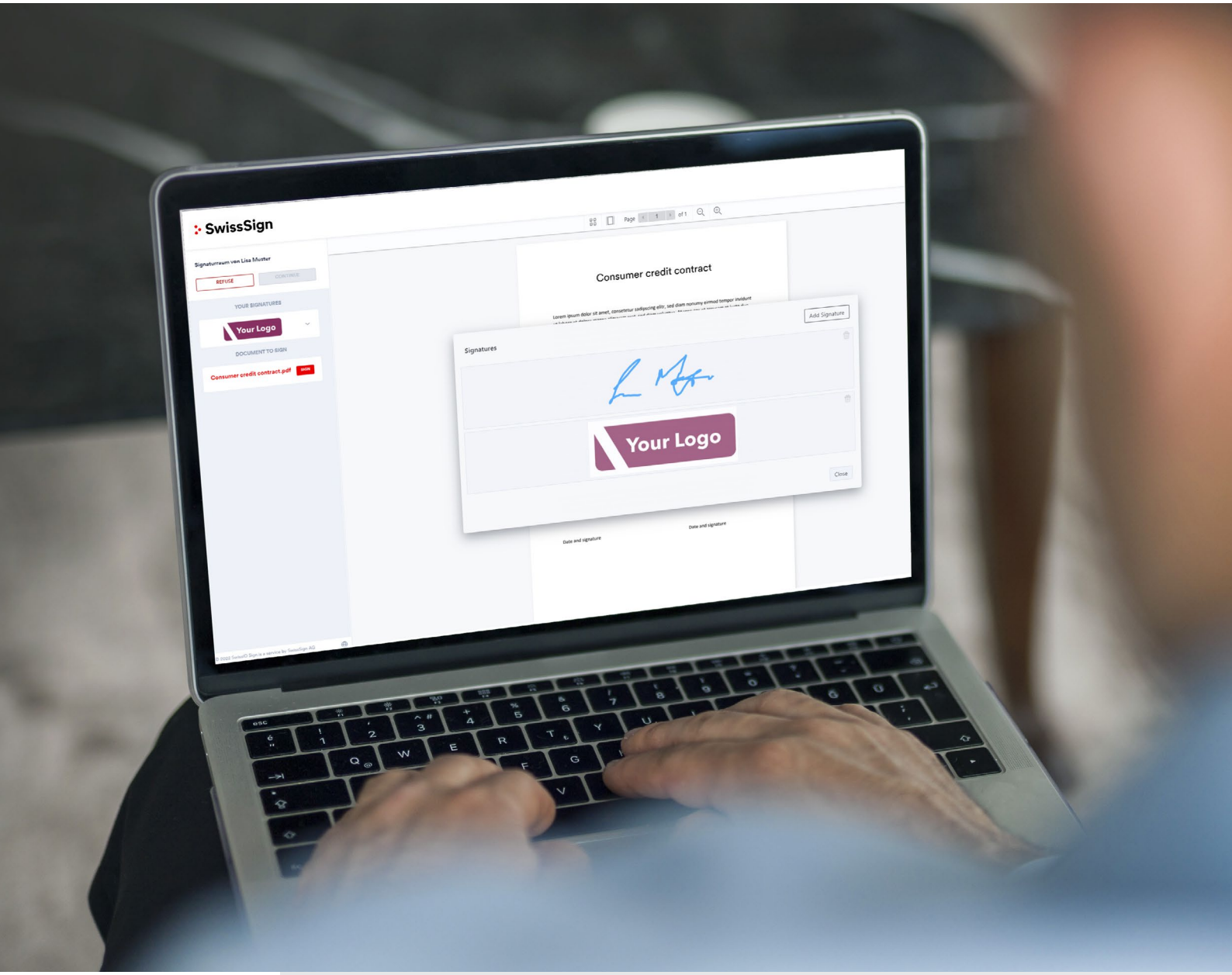
SwissSign



How to Implement Compliant Simple and Advanced Electronic Signatures in Banking IT – A Practical Guide

SwissSign

Electronic signatures are at the heart of digital transformation in banking. Whether you're digitising internal approvals, customer transactions or compliance workflows, electronic signatures help reduce time, increase traceability and remove paper from the equation. But if you're using **simple electronic signatures (SES)** or **advanced electronic signatures (AES)** and **qualified electronic signatures (QES)**—as this approach might be more efficient and provide a better return-on-investment—you need to make sure your implementation is **legally robust.**

This guide is for IT professionals in banking and financial services who consider using our on-premise solution or do so already to implement SES or AES in a way that satisfies Swiss and EU legal requirements and aligns with internal compliance standards.

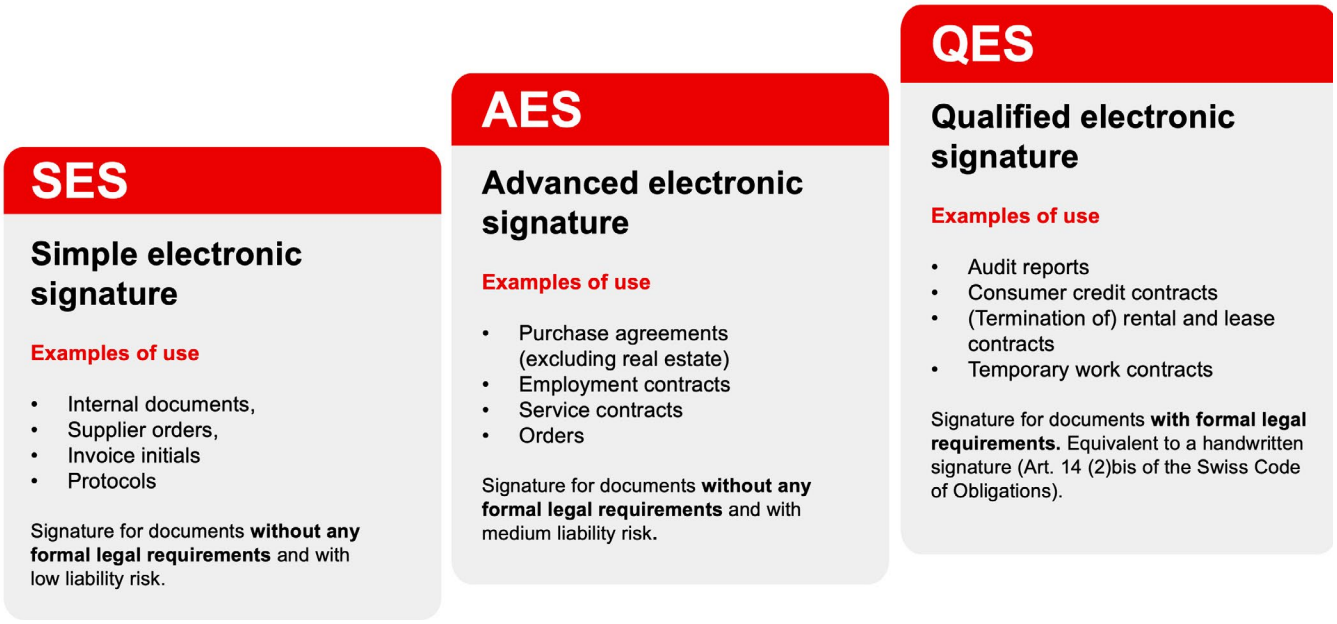
1. Understanding the Legal Requirements for SES and AES

SES and AES are legally valid under Swiss and EU law—but only when certain conditions are met (e.g. if a handwritten signature or a QES is not mandatory). The Swiss Federal Act on Electronic Signatures (ESigA) and the European eIDAS regulation define **four core principles for AES**:

1. The signature must be uniquely linked to the signatory.
2. It must enable identification of the signatory.
3. It must be created using means under the sole control of the signatory.
4. It must be linked to the signed data in a way that allows detection of any change.

For an SES it is only necessary to combine data so an authentication can be made.

These principles ensure that a signed document can be attributed to the signer. Implementing them properly—especially with SES and AES—requires thoughtful system design, secure identity handling and a trustworthy signature audit trail.



SwissSign

2. Building Trust Through Uniqueness

A digital signature should **be uniquely linked to the person** who signed. This starts with defining a **primary identifier**.

Our on-premise solution uses a **universally unique identifier (UUID)** for each user, ensuring technical uniqueness. This UUID can be linked to other identifiers such as:

- Mobile phone numbers (especially in Switzerland, where SIM issuance is ID-verified)
- Employee or customer IDs
- Bank account numbers
- National insurance or passport numbers

The higher the barrier to replication of this identifier, the stronger the legal trust. Uniqueness doesn't guarantee identification—but it's the foundation.

3. Identifying the Signatory

Proper identification is critical, especially for AES. Even the strongest authentication is irrelevant if you can't prove who was authenticated. Our on-premise solution supports different methods of identification, and allows you to define the level of trust depending on your business case.

3.1 Email-based Identification

Many SES solutions use an email address to identify the signer. This can be an acceptable risk in low-risk workflows but has limitations:

- Emails can be shared or anonymous.
- Trust depends heavily on how the email was collected (e.g., customer onboarding, internal HR systems).

3.2 SIM-based Identification

In Switzerland, obtaining a SIM card requires presenting an ID. This makes mobile numbers a strong identifier. Some AES solutions rely solely on this method.

3.3 Combined Identification

Our on-premise solution allows combining multiple data points—email, phone number, name, and even visual signature. If these are collected in a secure onboarding process (e.g., video ID, face-to-face verification), they can in general satisfy AES identification requirements.

3.4 Integration with Identity Providers (IdPs)

We support OpenID Connect (OIDC) integration with enterprise identity providers. The trust level then depends on the IdP's onboarding process. If users were verified using government-issued ID, the data is strong enough for an AES identification. If they only registered with an email, it's SES-level at best.

3.5 Internal Processes (KYC, HR, etc.)

Banks often have existing Know-Your-Customer (KYC) or employee onboarding processes. These can be leveraged for signature identification. If your KYC involves in-person verification and ID documentation, then your identification method is likely AES-compliant.

4. Capturing Signature Consent

The third legal requirement is about **signature consent**—proving that the user actually agreed to sign, and that only they had control over the signing act. Our on-premise solution provides multiple options for this:

4.1 SMS One-Time Password (OTP)

Still widely used, especially in Switzerland. SMS is strong when the number has been ID-verified, but has known weaknesses (e.g., SIM-swapping).

4.2 Mobile App Authentication

Our mobile app enables secure, AES-level signing by combining device ownership and biometric authentication. Users must authenticate using fingerprint or facial recognition before signing. The onboarding process—i.e., how the mobile app is activated—is key. Common methods include:

- QR code delivered in person
- Letter with activation code
- Authenticated session via internal system

The more secure the activation, the higher the trust level.

4.3 OIDC-Based Third-Party Authentication

Our solution can trigger authentication via your existing login system. This is ideal for banks using LDAP, Active Directory, or other SSO platforms.

We provide document metadata (hashes, IDs, timestamps) to the IdP, so you can bind authentication to the signing event.

4.4 Upstream Authentication

In some cases, users must log in to a portal before seeing documents to sign. This access control can double as signature consent.

4.5 SCAL2 and Sole Control

While not required for AES, SCAL2 (Sole Control Assurance Level 2) is mandatory for QES. If your bank plans to move toward QES in the future, you can consider SCAL2 readiness.

5. Ensuring Data Integrity

The fourth legal rule requires that the signature is bound to the signed data—and any modification invalidates the signature.

Our on-premise solution supports the following standards:

5.1 CAdES (Cryptographic Message Syntax Advanced Electronic Signatures)

Used for raw or structured data like JSON or XML. The signature is stored separately and referenced via hash in a secure audit trail.

5.2 PAdES (PDF Advanced Electronic Signatures)

Used for PDF files. Signature and metadata (name, time, reason, etc.) are embedded directly in the PDF, ensuring out-of-the-box validity checks in tools like Adobe Acrobat.

We maintain a **tamper-proof audit trail** that records:

- Signature events (timestamps, hash values)
- Authenticated identity details
- Device/browser context
- Certificates and cryptographic metadata

This allows independent verification and forensic analysis—even years later.

6. Visual Trust and the Human Factor

Even if legal validity is mathematical, people still want to “see” a signature.
Our on-premise solution supports:

- Visual signatures on each page (via signature annotations)
- Checkbox-based workflows (e.g., sign only after reviewing each page)
- Flattened PDF output with signature seal to prevent later edits

We also support **Adobe AATL-compatible** certificates. This ensures that signatures appear as valid in Adobe Reader and don’t trigger warning messages, even if they’re not based on a qualified signature.

If required, we can sign on behalf of the organisation using an organisational seal and include userdata (name, email, phone) in the PDF metadata.

7. Risk Analysis and Compliance Support

SES and AES rely heavily on **documentation and risk analysis**. Compliance teams must evaluate the implementation from end to end:

- **Uniqueness**: What identifier is used? How is duplication avoided?
- **Identification**: How is the signatory’s identity verified?
- **Authentication**: How is sole control enforced?
- **Data Binding**: How are document and signature securely linked?
- **Audit Trail**: Can every step be traced, verified and defended?

Our audit trail and documentation framework supports your compliance efforts. Whether you’re preparing for FINMA review, internal audits or external disputes—we help you deliver proof.

SwissSign

Conclusion

With our on-premise solution, banks can implement SES and AES that are legally robust, auditable, and user-friendly. Whether you're enabling secure internal workflows or streamlining client-facing processes, our platform adapts to your IT environment, identity architecture and compliance needs.

And if your institution is aiming for QES or eIDAS-qualified trust services in the future, we help you lay the technical and procedural groundwork today.

Disclaimer: this information represents the view of SwissSign, which collected the information to the best of their knowledge. However, as we are not a law firm, we do not guarantee the correctness of the below statements and do not assume any liability for decisions based on this information. In case you need legal advice if a specific set up meets your legal requirements, we kindly ask you to contact a respective law firm.

Are you ready to discuss how this could look like in your organisation?

Book a call with one of our experts:

www.swisssign.com/banks