Oliver Berndt, Leiter des Competence Centers Elektronische Signatur beim VOI: „Über die elektronische Signatur sind rein elektronische Prozesse ohne Sicherheitsverlust machbar."

Elektronische Signatur: Marktentwicklung und Hindernisse

Den Schrecken verloren

Ungeklärte rechtliche, organisatorische und technische Fragen haben früher zu allerlei Vorurteilen gegenüber der elektronischen Signatur geführt und den breiteren Einsatz verzögert. Heute ist der Austausch elektronischer Rechnungen eines der wichtigsten Anwendungsfelder der elektronischen Signatur. Und wie Oliver Berndt, beim VOI Leiter des „Competence Centers Elektronische Signatur", versichert, ist die E-Signatur inzwischen auch nicht mehr generell kompliziert und teuer.

Die Beschaffung via Internet ist ein Bereich mit starkem Wachstum. Sobald jedoch bestimmte Wertgrenzen überschritten werden, erfolgt die finale Bestellung und Rechnungsstellung über Papier und Unterschrift, weil sich die Lieferanten damit sicherer fühlen. Genauso ist es bei anderen sensiblen Vorgängen wie z. B. langfristigen Vereinbarungen mit Banken oder Versicherungen. Auch unternehmensinterne Prozesse wie die Freigabe einer Konstruktionszeichnung, einer Produktionsumstellung oder einer Bauabnahme sind mit erheblichen finanziellen Risiken versehen. Es ist somit wichtig, dass die Dokumente nach der finalen Abstimmung nicht verändert wurden (Integrität) und dass die Verantwortlichen eindeutig identifizierbar sind (Authentizität). Außerdem muss der Vorgang auch noch Jahre später nachvollziehbar sein.

Immer dann kommen Papier und Unterschriften zum Einsatz, obwohl dieses Medium in großer Menge in den Unternehmen erhebliche Handling-Kosten verursacht. Deshalb wurde bereits vor vielen Jahren die elektronische Signatur erfunden. Zunächst gab es jedoch vielfältige rechtliche, organisatorische und technische Fragen ohne verbindliche Antworten, die zu allerlei Vorurteilen gegenüber der E-Signatur führten und den breiteren Einsatz stark verzögerten. Dies hat sich jedoch in den letzten Jahren geändert. Unterschiedliche Entwicklungen haben dazu beigetragen:

- **Klare Vorgaben des Gesetzgebers** für bestimmte Anwendungsfälle, z. B. qualifzierte Signatur als Pflicht bzw. Voraussetzung in einer Reihe von Anwendungsfällen (elektronische Rechnungen, Scannen von Abrechnungsunterlagen bei Krankenkassen, Notareinreichung bei Amtsgerichten, Datenaustausch zwischen Unternehmen und Behörden sowie Behörden untereinander, Prozesse im Gesundheitswesen u. a.)
- **Nutzung biometrischer Varianten**, um an das geläufige Verfahren des Unterschreibens anknüpfen und dennoch sichere, elektronische Prozesse umsetzen zu können. Auch hier erfolgt die Sicherstellung der Integrität durch Verschlüsselung von Prüfsummen (Hash-Wert).
- Beantwortung von diversen **rechtlichen Fragen** und **Lösung von technischen Interoperabilitätsproblemen** zwischen den Komponenten verschiedener Hersteller.
- Die Möglichkeit, **Signaturerstellung und -verifikation an einen Dienstleister zu delegieren** ohne Einschränkungen beim Beweiswert (bei ordnungsgemäßer Prozessgestaltung).

Wenn man teilweise auch über die Sinnhaftigkeit einzelner Vorgaben streiten kann, so hat dies doch zu einer zunehmenden Verbreitung der Technologie geführt und gezeigt, dass die praktische Anwendung lange nicht so kompliziert ist, wie zum Teil auch heute noch behauptet wird. Kaum bekannt ist, dass bei Software-Entwicklung oder Datenkommunikation Zertifikate und Signaturen schon lange gang und gäbe sind, ohne dass es lange Diskussionen brauchte. Auch die „Grabenkämpfe" zwischen verschiedenen Signaturformen sind einer pragmatischen Sichtweise gewichen. Heute lässt sich sagen:

1. Wenn für den anvisierten Anwendungsfall ein Gesetz eine qualifizierte Signatur vorschreibt oder die zivilrechtliche Gleichstellung zur traditionellen Unterschrift zwingend ist, dann muss die qualifizierte Signatur eingesetzt werden.
2. Wenn 1. nicht zutrifft und es sich um einen Prozess mit direktem Konsumentenkontakt handelt, bietet sich die biometrische Variante an, weil Konsumenten auf absehbare Zeit kaum Smartcards/Reader haben werden.
3. Wenn 1. nicht zutrifft und es sich um einen rein internen Prozess handelt oder die Telekommunikation mit externen Partnern gesichert werden soll, können – abhängig vom benötigten Beweiswert – alle Signaturformen inklusive Software-Zertifikate und Biometrie zum Einsatz kommen. *(www.voi.de)*