



Certificats numériques

SwissSign, une spécialiste de la Poste Suisse pour la sécurité des données

Managed Public Key Infrastructure (MPKI)

Gestion automatisée des certificats pour une sécurisation de votre infrastructure informatique

De nouvelles connexions de données entre applications, apps et autres appareils sont ajoutées chaque jour. Cela est source d'opportunités, mais chaque nouveau réseau augmente également le risque potentiel. Les cybercriminels exploitent les éventuelles failles de sécurité. L'infrastructure Managed Public Key de la spécialiste de la sécurité des données SwissSign protège vos applications avec des certificats suisses pour SSL et Secure eMail basés sur les normes de sécurité les plus strictes. De plus, la MPKI de SwissSign est une solution moderne de pointe pour une gestion simple des certificats 24 heures sur 24. Exploitation et stockage des données en Suisse.

Qu'est-ce que la MPKI?

La Managed PKI de la spécialiste de la sécurité des données SwissSign vous permet de vous procurer de manière illimitée et 24 heures sur 24 des certificats de clés publiques pour

- SSL et
- la messagerie électronique sécurisée

Vous bénéficiez de rabais attrayants pour des volumes plus importants.

Vos avantages

- Garantisiez la confidentialité et la protection des données de vos clients et partenaires.
- Chiffrez et authentifiez votre trafic de messagerie électronique.
- Augmentez la confiance de la clientèle dans votre application web et témoignez de l'authenticité de votre présence en ligne.
- Protégez-vous du phishing et des attaques de type «man in the middle».
- Bénéficiez d'une meilleure visibilité en étant mieux classé par Google.
- SwissSign – Swiss Made Software – Swiss Quality



Fonctionnement de la MPKI

Vous gérez de manière autonome et à tout moment les certificats de vos collaboratrices et collaborateurs, de votre clientèle et de vos partenaires. Vous pouvez établir instantanément n'importe quel type de certificat à tout moment via une interface automatisée ou via l'outil d'administration web. Et grâce aux normes d'interface ACME et openAPI, vous pouvez également effectuer l'inscription automatique intégrale des produits partenaires. Les principales fonctions en bref:

- Portail web ergonomique pour l'administration de la MPKI
- Gestion automatisée du cycle de vie des certificats (API REST, ACME ou CMC)
- Rapports par type de certificat, groupe ou date d'expiration
- Traitement électronique des documents contractuels

Niveaux de confiance

Sélectionnez le niveau de confiance de votre certificat SSL. En tant qu'autorité de certification (CA) certifiée, SwissSign, spécialiste de la sécurité des données, se fonde sur les normes connues:

- **Validation de domaine (Domain Validation, DV):** Pour les sites web nécessitant une protection simple, par exemple les blogs, les serveurs de messagerie ou autres.
- **Validation d'organisation (Organisation Validation, OV):** Pour les entreprises qui souhaitent proposer une protection élevée à leurs clients, par exemple les boutiques en ligne ou autres.
- **Validation étendue (Extended Validation, EV):** Pour les entreprises qui souhaitent afficher le niveau de confiance le plus élevé, p. ex. les banques, les grandes boutiques en ligne ou autres.

Certificats d'e-mails

Vous trouverez ici également une sélection de certificats d'e-mail pour l'authentification ou la signature et le chiffrement d'e-mails:

- **E-Mail ID Silver (Personal):** Certificats pour les adresses e-mail. (*E-mail uniquement; également appelé «Mailbox Validated»*)
- **E-Mail ID Gold (Pro):** En plus de l'adresse e-mail, les certificats contiennent l'organisation et le nom (ou un pseudonyme) d'une personne. (*pour les collaborateurs, également appelé «Sponsor Validated»*)

Les arguments de la MPKI

- La spécialiste de la sécurité des données SwissSign est un fournisseur d'accès suisse reconnu par la Confédération.
- Les données sont hébergées à 100% en Suisse – selon les normes les plus strictes en matière de sécurité des logiciels et auditées chaque année.
- Seul le droit suisse est pris en compte.
- La spécialiste de la sécurité des données SwissSign répond aux normes nationales comme internationales, ainsi qu'aux exigences légales.

Interfaces

En plus de l'émission manuelle de certificats via une interface utilisateur web épurée, MPKI prend également en charge des protocoles modernes pour le cycle de vie automatisé des certificats:

- ACME (Automatic Certificate Management Environment) est fourni pour l'émission de certificats SSL.
- L'API REST basée sur OpenAPI V3 permet la gestion automatisée des certificats e-mail et SSL (y compris Wildcard).
- De la même manière, l'interface CMC (Certificate Management over CMS) selon Internet RFC5272 permet d'automatiser le cycle de vie de tous les certificats.

Pour l'automatisation, la spécialiste de la sécurité des données SwissSign vous propose un vaste [réseau de partenaires](#) pour les systèmes de gestion du cycle de vie des certificats et les solutions de passerelle d'e-mail.

Private Managed Public Key Infrastructure (MPKI)

Externalisation de la MPKI dans l'environnement SwissSign certifié

L'exploitation d'une infrastructure à clé publique (PKI) interne est souvent liée à des coûts élevés sur le plan financier et des ressources humaines. La solution à cela est l'externalisation sur le cloud de la PKI interne et privée dans l'environnement certifié de la spécialiste de la sécurité des données SwissSign (en combinaison avec une application partenaire). Ainsi, vous pouvez vous concentrer pleinement sur votre cœur de métier. Les certificats pour l'environnement Microsoft, la gestion des dispositifs mobiles (Mobile Device Management, MDM) ou l'Internet des objets (IdO) sont des exemples de MPKI privée. Profitez également du vaste réseau de partenaires de SwissSign pour automatiser la gestion des certificats.

Qu'est-ce qu'une MPKI privée?

Dans la Managed PKI, la spécialiste de la sécurité des données SwissSign exploite sur demande votre infrastructure de clé publique (PKI) selon vos spécifications et sous votre certificat racine (Root CA).

La Private Managed PKI s'adresse en particulier à la clientèle qui a besoin d'une solution cloud et qui souhaite profiter de l'environnement sécurisé et certifié de SwissSign.

Vous définissez l'étendue et les paramètres en fonction de vos besoins. L'offre comprend systématiquement une hiérarchie de certificats propre au client, à savoir:

- un organisme de certification racine (Root CA);
- un ou plusieurs organismes de certification et d'émission (Sub-CA);
- les certificats d'utilisateur ou d'appareil spécifiques à l'application.

Vos avantages

- Flexibilité maximale
- Faibles coûts et charges réduites
- Sécurité élevée
- Prestataire sûr et certifié

Fonctionnement de la Private MPKI

La Private Managed PKI repose sur le même système certifié qui est utilisé pour l'établissement de certificats «publics» SSL et d'e-mails.

Grâce à l'interface standardisée REST ou CMC, vous disposez d'applications partenaires performantes pour l'inscription automatique des certificats, l'intégration à la passerelle de messagerie ou dans votre solution de chiffrement. Vos certificats sont gérés et installés sur les terminaux finaux de manière automatique.

Avantages de la Private MPKI

- La spécialiste de la sécurité des données SwissSign est un fournisseur d'accès suisse reconnu par la Confédération.
- Les données sont hébergées à 100% en Suisse – selon les normes les plus strictes en matière de sécurité des logiciels et auditées chaque année.
- Seul le droit suisse est pris en compte.
- La spécialiste de la sécurité des données SwissSign répond aux normes nationales comme internationales, ainsi qu'aux exigences légales.

Certificates as a Service (CaaS)

Gestion automatisée des certificats pour une sécurisation de votre infrastructure informatique

Les durées de validité des certificats numériques sur Internet sont de plus en plus courtes et le besoin de chiffrer les flux de données ne cesse d'augmenter. Des certificats expirés non détectés peuvent compromettre la sécurité de l'entreprise et avoir des conséquences juridiques. Ces évolutions, et d'autres, augmentent considérablement les volumes de certificats à gérer et leur traitement devient techniquement plus complexe et plus coûteux. Un sujet difficile à maîtriser sans l'aide d'un outil. La solution Certificates-as-a-Service (CaaS) de la spécialiste de la sécurité des données SwissSign permet une gestion simple, sûre et automatisée des certificats.

Qu'est-ce que la solution CaaS?

La solution CaaS de la spécialiste de la sécurité des données SwissSign vous permet de gérer à tout moment et de manière centralisée les certificats de tout type ainsi que les cas d'application. En outre, l'ensemble du processus administratif peut être cartographié en un seul endroit. Cela va de la surveillance à la distribution des certificats aux systèmes cibles environnants, en passant par la demande et le renouvellement des certificats. La solution CaaS est évolutive pour répondre à n'importe quel besoin et convient ainsi particulièrement bien aux PME, qui souhaitent pleinement se concentrer sur leur cœur de métier, sans faire de concession en matière de sécurité informatique. Grâce à la simplicité de l'onboarding, vous êtes prêt à vous lancer en quelques étapes.

Vos avantages

- Couverture de l'ensemble du cycle de vie des certificats
- Gestion centralisée et uniforme de tous les certificats
- Haut niveau d'automatisation, disparition des certificats expirés
- Aucun autre logiciel nécessaire
- Solution basée sur le cloud avec une tarification attractive

Fonctionnement de la solution CaaS

CaaS est une solution basée sur le cloud qui combine l'outil de gestion des certificats [essendi xc](#) avec la Managed PKI de SwissSign, la spécialiste de la sécurité des données. Les connecteurs établissent la connexion jusqu'au bout pour livrer les certificats directement à vos serveurs et aux appareils cibles. Une fois configurés, la plupart des processus fonctionnent de manière automatisée. La solution comprend les produits de certificat suivants:

Certificats SSL

Sélectionnez le niveau de confiance de votre certificat SSL. En tant qu'autorité de certification (CA) certifiée, SwissSign, spécialiste de la sécurité des données, se fonde sur les normes connues:

- Silver Domain Validated (DV)
- Gold Organisation Validated (OV)
- Gold extended Validation (EV)

Certificats d'e-mails

Vous trouverez ici également une sélection de certificats d'e-mail pour l'authentification ou la signature et le chiffrement d'e-mails:

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