



Merkblatt

Qualifizierte elektronische Signatur (QES)

Gemäss Art. 14 Abs. 2^{bis} OR sind qualifizierte elektronische Signaturen (QES) nach dem Bundesgesetz vom 18. März 2016 über die elektronische Signatur ([ZertES](#)), die auf einem qualifizierten Zertifikat beruhen und mit einem elektronischen Zeitstempel verbunden sind, der eigenhändigen Unterschrift gleichgestellt.

Einfache elektronische Signaturen (EES) und fortgeschrittene elektronische Signaturen (FES) hingegen sind der eigenhändigen Unterschrift **nicht** gleichgestellt.

Dieses Merkblatt richtet sich an Anwältinnen und Anwälte.

1 Was ist eine QES?

Diese elektronische Signatur ist ein technisches Verfahren zur Überprüfung

- der Echtheit eines Dokuments, einer elektronischen Nachricht oder anderer elektronischer Daten sowie
- der Identität der oder des Unterzeichnenden.

Sie basiert auf einer Infrastruktur, die von den Anbietenden von Zertifizierungsdiensten betrieben wird. Die Schweizerische Akkreditierungsstelle SAS veröffentlicht eine [Liste der anerkannten Anbietenden von Zertifizierungsdiensten](#).

Gemäss Art. 2 lit. c und e ZertES ist die QES eine fortgeschrittene elektronische Signatur, die

- unter Verwendung einer sicheren Signaturerstellungseinheit erstellt wurde,
- auf einem geregelten, auf eine natürliche Person ausgestellten und
- zum Zeitpunkt der Erzeugung der elektronischen Signatur gültigen **qualifizierten** Zertifikat beruht.

Mit der Anbringung der QES wird die Datei gleichzeitig mit einem qualifizierten elektronischen Zeitstempel versehen. Dieser Zeitstempel ist unabänderlich.

2 Wie erhalte ich eine QES?

Um eine QES zu erstellen, werden folgende Komponenten benötigt:

- ein qualifiziertes Zertifikat,
- eine Dienstleistung und/oder Software, die mit diesem Zertifikat eine QES herstellt (sog. elektronische Signaturerstellungseinheit) und
- eine Verbindung zu einem zertifizierten online Zeitstempeldienst.

Für die Erstellung von QES existieren unterschiedliche Lösungen:

Erstellungstyp	Wo befindet sich das Zertifikat?	Wo wird die zu signierende Datei bearbeitet?
Zertifikat lokal / Signatur lokal	Im physischen Besitz des Unterzeichnenden (z.B. Chipkarte)	Lokal auf dem Computer des Unterzeichnenden
Zertifikat bei Dritten / Signatur lokal	Auf dem Server eines Dritten	Lokal auf dem Computer oder im Computer-Netzwerk des Unterzeichnenden
Cloudservice	Auf dem Server eines Dritten	Die Datei wird auf den Server eines Dritten hochgeladen, dort mit einer Signatur versehen und wieder heruntergeladen

Signaturlösungen, welche lokal signieren, jedoch das Zertifikat bei einem Dritten speichern, können in zwei Kategorien unterteilt werden:

- betriebsfertige Lösungen ohne Netzwerkintegration bzw. kundenspezifische Anpassungen
- Lösungen, die eine Netzwerkintegration und/oder weitere kundenspezifische Anpassungen voraussetzen

In vielen Fällen muss die Vertraulichkeit von Dokumenten gewahrt werden. Der Inhalt des zu unterschreibenden Dokuments oder darin enthaltene sensible Informationen werden bei der Anbringung der Signatur in der lokalen Umgebung – im Gegensatz zu Cloudlösungen – nicht an Dritte offengelegt.

3 Was ändert sich mit dem Inkrafttreten des BEKJ?

Mit dem vollständigen Inkrafttreten des Bundesgesetzes vom 20. Dezember 2024 über die Plattformen für die elektronische Kommunikation in der Justiz ([BEKJ](#)) **fällt** für Anwältinnen und Anwälte sowie andere natürliche und juristische Personen **die Anforderung der QES für Dokumente weg**, die via die Plattform justitia.swiss ausgetauscht werden. *«An Stelle der Unterschriften tritt die Authentifizierung gegenüber der Plattform [justitia.swiss] sowie das automatisierte Anbringen von geregelten elektronischen Siegeln.»¹*

Das bedeutet, dass Anwältinnen und Anwälte ab diesem Zeitpunkt für Eingaben, die sie über die Plattform justitia.swiss an Justizbehörden einreichen, **keine QES mehr benötigen**.

Allgemein ist zu prüfen, in welcher Form und über welche Kanäle Eingaben an Behörden zu richten sind, die nicht in den Anwendungsbereich des BEKJ fallen.

4 Wie überprüfe ich die Gültigkeit von QES bzw. elektronische Eingaben?

Die Gültigkeit einer QES bzw. einer elektronischen Eingabe können mittels dem vom Bund zur Verfügung gestellten [eGov Signaturvalidator](#) überprüft werden. Der eGov Signaturvalidator überprüft ein elektronisch signiertes Dokument hinsichtlich

- Authentizität (ist das Dokument gültig elektronisch signiert worden?) und
- Integrität (ist das Dokument nach seiner Signatur inhaltlich verändert worden?).

Dokumentiert werden die Ergebnisse der Prüfung durch den eGov Signaturvalidator in einem sogenannten "Prüfbericht für elektronische Signaturen", der auch (im .pdf-Format) heruntergeladen bzw. gedruckt werden kann.²

Der eGov Signaturvalidator kann von Privaten gegenwärtig nicht in der lokalen Umgebung betrieben werden. Treffen Sie also geeignete Vorkehrungen hinsichtlich des Berufsgeheimnisses, falls Sie ihn für Daten verwenden, die dem Berufsgeheimnis unterliegen.

5 Welche Hinweise gibt es für Anwältinnen und Anwälte?

- Erkundigen Sie sich sorgfältig, bevor Sie eine QES einrichten. Tauschen Sie sich mit Berufskolleginnen und -kollegen aus. Konsultieren Sie auch die zu diesem Thema auf den Webseiten des Schweizerischen Anwaltsverbands und der kantonalen Anwaltsverbände publizierten Informationen.
- Treffen Sie geeignete Vorkehrungen hinsichtlich des Berufsgeheimnisses, falls Sie zur Erstellung von QES eine Cloudlösung und den eGov Signaturvalidator verwenden.

¹ [BBl 2023 679](#), Ziffer 4.1.1 (Seite besucht am 21.10.2025)

² Mehr Informationen zum eGov Signaturvalidator unter: [Signature Validator - Anleitung zum Validator](#) (Seite besucht am 21.10.2025).

Falls die Fristwahrung bei elektronischen Eingaben von der Erstellung einer validen QES abhängt: Treffen Sie Vorkehrungen für den Fall, dass die Erstellung einer QES temporär nicht möglich ist (z.B. Zeitpuffer vor Fristablauf). Es gibt zahlreiche Konstellationen, die dazu führen können, dass eine QES (vorübergehend) nicht erstellt werden kann, unter anderem:

- Ablauf des Ausweispapiers, auf dessen Basis das Zertifikat ausgestellt wurde
- Wechsel oder Verlust des Autorisierungsmittels (Smartphone)
- Nichtverfügbarkeit der Dienste von Dritten (z.B. Zeitstempeldienst, Infrastruktur Zertifikatsanbieter)
- Revozierung oder Ablauf des Zertifikats
- Nichtverfügbarkeit der Signatur-Software
- Ausfall der Internetverbindung

Weiterführende Informationen

Weiterführende Informationen und Informationen zu verwandten Themen erhalten Sie via: info@justitia.swiss und/oder auf der Webseite www.justitia40.ch

Dieses Merkblatt wurde in Zusammenarbeit mit dem Schweizerischen Anwaltsverband (SAV) und auf Grundlage der vom Bernischen Anwaltsverband (BAV) erstellten Merkblätter (<https://www.bav-aab.ch/de/digitalisierung-justitia-4.0.html>) erarbeitet.