Skribble: Digitale Signaturen clever und rechtsgültig meistern

Category: Online-Marketing
geschrieben von Tobias Hager | 11. Februar 2026



Skribble: Digitale Signaturen clever und rechtsgültig meistern

Du willst digitale Signaturen nutzen, ohne dich durch ein juristisches Minenfeld zu kämpfen oder in der Tech-Hölle zu landen? Willkommen bei Skribble – der Lösung für alle, die Verträge digital unterschreiben wollen, ohne sich dabei die Finger zu verbrennen. Aber Achtung: Nur weil eine Unterschrift digital aussieht, heißt das nicht, dass sie auch rechtsgültig

ist. In diesem Artikel zerlegen wir die digitale Signatur in ihre Einzelteile, zeigen dir, warum Skribble mehr kann als PDF mit Kritzelei, und wie du das Ganze rechtssicher, compliant und effizient in deine Prozesse integrierst. Spoiler: Wer 2025 noch mit Word-Dokumenten und Dropbox hantiert, hat das Memo verpasst.

- Was eine digitale Signatur wirklich ist – und was sie von einer elektronischen Unterschrift unterscheidet
- Warum PDF unterschreiben nicht gleich rechtsgültige Signatur bedeutet
- Wie Skribble funktioniert – und warum es die eIDAS-Verordnung ernst nimmt
- Die drei Signatur-Level: Einfache, fortgeschrittene und qualifizierte elektronische Signatur
- Wie du Skribble in bestehende Workflows und Tools integrierst
- Welche rechtlichen Standards Skribble erfüllt – national und international
- API, WebApp, Plug-ins: Wie du Skribble technisch implementierst
- Warum Datenschutz und Hosting-Lokation über deinen Vertragsabschluss entscheiden können
- Für wen sich Skribble eignet – von Startups bis Konzernjuristen
- Ein kritischer Blick: Wo Skribble glänzt – und wo noch Luft nach oben ist

Digitale Signatur vs. elektronische Unterschrift: Wo liegt der Unterschied?

Bevor wir in das Thema Skribble eintauchen, müssen wir eine Sache klarstellen: Eine digitale Signatur ist nicht einfach nur eine Unterschrift mit dem Finger auf einem PDF. Das mag fancy aussehen, hat aber in den meisten Fällen die rechtliche Durchschlagskraft einer Post-it-Notiz. Der Begriff “digitale Signatur” wird oft inflationär gebraucht – und genau das führt zu Missverständnissen, die im schlimmsten Fall Verträge ungültig machen.

Rechtlich korrekt unterscheidet man zwischen der einfachen elektronischen Signatur (EES), der fortgeschrittenen elektronischen Signatur (FES) und der qualifizierten elektronischen Signatur (QES). Diese Unterscheidung ist keine juristische Haarspalterei, sondern fest in der eIDAS-Verordnung der EU verankert. Und nur die QES hat die gleiche Wirkung wie eine handschriftliche Unterschrift. Wer also denkt, ein PDF mit einer eingescannten Signatur sei “rechtsgültig”, lebt in einer rechtlichen Parallelwelt.

Die digitale Signatur im technischen Sinn basiert auf kryptografischen Verfahren. Sie nutzt asymmetrische Verschlüsselung, bei der ein privater Schlüssel zum Signieren und ein öffentlicher Schlüssel zum Verifizieren verwendet wird. Damit wird sichergestellt, dass das Dokument nach der Signatur nicht verändert wurde – ein zentraler Punkt für rechtliche Verbindlichkeit.

Die eIDAS-Verordnung definiert präzise, welche Voraussetzungen für die unterschiedlichen Signatur-Level erfüllt sein müssen. Und hier kommt Skribble ins Spiel – ein Anbieter, der diese Komplexität im Backend abwickelt, während du im Frontend einfach "Unterschreiben" klickst. Klingt simpel? Ist es auch – wenn du weißt, was du tust.

Wie Skribble digitale Signaturen rechtssicher umsetzt

Skribble ist keine simple PDF-Signatur-Lösung, sondern ein Signaturdienst, der die Anforderungen der eIDAS-Verordnung technisch und rechtlich korrekt umsetzt. Die Plattform bietet alle drei Signatur-Level – EES, FES und QES – und ermöglicht damit eine flexible Anpassung je nach Use Case. Ob NDA, Arbeitsvertrag oder Millionen-Deal: Skribble kann das juristisch abfedern.

Das Herzstück von Skribble ist die Einbindung qualifizierter Vertrauensdiensteanbieter (Trust Service Provider, kurz TSP). Diese übernehmen die Identitätsprüfung und stellen die qualifizierten Zertifikate aus, die für eine QES notwendig sind. Skribble selbst agiert als Vermittler und UI-Schicht, die den komplexen Backend-Prozess benutzerfreundlich verpackt. Du bekommst also Rechtsgültigkeit ohne juristische Bauchschmerzen.

Die Identifizierung erfolgt bei Skribble über verschiedene Verfahren: Video-Ident, eID, SwissID oder sogar persönlich vor Ort. Je nach Land und gesetzlichem Rahmen kannst du das passende Verfahren wählen. Die Signatur erfolgt dann per Zwei-Faktor-Authentifizierung – in der Regel per SMS-TAN oder App-basierter Bestätigung.

Technisch basiert Skribble auf einem API-First-Ansatz. Das bedeutet: Du kannst die Signaturprozesse direkt in deine bestehenden Systeme – ob CRM, ERP oder DMS – integrieren. Es gibt eine WebApp für Einzelanwender, eine REST-API für Entwickler und Plug-ins für Tools wie Microsoft Teams oder SharePoint. Damit wird die Signatur Teil deines Workflows – nicht ein nerviges Extra.

Die drei Signatur-Level erklärt: EES, FES und QES

Wer mit digitalen Signaturen arbeitet, muss verstehen, welches Signatur-Level für welchen Anwendungsfall passt. Denn nicht jede Signatur ist gleich viel wert – weder rechtlich noch technisch. Hier die Übersicht:

- Einfache elektronische Signatur (EES): Die niedrigste Stufe. Ein Klick auf "Ich akzeptiere" oder eine Unterschrift mit dem Finger auf dem Tablet reicht. Rechtlich kaum belastbar, aber für interne Freigaben oder

informelle Kommunikation ausreichend.
- Fortgeschrittene elektronische Signatur (FES): Verknüpft die Signatur eindeutig mit dem Unterzeichner. Authentifizierung ist erforderlich, und die Integrität des Dokuments muss gewährleistet sein. Ideal für NDAs, interne Verträge oder HR-Dokumente.
- Qualifizierte elektronische Signatur (QES): Die Königsklasse. Entspricht rechtlich der handschriftlichen Unterschrift. Erfordert Identifizierung über einen TSP und Zwei-Faktor-Authentifizierung. Pflicht bei vielen Behördenvorgängen, Bankverträgen oder Immobiliengeschäften.

Mit Skribble kannst du flexibel zwischen diesen Signatur-Leveln wählen – abhängig vom rechtlichen Risiko und der Komplexität des Dokuments. Unternehmen, die regelmäßig mit Verträgen arbeiten, sollten klare Guidelines definieren, wann welches Level eingesetzt wird. Spoiler: Die QES ist nicht immer notwendig – aber wenn du sie brauchst, dann besser richtig.

Technische Integration: Skribble API, Plug-ins und Automatisierung

Skribble glänzt dort, wo viele Anbieter scheitern: bei der technischen Integration. Die REST-API ermöglicht eine vollständige Automatisierung von Signaturprozessen – vom Upload über die Identifizierung bis zur Archivierung des unterschriebenen Dokuments. Entwickler finden ausführliche API-Dokumentationen, SDKs und Sandbox-Zugänge. Das spart nicht nur Zeit, sondern auch Nerven.

Für weniger technische Teams gibt es Plug-ins für Microsoft Teams, SharePoint und diverse DMS-Systeme. Auch Zapier-Workflows sind möglich, wodurch Skribble leicht in bestehende Automatisierungsprozesse eingebunden werden kann. Das bedeutet: Outlook-Mail mit Vertrag landet automatisch in Skribble, wird signiert, archiviert und im CRM gespeichert – ohne manuelles Eingreifen.

Die WebApp richtet sich an Einzelanwender oder kleine Teams. Hier kannst du Dokumente hochladen, Empfänger definieren und das Signatur-Level festlegen. Die intuitive UI sorgt dafür, dass auch Juristen ohne Tech-Hintergrund sofort loslegen können. Und falls doch Fragen auftauchen: Der Support ist erreichbar und tatsächlich kompetent – was in SaaS-Land nicht selbstverständlich ist.

Auch das Thema Hosting ist bei Skribble durchdacht. Der Dienst hostet in der Schweiz, erfüllt die DSGVO und bietet optional auch Hosting in der EU. Das ist besonders für Konzerne mit Compliance-Anforderungen ein echter Pluspunkt – und ein Grund, warum Skribble auch bei Banken, Versicherungen und Kanzleien im Einsatz ist.

Rechtliche Konformität: eIDAS, ZertES und mehr

Die eIDAS-Verordnung ist die rechtliche Grundlage für elektronische Signaturen in der EU. Sie definiert, was eine qualifizierte Signatur ist, wie sie erstellt werden muss und welche Anbieter als “qualifiziert” gelten. Skribble erfüllt diese Anforderungen – in Zusammenarbeit mit zertifizierten TSPs wie Swisscom Trust Services oder A-Trust.

Für Anwender in der Schweiz gilt zusätzlich das ZertES-Gesetz, das ähnlich wie eIDAS funktioniert, aber nationale Anforderungen ergänzt. Skribble ist auch hier konform und stellt sicher, dass Signaturen sowohl in der EU als auch in der Schweiz rechtlich gültig sind. Für internationale Unternehmen ist diese Dualität ein entscheidender Vorteil.

Ein häufiger Irrtum: Nur weil ein Anbieter Signaturen “digital” nennt, heißt das nicht, dass sie eIDAS-konform sind. Viele Tools – darunter auch große Namen – bieten lediglich EES- oder bestenfalls FES-Level an, ohne rechtliche Absicherung. Skribble hingegen geht den kompletten Weg bis zur QES – inklusive Identitätsprüfung, Audit-Trail und Zertifikatmanagement.

Die Plattform dokumentiert jede Signatur mit einem vollständigen Audit-Log, speichert die Signaturzertifikate revisionssicher und stellt sicher, dass alle Prozesse den Anforderungen von ISO 27001 und DSGVO entsprechen. Das macht Skribble nicht nur rechtskonform, sondern auch revisionssicher – ein Muss für regulierte Branchen.

Fazit: Skribble als Gamechanger für digitale Vertragsprozesse

Wenn du 2025 noch Verträge ausdruckst, unterschreibst, einscannst und per E-Mail zurückschickst, bist du nicht oldschool – du bist ineffizient. Digitale Signaturen sind längst Standard, aber nur dann rechtsgültig, wenn sie korrekt umgesetzt werden. Skribble liefert genau das: eine Plattform, die technische Exzellenz mit juristischer Wasserdichtigkeit kombiniert. Nicht mehr, nicht weniger.

Ob du Start-up bist, das schnell skalieren will, oder Konzern mit umfangreichen Compliance-Anforderungen – Skribble passt sich an. Die Plattform ist robust, flexibel, integrationsfähig und tatsächlich einfach zu bedienen. Und das Beste: Sie macht Schluss mit dem Chaos aus PDF-Anhängen, Scans und Office-Workarounds. Wer heute noch analog unterschreibt, hat den digitalen Wandel verschlafen. Wer Skribble nutzt, ist einen Schritt voraus.