

Anbietervergleich für elektronische Signaturen

Auf dem Markt der elektronischen Signaturen gibt es mittlerweile viele Anbieter. In der nachfolgenden Tabelle finden Sie eine Übersicht über einen Teil der Anbieter. Die Darstellung fokussiert sich auf den wesentlichen Anwendungsfall, die elektronische Signatur durch eine physische Person.

Anbieter	Land	Server	oP ¹	EUTL	Verifikation ²	eIDAS	A/A ³
Adobe Sign	US					SES, AES, QES	-/x
d.velop	DE	EU		Sign8, D-Trust, Swisscom, A-Trust	via TSPs	SES, AES, QES	-/x
D-Trust	DE	DE	x ⁴	D-Trust (DE)		QES	x/x
DocuSign	US		x ⁵	DocuSign France (FR)	x	SES, AES, QES, electronic Seal	-/x
Moxis	AT	EU(AT)	x		x	SES, AES, QES	-/x
Paperless Postident	DE	DE				SES, AES, QES	-/x
Sign	DE					QES	x/-
Sign2x	US					QES	-/x
Sign2x	DE	DE	x	Sign8	via TSPs	SES, AES, QES, electronic Seal	-/x
YouSign	FR	FR		Yousign (FR)	x	SES, AES, QES, electronic Seal	x/x

¹ on Premise; ² Verifikation von physischen Personen; ³ App/API; ⁴ portiQ, sign-me-API; ⁵ DocuSign Security Appliance

Ein Blick auf die Spalte eIDAS zeigt, dass alle gelisteten Anbieter eine „Qualified Electronic Signature“ anbieten, wobei manche sich auf diese Funktionalität beschränken, da es die einzige Variante ist, die als juristisch zugelassener Ersatz einer physischen Unterschrift gilt.

Wenn es um die Verifikation der elektronischen Unterschrift geht ist nicht jeder Anbieter zuvorkommend und stellt die notwendige Information auf der Webseite zur Verfügung. Manche der Anbieter, wie DocuSign oder Yousign, haben eine eigene Verifikationsfunktion, die mit ihrem eigenen EUTL-TSP verknüpft ist, während andere, wie d.velop oder Sign2x, die Verifikation über die TSPs abwickeln, mit denen sie zusammenarbeiten.

An dieser Stelle sei darauf hingewiesen, dass EUTL die Interoperabilität auf Vertrauensebene erleichtert, die technische Integration der QTSPs bleibt jedoch anbieterspezifisch.

Sign2x kann in Verbindung mit dem passenden Identitätsprovider und deren QTSP auch Prozesse unterstützen, die auf GWG-Konformität ausgerichtet sind. Die Identifizierung erfolgt dabei über geprüfte Verfahren des Identitätsproviders, während die elektronische Signatur über den angebundenen Qualified Trust Service Provider abgesichert wird.

Damit lassen sich digitale Abschlussstrecken realisieren, bei denen Identitätsprüfung, Nachweisführung und Signaturprozess medienbruchfrei zusammengeführt werden. Je nach fachlicher und regulatorischer Anforderung können so Prozesse für einfache, fortgeschrittene oder qualifizierte elektronische Signaturen umgesetzt werden.

Sign2x schafft damit die technische Grundlage, um vertrauenswürdige digitale Signaturprozesse auch in regulierten Anwendungsfällen einzusetzen. Die konkrete GWG-Konformität hängt dabei vom eingesetzten Identitätsverfahren, dem Identitätsprovider und der fachlichen Ausgestaltung des Gesamtprozesses ab.

Viele der Anbieter geben an, dass ihre Server in der EU stehen bzw. geben das Land explizit an. Für die Anbieter aus den US wird entweder keine Angabe gemacht (Adobe, Sign) oder es wird darauf hingewiesen, dass man einen EUTL-Server in Frankreich betreibt, ohne anzumerken, dass der Cloud-Act die DSGVO aushebeln kann.

Wenn es darum geht, dass die angestrebte Lösung „on Premise“ laufen soll/muss, stehen deutlich weniger Anbieter zur Verfügung. Für die beiden Anbieter D-Trust und DocuSign ist das nur machbar für einen Teil Ihrer jeweiligen Lösungen: portiQ & sign-me-API (D-Trust) bzw. DocuSign Security Appliance (DocuSign). Für Moxis und Sign2x sind keine Einschränkungen für den „on Premise“-Betrieb angegeben.

Sind die Randbedingungen, dass der Server in der EU stehen muss und die DSGVO nicht umgangen werden kann, bei gleichzeitigem Betreiben der Lösung „on Premise“, bleiben nur die Anbieter D-Trust, Moxis & Sign2x zur Auswahl. Und wenn es um die volle Datensouveränität geht, dann bleibt nur Sign2x als Lösung.