden Fall eine kundeneigene Zertifikats-Hierarchie, also

- eine eigene Wurzel-Zertifizierungsstelle (Root-CA),
- eine oder mehrere ausstellende Zertifizierungsstellen (Sub-CA) und
- die anwendungsspezifischen Benutzer- oder Geräte-Zertifikate.

Ihre Vorteile

- Maximale Flexibilität
- Tiefe Kosten und reduzierter Aufwand
- Hohe Sicherheit
- Zertifizierter, sicherer Anbieter

So funktioniert die Private MPKI

Die Private Managed PKI basiert auf demselben zertifizierten System, das auch für die Ausstellung von «öffentlichen» SSL- und E-Mail-Zertifikaten verwendet wird.

Dank standardisierter REST- oder CMC-Schnittstelle stehen Ihnen leistungsfähige Partner-Applikationen für das Auto-enrollment der Zertifikate, für den Einsatz im Mail-Gateway oder in Ihrer Verschlüsselungslösung zur Verfügung. Ihre Zertifikate werden automatisch verwaltet und auf Endgeräten installiert.

Das spricht für die Private MPKI

- Die Datensicherheitsspezialistin SwissSign ist ein vom Bund anerkannter Schweizer Trust Service Provider (TSP).
- Die Daten werden zu 100 Prozent in der Schweiz gehalten – basierend auf den höchsten, jährlich auditierten Sicherheitsstandards.
- Es kommt nur Schweizer Recht zum Tragen.
- Die Datensicherheitsspezialistin SwissSign erfüllt nationale und internationale Normen und gesetzliche Anforderungen.

Post CH Kommunikation AG
Digital Business
Wankdorfallee 4
3030 Bern

E-Mail digital-business@post.ch
post.ch/zertifikate

Certificates as a Service (CaaS)
Automatisierte Zertifikatsverwaltung zur Absicherung Ihrer IT-Infrastruktur

Die Laufzeiten von digitalen Zertifikaten für das Internet werden immer kürzer, und der Bedarf an Verschlüsselung von Datenströmen steigt kontinuierlich. Unentdeckt abgelaufene Zertifikate können die Betriebssicherheit gefährden und rechtliche Konsequenzen nach sich ziehen. Diese und weitere Entwicklungen erhöhen die Mengen der zu verwaltenden Zertifikate deutlich, und das Handling wird technisch komplexer und aufwendiger. Ohne Toolunterstützung ist dieses Thema daher kaum mehr zu bewältigen. Die Certificates-as-a-Service-Lösung (CaaS) der Datensicherheitsspezialistin SwissSign ermöglicht eine einfache, sichere und automatisierte Zertifikatsverwaltung.

Was ist CaaS?

Mit der CaaS-Lösung der Datensicherheitsspezialistin SwissSign können Sie Zertifikate aller Typen und Anwendungsfälle zentral und rund um die Uhr verwalten. Ausserdem kann der gesamte Verwaltungsprozess an einem Ort abgebildet werden. Dies reicht vom Monitoring über das Beantragen und Erneuern von Zertifikaten bis hin zu deren Verteilung auf die umliegenden Zielsysteme. CaaS ist skalierbar für jeden Bedarf und eignet sich daher besonders für kleine und mittlere Unternehmen, die sich voll und ganz auf ihr Kernbusiness fokussieren möchten, ohne Kompromisse bei der IT-Sicherheit einzugehen. Durch das einfache Onboarding sind Sie in wenigen Schritten startklar.

Ihre Vorteile

- Abdeckung des gesamten Zertifikats-Lifecycle
- Zentrale und einheitliche Verwaltung aller Zertifikate
- Hoher Automationsgrad, keine abgelaufenen Zertifikate mehr
- Keine zusätzliche Software notwendig
- Cloudbasierte Lösung mit attraktiver Preisgestaltung

So funktioniert CaaS

CaaS ist eine cloudbasierte Lösung und kombiniert das Zertifikatsmanagement-Tool essendi xc mit der Managed PKI der Datensicherheitsspezialistin SwissSign. Konnektoren schaffen die Verbindung bis zur letzten Meile und bringen die Zertifikate direkt in Ihre Server und Ziel-Devices. Einmal eingerichtet, laufen die meisten Prozesse automatisiert. Die Lösung beinhaltet die folgenden Zertifikatsprodukte:

SSL-Zertifikate

Wählen Sie die Vertrauensstufe Ihres SSL-Zertifikats aus. Als zertifizierte Certificate Authority (CA) orientiert sich die Datensicherheitsspezialistin SwissSign an den bekannten Standards:

- Silver domainvalidiert (DV)
- Gold organisationsvalidiert (OV)
- Gold Extended Validation (EV)

E-Mail-Zertifikate

Entsprechend finden Sie hier auch die Auswahl an E-Mail-Zertifikaten für die Authentisierung bzw. Signatur und Verschlüsselung von E-Mails:

- E-Mail ID Silver (Personal)
- E-Mail ID Gold (Pro)

Post CH Kommunikation AG
Digital Business
Wankdorfallee 4
3030 Bern

E-Mail digital-business@post.ch
post.ch/zertifikate