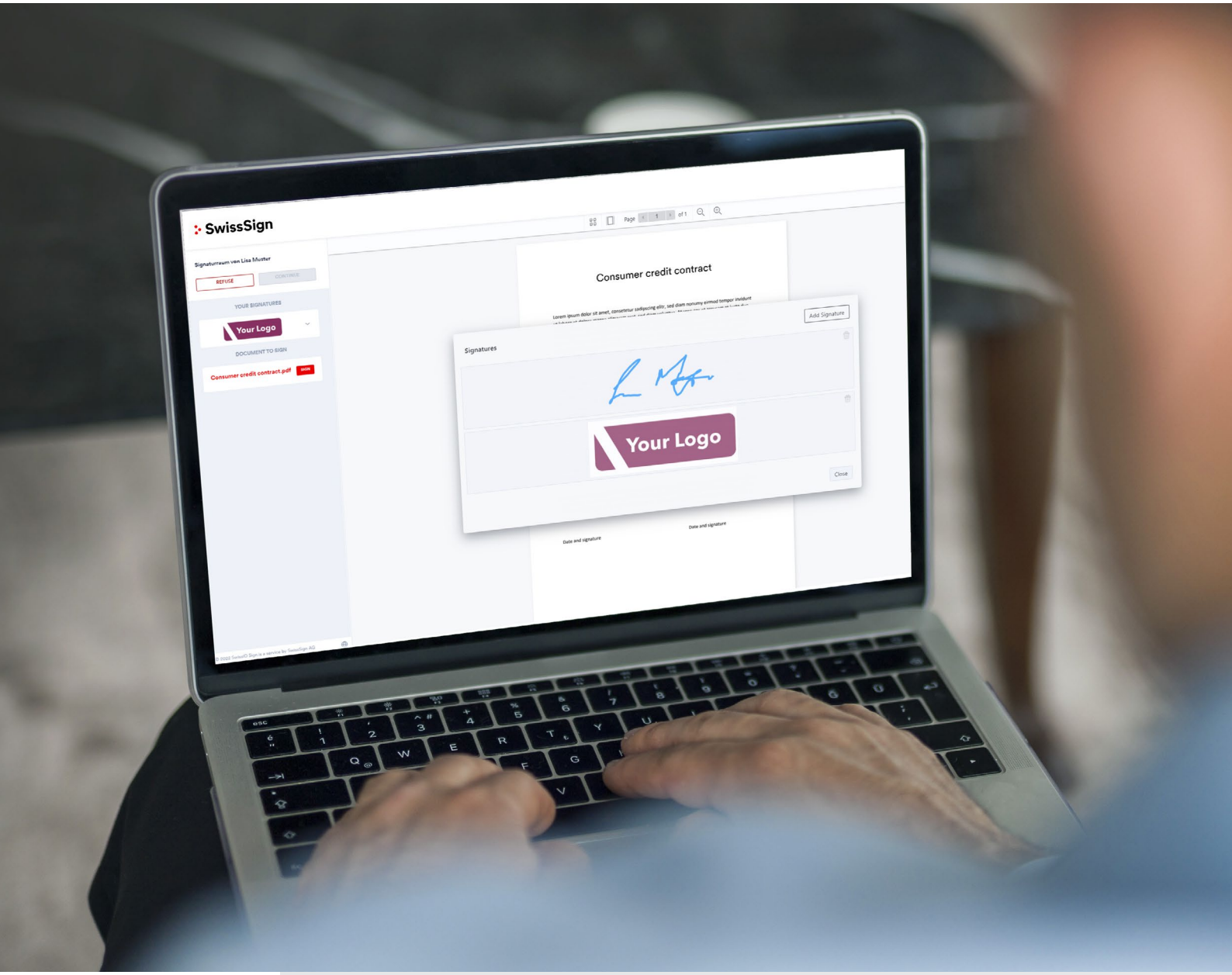
SwissSign



Wie man einfache und fortgeschrittene elektronische Signaturen compliant in der Banken-IT umsetzt – Ein praktischer Leitfaden

SwissSign

Die elektronische Signatur ist ein Schlüsselelement der Digitalisierung im Bankwesen. Egal ob Sie interne Genehmigungsprozesse, Transaktionen mit Kunden oder Compliance-Prozesse digitalisieren: Elektronische Signaturen reduzieren die Bearbeitungszeit, erhöhen die Rückverfolgbarkeit und ersetzen Papier. Wenn Sie jedoch **einfache elektronische Signaturen (SES)**, **fortgeschrittene elektronische Signaturen (AES)** oder **qualifizierte elektronische Signaturen (QES)** verwenden - was eine effizientere Vorgehensweise und eine bessere Rendite verspricht -, müssen Sie sicherstellen, dass die Umsetzung **rechtlich abgesichert** ist.

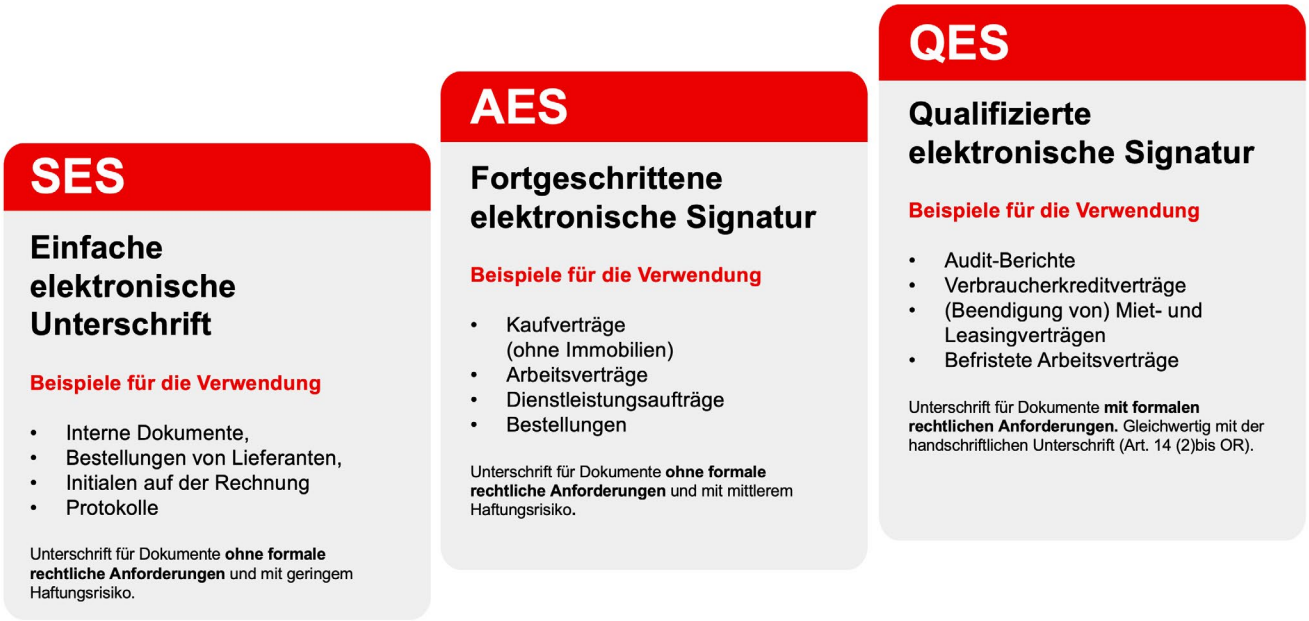
Dieser Leitfaden richtet sich an IT-Profis in der Banken- und Finanzdienstleistungsbranche, die unsere On-Premise-Lösung in Betracht ziehen oder bereits nutzen, um SES oder AES so umzusetzen, dass die rechtlichen Anforderungen in der Schweiz und in der EU erfüllt werden und die internen Compliance-Standards eingehalten werden.

1. Verstehen der rechtlichen Anforderungen für SES und AES

SES und AES sind unter Schweizer und EU-Recht gültig – aber nur unter bestimmten Bedingungen, etwa wenn eine handschriftliche Signatur oder QES nicht vorgeschrieben ist. Das Schweizerische Gesetz über elektronische Signaturen (ESigG) und die EU-eIDAS-Verordnung definieren **vier Kernprinzipien** for AES:

1. Die Unterschrift muss eindeutig mit dem Unterzeichnenden verknüpft sein.
2. Es muss die Identifizierung des Unterzeichners ermöglichen.
3. Es muss mit Mitteln erstellt werden, die sich allein in der Hand des Unterzeichners befinden.
4. Es muss auf eine Weise mit den signierten Daten verknüpft sein, die eine Erkennung von Änderungen ermöglicht.

Für eine SES müssen lediglich Daten kombiniert werden, damit eine Authentifizierung erfolgen kann. Diese Grundsätze stellen sicher, dass ein unterschriebenes Dokument vor Gericht als vertrauenswürdig gilt. Ihre korrekte Umsetzung - insbesondere bei SES und AES - erfordert eine sorgfältige Systemgestaltung, eine sichere Identitätsverwaltung und eine vertrauenswürdige Überprüfung der Unterschriften.



2. Vertrauen durch Einzigartigkeit aufbauen

Eine digitale Unterschrift sollte **einzigartig mit der unterschreibenden Person** verknüpft sein. Dies beginnt mit der Definition eines **primären Identifikators**.

Unsere On-Premise-Lösung verwendet für jeden Benutzer einen **universell eindeutigen Identifikator (UUID)**, der für technische Eindeutigkeit sorgt. Dieser UUID kann mit anderen Identifikatoren verknüpft werden, wie zum Beispiel:

- Mobiltelefonnummern (besonders in der Schweiz, wo die SIM-Kartenausgabe ID-geprüft ist)
- Mitarbeiter- oder Kundennummern
- Bankkontonummern
- Sozialversicherungs- oder Passnummern

Je höher die Hürde für die Replikation dieser Kennung, desto stärker das rechtliche Vertrauen. Einzigartigkeit garantiert zwar nicht die Identifizierung, ist aber die Grundlage dafür.

3. Identifizierung des Unterzeichners

Eine korrekte Identifizierung ist besonders bei AES entscheidend. Selbst die stärkste Authentifizierung ist irrelevant, wenn man nicht beweisen kann, wer authentifiziert wurde.

Unsere On-Premise-Lösung unterstützt verschiedene Identifikationsmethoden und ermöglicht Ihnen, das Vertrauensniveau je nach Geschäftsfall zu definieren.

3.1 E-Mail-basierte Identifizierung

Viele SES-Lösungen verwenden eine E-Mail-Adresse zur Identifizierung des Unterzeichners. Dies kann in risikoarmen Umgebungen ein akzeptables Risiko darstellen, hat jedoch seine Grenzen:

- E-Mails können geteilt oder anonym sein.
- Das Vertrauen hängt stark davon ab, wie die E-Mail gesammelt wurde (z.B. Kundeneinzug, interne HR-Systeme).

3.2 SIM-basierte Identifizierung

In der Schweiz ist die Beschaffung einer SIM-Karte mit einem Ausweisdokument verbunden. Mobiltelefonnummern sind damit ein starkes Identifikationsmerkmal. Einige AES-Lösungen verlassen sich ausschliesslich auf diese Methode.

3.3 Kombinierte Identifizierung

Unsere On-Premise-Lösung ermöglicht es, mehrere Datenpunkte zu kombinieren - E-Mail-Adresse, Telefonnummer, Name und sogar eine visuelle Unterschrift. Wenn diese im Rahmen eines sicheren Onboarding-Prozesses (z.B. Video-ID oder Face-to-Face-Verifizierung) erfasst werden, können sie den Anforderungen der AES-Identifizierung genügen.

3.4 Integration mit Identitätsanbietern (IdPs)

Wir unterstützen die Integration von OpenID Connect (OIDC) mit Identitätsanbietern für Unternehmen. Das Vertrauensniveau hängt dann vom Onboarding-Prozess des IdP ab. Wenn die Identität der Nutzer mit einem vom Staat ausgestellten Ausweis verifiziert wurde, ist das Datenmaterial für eine AES-Identifikation stark genug. Wenn sie sich nur mit einer E-Mail-Adresse registriert haben, ist das bestenfalls SES-Level.

3.5 interne Prozesse (KYC, HR usw.)

Banken verfügen oft über bestehende Know-Your-Customer- (KYC) oder Mitarbeiter-Einstellungsprozesse. Diese können für die Identifizierung der Unterschrift genutzt werden. Wenn Ihre KYC-Verfahren eine Identifizierung vor Ort und die Vorlage von Ausweisdokumenten erfordern, ist Ihre Identifizierungsmethode wahrscheinlich AES-konform.

4. Erfassung der Unterschrift

Die dritte rechtliche Anforderung betrifft die **Unterschriftenerlaubnis** - den Nachweis, dass der Benutzer tatsächlich zugestimmt hat, seine Unterschrift zu leisten, und dass nur er die Kontrolle über die Unterschriftshandlung hatte.

Unsere On-Premise-Lösung bietet hierfür mehrere Optionen:

4.1 SMS-Einmalpasswort (OTP)

Wird immer noch weit verbreitet verwendet, insbesondere in der Schweiz. SMS ist stark, wenn die Nummer verifiziert wurde, hat aber bekannte Schwachstellen (z.B. SIM-Swap).

4.2 Authentifizierung über die Mobile App

Unsere mobile App ermöglicht eine sichere Signatur auf dem Niveau von AES durch die Kombination von Gerätebesitz und biometrischer Authentifizierung. Der Benutzer muss sich vor der Unterzeichnung mit Fingerabdruck oder Gesichtserkennung authentifizieren.

Der Onboarding-Prozess - also wie die mobile App aktiviert wird - ist entscheidend. Häufige Methoden sind:

- QR-Code persönlich übermittelt
- Brief mit Aktivierungscode
- Authentifizierte Sitzung über internes System

Je sicherer die Aktivierung, desto höher das Vertrauensniveau.

4.3 OIDC-basierte Authentifizierung durch Dritte

Unsere Lösung kann die Authentifizierung über Ihr bestehendes Login-System auslösen. Dies ist ideal für Banken, die LDAP, Active Directory oder andere SSO-Plattformen verwenden.

Wir liefern dem IdP Dokumentmetadaten (Hashs, IDs, Zeitstempel) bereit, damit Sie die Authentifizierung mit dem Unterschreibungsereignis verknüpfen können.

4.4 Authentifizierung auf Ebene des Oberlaufs

In einigen Fällen müssen Benutzer sich in ein Portal einloggen, bevor sie Dokumente zur Unterschrift sehen können. Diese Zugriffskontrolle kann als Zustimmung zur Unterschrift dienen - aber nur, wenn das Risiko der Vertretung (z. B. dass jemand anders die Sitzung nutzt) minimal ist.

4.5 SCAL2 und Sole Control

Während AES diese nicht erfordert, ist SCAL2 (Sole Control Assurance Level 2) für QES obligatorisch. Wenn Ihre Bank in Zukunft auf QES umstellen möchte, können Sie die SCAL2-Reifeprüfung in Betracht ziehen.

5. Gewährleistung der Datenintegrität

Die vierte rechtliche Regel besagt, dass die Unterschrift an die unterschriebenen Daten gebunden ist und jede Änderung die Gültigkeit der Unterschrift aufhebt.

Unsere On-Premise-Lösung unterstützt die folgenden Standards:

5.1 CAdES (Cryptographische Nachrichtensyntax für fortgeschrittene elektronische Signaturen)

Für Rohdaten oder strukturierte Daten wie JSON oder XML verwendet. Die Signatur wird separat gespeichert und über einen Hash in einer sicheren Audit-Trail-Datei referenziert.

5.2 PAdES (PDF Advanced Electronic Signatures)

Für PDF-Dateien verwendet. Die Signatur und Metadaten (Name, Datum, Grund usw.) werden direkt in das PDF eingebettet, um so eine sofortige Gültigkeitsprüfung in Tools wie Adobe Acrobat zu ermöglichen.

Wir führen eine **manipulationssichere Audit-Trail,** der Folgendes aufzeichnet:

- Signaturereignisse (Zeitstempel, Hash-Werte)
- Authentifizierte Identitätsdaten
- Geräte-/Browserkontext
- Zertifikate und kryptografische Metadaten

Dies ermöglicht eine unabhängige Überprüfung und forensische Analyse - sogar Jahre später.

6. Visuelle Vertrauensbildung und der menschliche Faktor

Auch wenn die rechtliche Gültigkeit mathematisch ist, wollen die Menschen immer noch eine “Unterschrift” sehen.

Unsere On-Premise-Lösung unterstützt:

- Visuelle Signaturen auf jeder Seite (über Signaturhinweise)
- Workflows basierend auf Checkboxen (z. B. erst nach Überprüfung jeder Seite unterschreiben)
- Flachgedrucktes PDF mit Siegelung der Unterschrift zur Verhinderung von späteren Bearbeitungen

SwissSign

Wir unterstützen auch **Adobe AATL-kompatible** Zertifikate. Dies gewährleistet, dass die Signaturen in Adobe Reader als gültig erkannt werden und keine Warnmeldungen auslösen, selbst wenn sie nicht auf einer qualifizierten Signatur basieren.

Wenn erforderlich, können wir im Namen der Organisation mit einem Organisationsstempel unterschreiben und Benutzerdaten (Name, E-Mail, Telefon) in den PDF-Metadaten aufnehmen.

7. Risikoanalyse und Unterstützung bei der Einhaltung

SES und AES verlassen sich stark auf **Dokumentation und Risikoanalyse**. Die Compliance-Teams müssen die Umsetzung von Anfang bis Ende bewerten:

- **Einzigartigkeit**: Welcher Identifikator wird verwendet? Wie wird eine Duplizierung verhindert?
- **Identifizierung**: Wie wird die Identität des Unterzeichners verifiziert?
- **Authentifizierung**: Wie wird die alleinige Kontrolle durchgesetzt?
- **Datenbindung**: Wie werden Dokument und Unterschrift sicher miteinander verknüpft?
- **Audit Trail**: Kann jeder Schritt zurückverfolgt, verifiziert und verteidigt werden?

Unser Audit-Trail- und Dokumentationskonzept unterstützt Sie bei Ihren Compliance-Anstrengungen. Egal ob Sie sich auf eine FINMA-Prüfung, interne Audits oder externe Streitigkeiten vorbereiten - wir helfen Ihnen dabei, Beweise zu erbringen.

Fazit

Mit unserer On-Premise-Lösung können Banken robuste, nachprüfbare und benutzerfreundliche SES- und AES-Lösungen umsetzen. Egal ob Sie interne Abläufe absichern oder Prozesse für die Kundenbetreuung optimieren möchten - unsere Plattform passt sich Ihrer IT-Umgebung, Ihrer Identitätsarchitektur und Ihren Compliance-Anforderungen an.

Und wenn Ihre Institution in Zukunft auf QES- oder eIDAS-zertifizierte Trust Services abzielt, helfen wir Ihnen heute, die technische und prozessuale Grundlage dafür zu schaffen.

Haftungsausschluss: Diese Informationen geben die Meinung von SwissSign wieder, die diese nach bestem Wissen und Gewissen zusammengestellt hat. Da wir jedoch keine Anwaltskanzlei sind, übernehmen wir keine Gewähr für die Richtigkeit der nachstehenden Aussagen und keine Haftung für Entscheidungen, die auf der Grundlage dieser Informationen getroffen werden. Wenn Sie Rechtsberatung benötigen, um zu klären, ob eine bestimmte Konfiguration Ihren rechtlichen Anforderungen entspricht, wenden Sie sich bitte an eine entsprechende Anwaltskanzlei.

Wollen wir besprechen, wie dies in Ihrem Unternehmen aussehen könnte?

Vereinbaren Sie einen Termin mit einem unserer Experten:

www.swisssign.com/banks