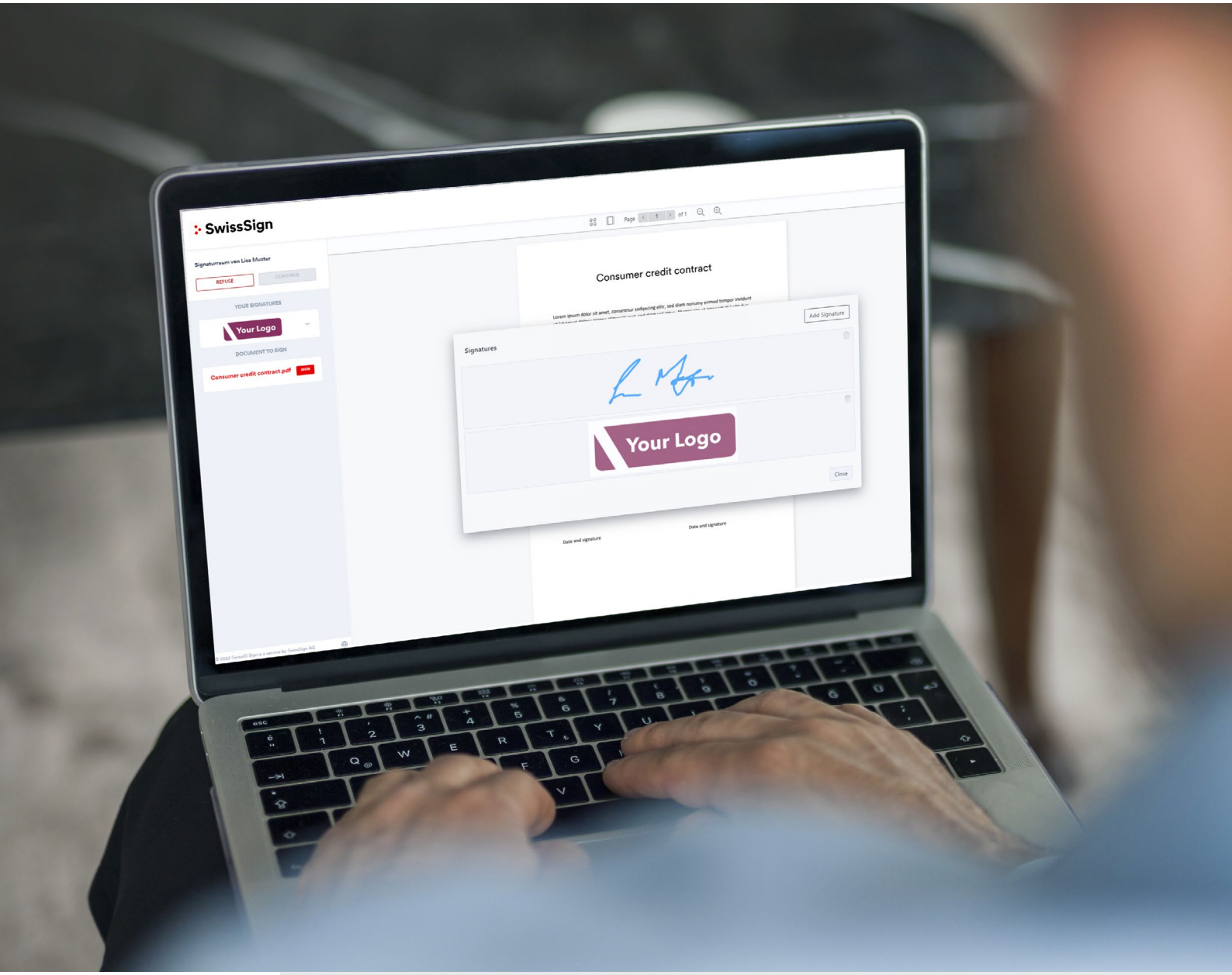
SwissSign



Guide pratique pour la mise en œuvre de signatures électroniques simples et avancées juridiquement conformes dans l'informatique bancaire

SwissSign

Les signatures électroniques se situent au cœur de la transformation numérique dans le secteur bancaire. Qu'il s'agisse de numériser les approbations internes, les transactions avec les clients ou les flux de travail relatifs à la conformité, les signatures électroniques permettent de réduire les délais, de renforcer la traçabilité et d'éliminer le papier de l'équation. Mais si vous avez recours aux **signatures électroniques simples (SES)** ou aux **signatures électroniques avancées (SEA)** au lieu de **signatures électroniques qualifiées (SEQ)**, car cette approche peut s'avérer plus efficace et offrir un meilleur retour sur investissement, vous devez vous assurer que leur mise en œuvre est **solide sur le plan juridique**.

Ce guide s'adresse aux spécialistes IT des services bancaires et financiers qui envisagent d'utiliser notre solution sur site ou qui l'utilisent déjà afin de mettre en œuvre des SES ou des SEA dans le respect des exigences légales de la Suisse et de l'UE et qui s'alignent sur les normes internes en matière de conformité.

1. Connaître les exigences légales relatives aux SES et aux SEA

Les SES et les SEA sont juridiquement valides en vertu du droit suisse et du droit européen, à condition toutefois qu'elles remplissent certaines conditions, par exemple, si une signature manuscrite ou une signature électronique qualifiée n'est pas obligatoire. La loi fédérale suisse sur les signatures électroniques (SCSE) et le règlement européen eIDAS définissent **quatre principes fondamentaux pour les AES:**

1. La signature doit être liée au signataire de manière univoque.

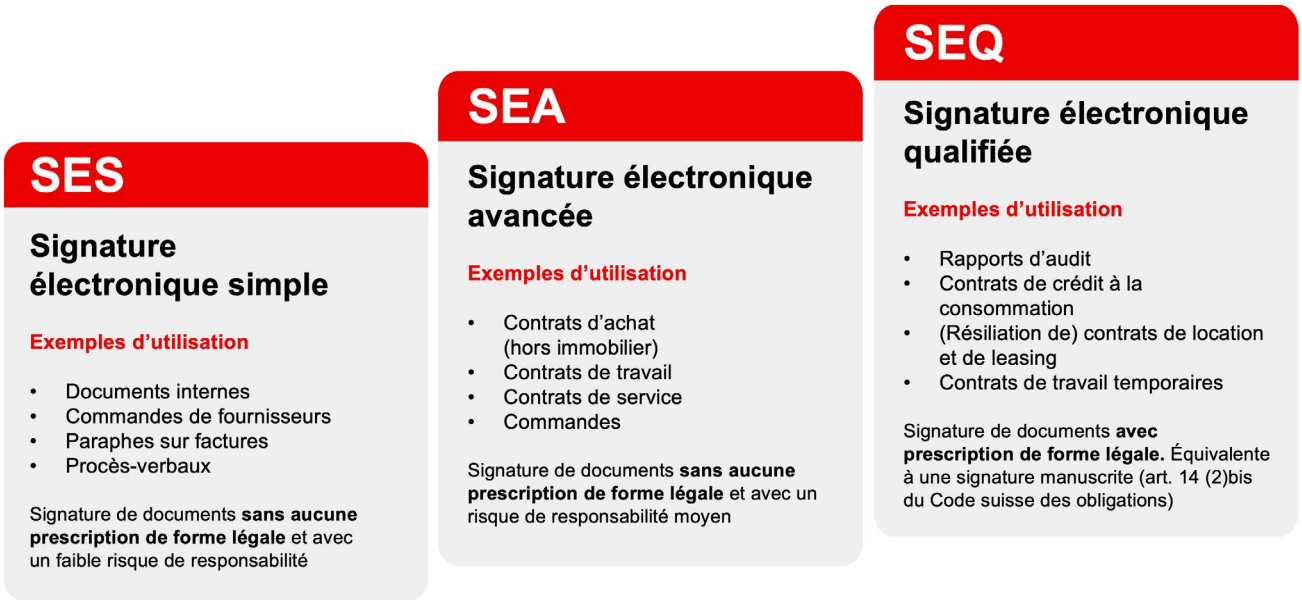
2. Elle doit permettre d'identifier le signataire.

3. Elle doit être créée à l'aide de méthodes placées sous le contrôle exclusif du signataire.

4. Elle doit être liée aux données associées à cette signature de manière à ce que toute modification soit détectable.

Pour un SES, il suffit de combiner les données afin de pouvoir procéder à une authentification.

Ces principes garantissent la fiabilité d'un document signé devant un tribunal. Leur mise en œuvre correcte (en particulier les SES et les SEA) nécessite de concevoir un système cohérant, de gérer les identités de manière sécurisée et de disposer d'une piste d'audit des signatures digne de confiance.



SwissSign

2. Établir la confiance à travers l'unicité

Une signature numérique devrait **être liée de manière univoque à la personne signataire**.

Tout commence en définissant **un identifiant primaire**.

Notre solution sur site se base sur un **identifiant universel unique (UUID)** pour chaque utilisateur, garantissant ainsi l'unicité technique. Cet UUID peut être remplacé par d'autres identifiants propriétaires tels que:

- les numéros de téléphone mobile (en particulier en Suisse, où l'émission des cartes SIM est vérifiée),
- les identifiants des employés ou des clients,
- les numéros de compte bancaire,
- les numéros d'assurance nationale ou de passeport.

Plus les obstacles à la reproduction de cet identifiant sont solides, plus la confiance juridique est forte. L'unicité ne suffit pas à garantir l'identification, mais elle en est la base.

3. Identification du signataire

L'identification correcte constitue un point essentiel, en particulier pour les SEA. En effet, même la méthode d'authentification la plus solide n'a aucune valeur si vous ne pouvez pas prouver qui a été authentifié.

Notre solution sur site prend en charge différentes méthodes d'identification et vous permet de définir un niveau de confiance en fonction de vos besoins.

3.1 Identification par e-mail

De nombreuses solutions SES s'appuient sur une adresse électronique pour identifier le signataire. Cette solution peut être un risque acceptable dans les flux de travail à faible risque, mais présente des limites:

- Les e-mails peuvent être partagés ou anonymes.
- La fiabilité dépend fortement de la manière dont l'email a été collecté (par exemple, intégration des clients, systèmes internes de ressources humaines).

3.2 Identification basée sur la carte SIM

En Suisse, l'obtention d'une carte SIM nécessite la présentation d'une pièce d'identité. Les numéros de téléphone mobile constituent ainsi un identifiant fiable. Certaines solutions SEA reposent uniquement sur cette méthode.

3.3 Identification combinée

Notre solution sur site permet de combiner plusieurs points de données: adresse e-mail, numéro de téléphone, nom et même signature visuelle. Si ces informations sont collectées dans le cadre d'un processus d'intégration sécurisé (par exemple, identification vidéo, vérification face à face), elles peuvent satisfaire aux exigences d'identification de la SEA généralement.

3.4 Intégration avec les fournisseurs d'identité (IdP)

Nous prenons en charge l'intégration d'OpenID Connect (OIDC) avec les fournisseurs d'identité d'entreprise. Le niveau de confiance dépend alors du processus d'intégration de l'IdP. Si l'identité des utilisateurs a été vérifiée à l'aide d'une pièce d'identité délivrée par un gouvernement, les données sont suffisamment fiables pour une identification SEA. S'ils ne se sont inscrits qu'à l'aide d'une adresse e-mail, il s'agit au mieux d'un niveau SES.

3.5 Processus internes (KYC, RH, etc.)

Les banques disposent souvent de processus de connaissance client (KYC) ou d'intégration des employés. Ces méthodes peuvent être utilisées à des fins d'identification de signature. Si votre KYC implique une vérification en personne et la présentation d'une pièce d'identité, il est probable que votre méthode d'identification soit conforme à la SEA.

4. Recueillir le consentement par signature

La troisième exigence légale concerne le **consentement par signature**, à savoir démontrer que l'utilisateur a réellement accepté de signer et qu'il est le seul à avoir le contrôle de l'acte de signature.Notre solution sur site prévoit plusieurs options à cet effet:

4.1 Code de mot de passe à usage unique (OTP) par SMS

Méthode encore largement utilisée, en particulier en Suisse. Le SMS constitue une solution solide lorsque le numéro a été vérifié, mais présente des faiblesses connues (par exemple, l'échange de cartes SIM).

4.2 Authentification par application mobile

Notre application mobile permet d'effectuer des signatures sécurisées de niveau SEA en combinant propriété de l'appareil et authentification biométrique. Les utilisateurs doivent s'authentifier à l'aide de leur empreinte digitale ou de la reconnaissance faciale avant de signer.

Le processus d'intégration, c'est-à-dire la manière dont l'application mobile est activée, joue un rôle essentiel. Les méthodes les plus courantes sont les suivantes:

- Code QR remis en mains propres
- Lettre contenant un code d'activation
- Session authentifiée via le système interne

Plus l'activation est sécurisée, plus le niveau de confiance est élevé.

4.3 Authentification de tiers basée sur l'OIDC

Notre solution permet de déclencher l'authentification via votre système de connexion existant. Cette solution convient particulièrement aux banques qui utilisent le protocole LDAP, Active Directory ou d'autres plateformes SSO.

Nous fournissons les métadonnées des documents (hachages, identifiants, horodatages) à l'IdP, afin que vous puissiez rattacher l'authentification à l'événement de signature.

4.4 Authentification en amont

Dans certains cas, il est demandé aux utilisateurs de se connecter à un portail avant de voir les documents à signer. Ce contrôle d'accès peut se doubler d'un consentement par signature.

4.5 SCAL2 et contrôle exclusif

Bien qu'il ne soit pas requis pour les SEA, le niveau 2 de garantie de contrôle exclusif (SCAL2: Sole Control Assurance Level 2) est obligatoire pour les SEQ. Si votre banque envisage de passer aux SEQ à l'avenir, vous pouvez envisager de vous préparer au SCAL2.

5. Garantir l'intégrité des données

La quatrième règle juridique exige que la signature soit liée aux données signées et que toute modification entraîne l'invalidation de la signature.

Notre solution sur site prend en charge les normes suivantes:

5.1 CAdES (Cryptographic Message Syntax Advanced Electronic Signatures)

Norme utilisée pour les données brutes ou structurées telles que JSON ou XML. La signature est alors stockée séparément et référencée par hachage dans une piste d'audit sécurisée.

5.2 PAdES (PDF Advanced Electronic Signatures)

Norme employée pour les fichiers PDF. La signature et les métadonnées (nom, heure, motif, etc.) sont intégrées directement dans le PDF, assurant des contrôles de validité prêts à l'emploi dans des outils tels qu'Adobe Acrobat.

Nous conservons une **piste d'audit inviolable** qui enregistre:

- les événements de signature (horodatage, valeurs de hachage),
- les détails de l'identité authentifiée,
- le contexte de l'appareil / du navigateur,
- les certificats et métadonnées cryptographiques.

Cette procédure garantit une vérification indépendante et une analyse médico-légale, même des années plus tard.

6. La confiance visuelle et le facteur humain

Même si la validité juridique est mathématique, les gens souhaitent toujours «voir» une signature.

Notre solution sur site prend en charge:

- les signatures visuelles sur chaque page (via les annotations de signature),
- les flux de travail basés sur des cases à cocher (par exemple, ne signer qu'après avoir passé en revue chaque page),
- la sortie au format PDF aplati et comportant un sceau de signature pour empêcher toute modification ultérieure.

Nous prenons également en charge les certificats **Adobe compatibles AATL**. Ainsi, les signatures apparaissent comme valides dans Adobe Reader et ne déclenchent aucun message d'avertissement, même si elles ne sont pas basées sur une signature qualifiée.

Si nécessaire, nous pouvons signer au nom de l'organisation à l'aide d'un caché d'organisation et inclure les données de l'utilisateur (nom, courriel, téléphone) dans les métadonnées du PDF.

7. Analyse des risques et soutien à la conformité

Les SES et SEA s'appuient essentiellement sur la **documentation et l'analyse des risques**. Les équipes chargées de la conformité doivent évaluer la mise en œuvre de bout en bout:

- **Unicité**: Quel est l'identifiant utilisé? De quelle manière la duplication est-elle évitée?
- **Identification**: De quelle manière l'identité du signataire est-elle vérifiée?
- **Authentication**: De quelle manière le contrôle exclusif est-il mis en œuvre?
- **Liaison des données**: Par quel moyen sécurisé le document et la signature sont-ils liés?
- **Piste d'audit**: Chaque étape peut-elle être tracée, vérifiée et défendue?

Notre piste d'audit et notre cadre de documentation appuient vos efforts en matière de conformité. Que vous vous prépariez à un contrôle de la FINMA, à des audits internes ou à des litiges externes, nous vous aidons à fournir des preuves.

Conclusion

Grâce à notre solution sur site, les banques sont en mesure de mettre en œuvre des systèmes SES et SEA juridiquement robustes, vérifiables et conviviaux. Que vous souhaitiez mettre en place des flux de travail internes sécurisés ou rationaliser les processus d'interaction avec la clientèle, notre plateforme s'adapte à votre environnement IT, à votre architecture d'identité et à vos besoins en matière de conformité.

Et si votre institution vise à obtenir à l'avenir des services fiduciaires qualifiés SEQ ou eIDAS, nous vous aidons dès aujourd'hui à mettre en place les bases techniques et procédurales nécessaires.

Avertissement : ces informations représentent l'opinion de SwissSign, qui les a recueillies au mieux de ses connaissances. Cependant, comme nous ne sommes pas un cabinet d'avocats, nous ne garantissons pas l'exactitude des déclarations et n'assumons aucune responsabilité pour les décisions prises sur la base de ces informations. Si vous avez besoin de conseils juridiques pour savoir si une configuration spécifique répond à vos exigences légales, nous vous prions de contacter un cabinet d'avocats compétent.

Alors, êtes-vous prêt à discuter de comment on pourrait faire pour que ça devienne réalité dans votre organisation ?

Prenez rendez-vous avec l'un de nos experts:

www.swisssign.com/banks