eSignR
according to swiss/eu laws

Whitepaper

Die digitale Signatur: «Ein Enabler der digitalen Transformation»

Administrative Prozesse im Homeoffice

In der Zeit des Corona-bedingten Lockdowns wurden sich viele Unternehmen schmerzlich bewusst, dass ihre administrativen Abläufe gar nicht oder nur partiell digitalisiert sind. Wer im Homeoffice sitzt und Zugriff auf relevante Dokumente braucht, wäre froh um eine elektronische Ablage. Doch die elektronische Ablage allein reicht nicht, wenn es darum geht mit Kunden und Geschäftspartnern Verträge zu unterzeichnen.

Sehr viele Unternehmen setzen noch immer auf die Handunterschrift bei relevanten Dokumenten wie Verträgen. Wenn die Unterschriftsregelung im Unternehmen in gewissen Fällen keine Einzelunterschriften vorsieht, wird die Unterschriftenrunde im Homeoffice ein mühseliges Unterfangen. Akzeptiert beispielsweise eine der Vertragsparteien keine Faksimile-Unterschriften (Scan der Handunterschrift), müssen zwar elektronisch vorhandenen Dokumente ausgedruckt, von Hand unterschrieben und auf dem Postweg zirkuliert werden. Dies ist bei der aktuellen Auslastung der Post ein zeitaufwändiger Prozess.

Die digitale Signatur ist ein Faktor, der die digitale Transformation der administrativen Prozesse vereinfachen und beschleunigen kann.

Was ist die digitale Signatur?

Die elektronische Signatur ist ein kryptografisches (also mathematisches) Verfahren, das ermöglicht, die nicht abstreitbare Urheberschaft und die Integrität eines Dokumentes zu prüfen. Das Verfahren funktioniert mit einem Schlüsselpaar. Einem geheimen Signaturschlüssels (Private Key) und einem öffentlichen Verifikationsschlüssels (Public Key). Der Urheber eines Dokumentes signiert das Dokument mit seinem geheimen Signaturschlüssel. Dabei wird ein Wert errechnet (die digitale Signatur), den der Empfänger des Dokumentes mit dem öffentlichen Verifikationsschlüssels des Urhebers überprüfen kann. Die Zuordnung eines bestimmten Schlüsselpaares zu einer konkreten Person erfolgt durch ein sogenanntes digitales Zertifikat. Über das Zertifikat kann somit eine vorhandene Signatur zweifelsfrei einer Person zugeordnet werden. Ein signiertes Dokument kann nachträglich nicht mehr verändert werden, ohne dass die Signatur seine Gültigkeit verliert.

Die Stellung der digitalen Signatur im Gesetz

Das schweizerische Bundesgesetz über die elektronische Signatur (ZertES) regelt, wie die Signatur- und Verifikationsschlüssel von vertrauenswürdigen Dritten eingesetzt und verwaltet werden müssen. Diese sogenannten Anbieterinnen von Zertifizierungsdiensten müssen sich gemäss ZertES anerkennen lassen, damit deren Produkte die gewünschte rechtliche Wirkung entfalten.

Die von den Anbieterinnen von Zertifizierungsdiensten ausgestellten Schlüsselpaare können verwendet werden, um sogenannte qualifizierte elektronische Signaturen auf Dokumenten anzubringen. Solche Signaturen sind gemäss Obligationenrecht (OR Art. 14 Abs. $^{2\,bis}$) der Handunterschrift gleichgestellt.

Im grenzübergreifenden Geschäftsverkehr muss berücksichtigt werden, dass es aktuell keine gegenseitigen Anerkennungen digitaler Signaturen zwischen der Schweiz, der EU und anderen Staaten gibt. Ein Vertrag sollte in diesem Fall sinnvollerweise digitale Signaturen des Landes tragen, dessen Recht angewendet wird und wo der Gerichtsstand ist.

Was brauche ich für eine digitale Signatur?

Um digital zu signieren brauche ich:

1) Ein von einer anerkannten Anbieterin von Zertifizierungsdiensten ausgestelltes Zertifikat (also ein Schlüsselpaar).

2) Eine Software, um Dokumente in das PDF-Format umzuwandeln.

3) Eine Signaturssoftware, um ein PDF-Dokument mit meinem geheimen Signaturschlüssel zu signieren.

In der Schweiz gibt es fünf anerkannte Anbieterinnen von Zertifizierungsdiensten. Es sind dies Swisscom, QuoVadis, SwissSign, Swiss Government PKI (Anbieterin von Zertifizierungsdiensten für die Bundesverwaltung) und UBS (die Bank!).

Für das Publikum stellen im Augenblick nur Swisscom und QuoVadis Zertifikate aus. Digitale Signaturen werden im Regelfall auf Dokumenten angebracht, die im PDF-Format, dem «digitalen Papier», vorliegen.

Die Swisscom bietet momentan nur Zertifikate in Verbindung mit eigenen Signaturdiensten an. Wie beispielsweise Skribble (www.skribble.com). Da diese Software aber voraussetzt, dass Dokumente für das Anbringen der Signatur hochgeladen werden müssen, ist die Verwendung für vertrauliche Dokumente für viele vermutlich ein No-Go.

Wie kann ich die Signatur auf einem Dokument prüfen?

Ob ein signiertes Dokument «gültig» ist, kann nicht allein durch die Prüfung kryptographischer Eigenschaften beantwortet werden. Es muss vielmehr der Kontext des Dokumentes miteinbezogen werden:

- Ein signierter Vertrag zwischen zwei Unternehmen ist nur dann gültig, wenn alle darauf angebrachten Signaturen gemäss Gesetz der Handunterschrift gleichgestellt sind. Zudem müssen die unterzeichnenden Personen gemäss Handelsregistereintrag für die Unternehmen zeichnungsberechtigt sein und gemäss Unterschriftenregelung (Einzelunterschrift, Unterschrift zu zweien) signiert haben.

- Ein digitaler Strafregisterauszug ist nur dann gültig, wenn die einzige darauf angebrachte Signatur die der Handunterschrift gleichgestellte Signatur des Verantwortlichen des Strafregisters ist.

- Eine elektronische Urkunde ist nur dann gültig, wenn sie eine der Handunterschrift gleichgestellte Signatur einer gemäss Gesetz zur Ausstellung von Urkunden ermächtigen Person trägt, also etwa eines Notars.

Da Signaturen vor allem auf PDF-Dokumenten angebracht werden, haben die PDF-Betrachter verschiedener Hersteller entsprechende Funktionen für die Überprüfung von Signaturen implementiert.

Beispiele dafür sind etwa Adobe Acrobat Reader oder Foxit Reader. All diese Programme sind zwar in der Lage, die kryptographischen (also mathematischen) Prüfungen der Signaturen durchzuführen, scheitern aber daran, die oben aufgeführten Aspekte zu berücksichtigen.

Um nicht nur die kryptographische, sondern auch die kontextbasierte Prüfung der Signaturen durchzuführen, haben wir im Auftrag vom Bund, den Signaturvalidator (www.validator.ch) entwickelt. Der Validator unterstützt die Prüfung von Signaturen, da er in der Lage ist, den Kontext miteinzubeziehen. Der Validator ist eine Webanwendung, in die man das zu prüfende Dokument hochladen muss.

Für vertrauliche Dokumente ist dies aber für viele vermutlich ein No-Go. Aus diesem Grund bietet die von uns entwickelte rechtsgültige Signatursoftware *Open eGov LocalSigner* die Möglichkeit Signaturen «diskret» zu prüfen, dass heisst User müssen Dokumente nicht bei einem Cloud-Anbieter hochladen.

Ab dem Q1 2021 wird ein brandneuer *LocalSigner* ***«eSignR»*** verfügbar sein. Bis der *eSignR* jedoch fertig entwickelt ist, empfehlen wir die von uns im Auftrag der Bundesverwaltung entwickelte Signatursoftware *Open eGov LocalSigner* zu benutzen. *LocalSigner* wird kostenfrei für Windows, macOS und Linux angeboten und kann hier heruntergeladen werden: ***www.openegov.ch/localsigner***

Mehr Infos zum eSignR unter: ***www.esignr.ch***