

Geschäfte elektronisch und rechtssicher abwickeln

Felix Lämmler, Dipl. El. Ing. FH/EMBA

Der rechtssichere und medienbruchfreie Austausch elektronischer Dokumente ist ein zentrales Bedürfnis im privaten wie im geschäftlichen Alltag. Die Lösung liegt auf der Hand: qualifizierte digitale Signaturen. Sie sind im Obligationenrecht verbrieft und rechtlich der eigenhändigen Unterschrift gleichgestellt.

Damit Dokumente in elektronischer Form sicher sind, müssen drei Anforderungen erfüllt sein: Erstens müssen die Integrität des Dokuments garantiert und alle nicht autorisierten Änderungen im Dokument durch den Anwender ersichtlich sein. Zweitens müssen die Verbindlichkeit und die Nachvollziehbarkeit sichergestellt bleiben, damit die Echtheit des Dokuments nicht abgestritten werden kann. Drittens muss die Vertraulichkeit gewährleistet sein, das heisst, das Dokument ist vor unbeabsichtigter oder missbräuchlicher Veröffentlichung zu schützen. Die signierten Dokumente werden zudem mit einem Zeitstempel versehen, der exakt festhält, wann ein Dokument signiert wurde.

Diese Sicherheitsstufen sorgen dafür, dass der Absender seine Signatur nicht bestreiten und der Empfänger gleichzeitig mögliche Veränderungen unmittelbar erkennen kann. Grundlage dieser Technologie sind qualifizierte digitale Zertifikate. Sie erfüllen die hohen Ansprüche einer digitalen Signatur und sind beweissicher.

Qualifizierte Zertifikate sind weltweit gültig und werden ausschliesslich durch Zertifizierungsanbieter ausgestellt. Damit ist gewährleistet, dass die Zertifikate von vertrauenswürdigen Unternehmen auf einer sicheren Infrastruktur erstellt werden. Für die Verwaltung der Zertifikate über ihren Lebenszyklus von wenigen Jahren hinweg ist eine Public Key Infrastructure (PKI) erforderlich. Diese sorgt für die Ausstellung, Erneuerung oder Aufhebung der Zertifikate sowie für die Überprüfung der Gültigkeit durch den Empfänger. Die PKI muss nicht selbst beschafft und betrieben werden, preiswerte Produkte integrieren sich einfach in bestehende Informatiklösungen und erleichtern die Anwendung direkt am Arbeitsplatz. Erforderlich sind ein PC, eine Signatursoftware und ggf. ein geeignetes «Trägermedium». Das Zertifikat selbst lässt sich sicher ablegen, da der Zugriff darauf nur via ein zusätzliches Kennwort möglich ist.



Management & Technology

Durch den geschickten Einsatz von digitalen Signaturen lassen sich viele private und öffentliche Ausweisfunktionen problemlos mit qualifizierten Zertifikaten kombinieren, beispielsweise mit Hilfe der elektronischen Identitätskarte (eID), der elektronischen Patienten- oder Versicherungskarte oder als eindeutiges Identifikationsmittel für den sicheren Zugang zu privaten oder unternehmensspezifischen Informatikdiensten oder -anwendungen. Die Nachfrage nach und das Angebot an nutzbaren Diensten ist indessen weit grösser, wie die aktuelle Praxis in der EU oder in den EWR-Ländern zeigt: Von der Speicherung medizinischer Notfall- oder biometrischer Daten bis zu konkreten Amtshandlungen wie etwa der Bestellung und Erstellung von amtlichen Ausweisen. Ebenso wird der tägliche E-Mail-Verkehr durch eine exakte Identifikation des Absenders für den Empfänger sicherer respektive: erst vertrauenswürdig.

Mit der elektronischen Signatur können Unternehmen wie Private medienbruchfrei arbeiten. Was bisher auf Papier erledigt und abgelegt wurde, lässt sich heute gleichwertig elektronisch vollziehen. Der elektronische Absender wird zum eindeutig identifizierbaren Vertragspartner, und alle Rechtsgeschäfte lassen sich verbindlich durchführen. Damit eröffnen sich neue Geschäftsmodelle: der elektronische Briefkasten oder der elektronische Zustelldienst, der ohne Zeitverlust, ortsunabhängig und zu sehr attraktiven Preisen die gewünschte Dienstleistung verrichtet, steht im Arbeitszimmer bereit. Wirtschaft wie Verwaltung haben das Potenzial erkannt. Wir beraten Sie gerne.