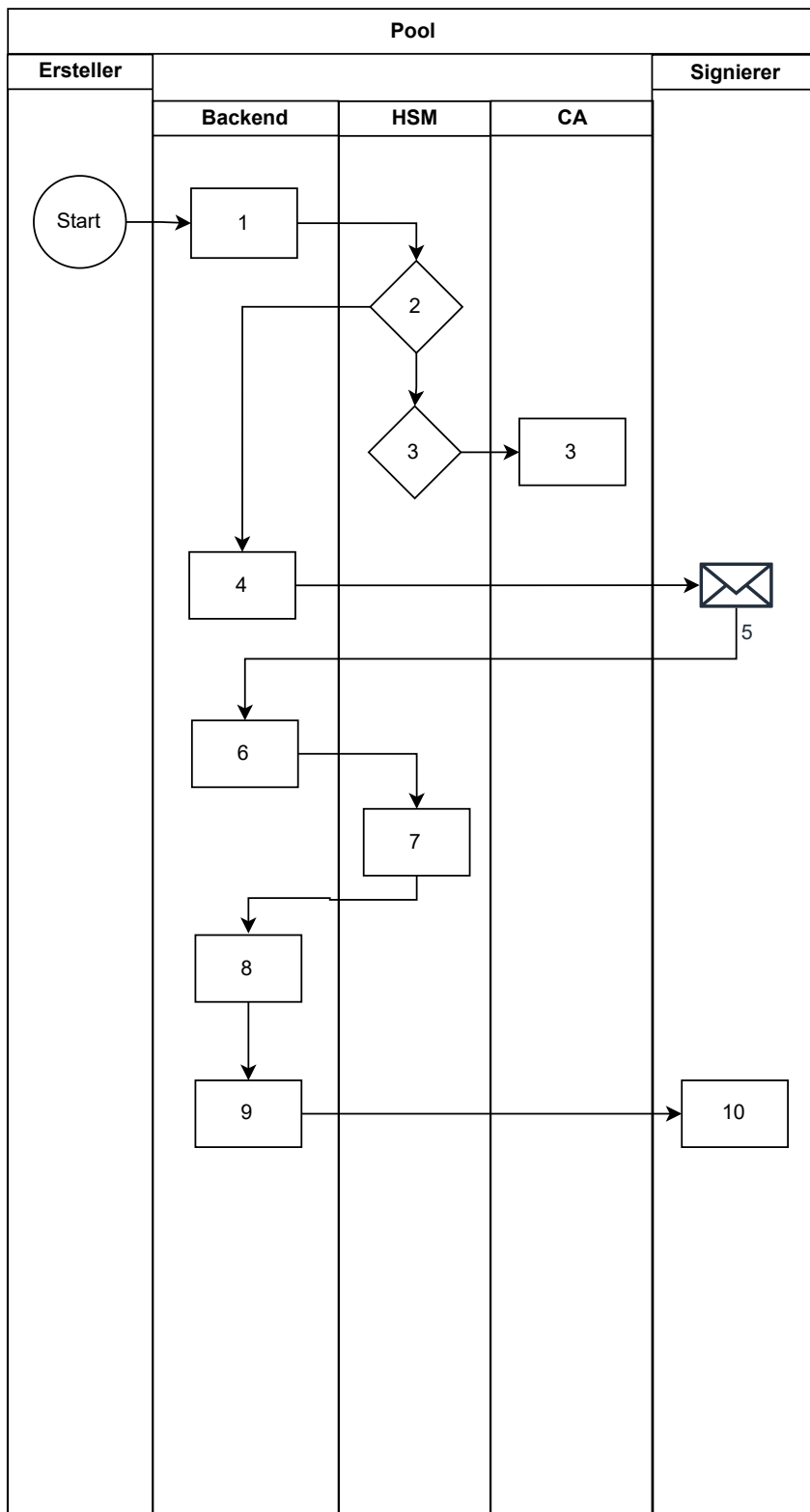




1. Der Ersteller lädt das Dokument hoch und legt die Empfänger fest (Diese sind identifiziert durch E-Mail Adresse und Mobilnummer - für die zwei Faktor Authentifizierung).

2. Ist ein gültiges Unternehmenszertifikat vorhanden, so ist dieses im HSM gespeichert. Zusätzlich zu diesem Zertifikat hat das HSM ein Unternehmensschlüsselpaar bestehend aus privatem und öffentlichem Schlüssel erzeugt und zu diesem Zertifikat abgelegt. Mit diesen drei Komponenten können beliebig viele Signaturen von beliebig vielen Signierern erzeugt werden. Für das Unternehmen ist eine User-Pin vergeben worden.

3. Existiert kein gültiges Unternehmenszertifikat so muß dieses rechtzeitig (mind. drei Monate vor Ablauf) beim CA beantragt werden. Erfolgt die Beantragung nicht rechtzeitig, so muß eine erneute Unternehmensüberprüfung durch den CA erfolgen.

4. Dem Signierer wird eine E-Mail, mit dem Hinweis, dass ein neues Dokument zum signieren vorliegt inkl. link, versendet.

5. Der Signierer benutzt den link. Er erhält einen Code per SMS zur Zwei Faktor Authentifizierung. Diesen gibt er ein und unterzeichnet das Dokument. Achtung! Das Dokument mit Unterschriftfeld ist noch keine elektronische Signatur. Diese erfolgt in den nächsten Schritten.

6. Im Backend wird der Hashwert des Dokumentes zum jeweiligen Signiervortschritt erzeugt. Dieser wird mit der User-Pin an das HSM übergeben.

7. Im HSM wird aus diesem Hashwert und dem privaten Schlüssel die digitale Signatur erzeugt. Diese wird mit dem hinterlegtem Zertifikat an das Backend zurückgegeben.

8. Das Backend fügt die digitale Signatur und das Zertifikat in die PDF-Datei ein. Werden die Unternehmenskomponenten verwendet, ist das Zertifikat für alle Signierer identisch. Für alle Signierer wird auch das Firmenschlüsselpaar verwendet. Um die Signierer zu identifizieren wird für alle Signierer ein Audit-Trail erzeugt. Dieses beinhaltet folgende Werte:

- **Identitätsdaten:** Vorname, Nachname und E-Mail-Adresse des Unterzeichners.
- **2FA-Nachweis:** Die Mobilnummer sowie der Nachweis, dass der OTP (One-Time-Password)-Code erfolgreich eingegeben wurde (inkl. Zeitstempel des Versands und der Verifizierung).
- **Technische Marker:** Die IP-Adresse des Unterzeichners und der verwendete Browser/Gerätetyp (User-Agent).
- **Eindeutige IDs:** Eine eindeutige Vorgangs- oder Transaktions-ID vom Signflow.
- **Zeitstempel:** Exakte Datums- und Uhrzeitangaben (idealerweise über einen qualifizierten Zeitstempeldienst/TSA gekoppelt). den Zeitstempel-Token (Base64/ASN.1), den Zeitstempeldienst (Name, Zertifikat) und den Signaturzeitpunkt (UTC) für jeden Schritt (Dokument aufgerufen, SMS gesendet, SMS bestätigt, Siegel aufgebracht).
- **Hash Werte:** Einen cryptographischen Hash des (signierten) Dokuments und die Angaben zum verwendeten Hash-Algorithmus (z.B. SHA-256). Diese Prozedur wird für alle Signierer durchgeführt. Am Ende werden die Audit-Trails aller Signierer als separate Seite(n) am Ende des Dokumentes angehängt.

9. Das von allen Signieren unterzeichnete Dokument wird rechtssicher archiviert.

10. Jeder Signierer erhält eine Kopie des von allen Signierern unterzeichneten Dokumentes.