Papierlos beglaubigen, Teil III

Die qualifizierte elektronische Signatur

Während in der Privatwirtschaft die fortgeschrittene elektronische Signatur (vorgestellt in Teil I und II dieser Reihe) eine adäquate Alternative zur eigenhändigen Unterschrift auf Papier darstellt, fordern Behörden, Notare oder Gerichte oft eine qualifizierte Signatur (QES) Oliver Clanget erläutert, wie man diese erstellt.

Eine Unterschrift ist eine Unterschrift ist eine Unterschrift – zumindest auf dem Papier. Ein wenig anders sieht es bei den elektronischen Unterschriftsformen aus. Für die wurden im Signaturgesetz aus dem Jahr 2001 gleich drei verschiedene Arten definiert:

- die (einfache) elektronische Signatur,
- die fortgeschrittene elektronische Signatur und
- die qualifizierte elektronische Signatur.

Ein Blick auf die wesentlichen Unterschiede der drei Verfahren macht deutlich, warum der Gesetzgeber mehrere Formen elektronischer Signaturen unterscheidet und welche Art für welchen Zweck geeignet ist.

Die einfache elektronische Signatur

Paragraph 2 Nr. 1 des Signaturgesetzes definiert eine elektronische Signatur als „*elektronische Daten, die anderen elektronischen Daten beigefügt oder logisch mit ihnen verknüpft sind und die zur Authentifizierung dienen*“. Das ist zunächst nichts Besonderes: Jeder, der schon einmal den eigenen Namen unter eine E-Mail getippt hat, hat damit einer Menge von elektronischen Daten – nämlich seiner Nachricht – weitere elektronische Daten beigefügt, nämlich seinen Vor- und Nachnamen unter der Nachricht. Diese Art der Signatur wird für gewöhnlich gar nicht als richtige Unterschrift von uns wahrgenommen, da sowohl die Signatur als auch die Nachricht selbst ohne Weiteres von jedermann gefälscht bzw. geändert werden können.

Die fortgeschrittene elektronische Signatur

Die in § 2 Nr. 2 des Signaturgesetzes definierte „fortgeschrittene elektronische Signatur“ hingegen bietet bereits einige Sicherheit: Zunächst muss sie mit einem „Signaturschlüssel“ erstellt werden. Außerdem muss sie u.a. „*ausschließlich dem Signaturschlüssel-Inhaber zugeordnet*“ werden können und darüberhinaus mit dem Text „*so verknüpft [sein], dass eine nachträgliche Veränderung der Daten erkannt werden kann*“.

Der erwähnte Signaturschlüssel ist nichts anderes als eine Zeichenfolge, ähnlich einem Kennwort oder einer PIN, nur um einiges länger. Wendet man den Schlüssel auf die Daten an, die man signieren möchte, erhält man wiederum eine neue Zeichenfolge – die Signatur.

Diese Signatur ist für jedes Dokument und jeden Signaturschlüssel individuell, so dass man im Nachhinein sicher nachweisen kann, ob eine empfangene Datei mit einem bestimmten Schlüssel signiert wurde. Eine Datei, die mit einem Signaturschlüssel unterschrieben wurde, kann somit nach dem Signieren nicht mehr verändert werden (s. auch Kasten “Hintergrund” rechts).

Ein Verfahren zum Erstellen fortgeschrittener Signaturen mit Adobe Acrobat wurde in MDÜ Heft 5/11 ausführlich beschrieben. In vielen Fällen ist diese Art der Signatur ausreichend. Zudem ist das Verfahren unkompliziert: Sobald man sich ein Schlüsselpaar generiert hat, kann man sofort Dateien mit einer fortgeschrittenen elektronischen Signatur unterschreiben.

Wer sowieso, wie wohl viele Kollegen, über eine Acrobat-Vollversion verfügt, muss zudem keine zusätzlichen Kosten auf sich nehmen.Die fortgeschrittene elektronische Signatur hat jedoch auch ihre Grenzen. Der große Nach-

Hintergrund

Wie funktionieren Signaturschlüssel?

Unterschreiben

Ein stark vereinfachtes Beispiel: Alice möchte die Nachricht „Kino“ an Bob versenden. Damit Bob sicher sein kann, dass die Nachricht von Alice stammt, signiert Alice die Nachricht zuvor. Sie benutzt zum Signieren immer ihren Signaturschlüssel, z.B. „1234“.

Zunächst einmal wandelt Sie Ihre Nachricht in Zahlen um (a=1, b=2, ...), aus „K i n o“ wird also „11 9 14 15“. Nun nimmt sie von jeder der vier Zahlen die Quersumme und erhält damit die Zahl 2956, eine einfache Variante eines sogenannten Hashwertes der Originalnachricht.

Diesen kombiniert sie nun mit ihrem Schlüssel – der Einfachheit halber sagen wir, sie addiert beide Zahlen: 2956 + 1234 = 4190. Die Signatur für diese Nachricht wäre dann die Zahl 4190. Alice sendet also an Bob die signierte Nachricht „Kino 4190“.

Unterschrift prüfen

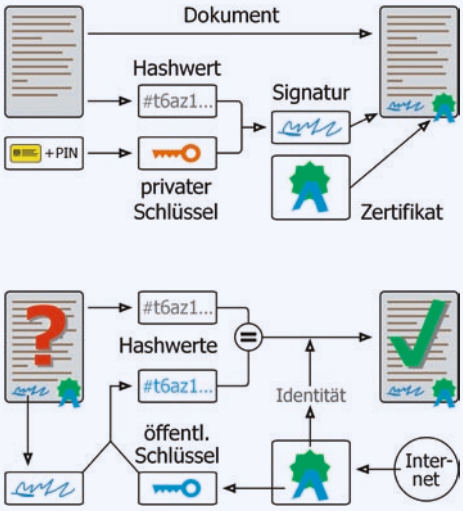
Bob möchte nun überprüfen, ob die Nachricht tatsächlich so von Alice gesendet wurde. Da er Alice kennt, weiß er, dass sie mit dem Schlüssel „1234“ unterschreibt.

Er geht also jetzt den umgekehrten Weg und errechnet sich aus der Signatur den Hashwert, den die von Alice signierte Nachricht gehabt haben muss: 4190 - 1234 = 2956. Außerdem errechnet er sich den Hashwert, der sich aus der empfangenen Nachricht ergibt: K i n o → 11 9 14 15 → 2956.

Wenn er auf beiden Wegen denselben Wert erhält, kann er sicher sein, dass die Nachricht von Alice stammt und auch von niemandem nachträglich verändert wurde.

Nur der Schlüsselinhaber kann signieren.

Die tatsächlichen mathematischen Verfahren sind selbstverständlich aufwändiger. Vor allem aber werden Hashwert und Schlüssel nicht einfach addiert, sondern durch eine sogenannte Einwegfunktion miteinander verknüpft – ein Verfahren, das praktisch nicht mehr umkehrbar ist. Auch ist der Schlüssel wesentlich



länger, so dass es nicht mehr oder nur mit unverhältnismäßigem Aufwand möglich ist, den Schlüssel zu errechnen oder durch Probieren eine gültige Signatur ohne Kenntnis des Schlüssels zu erstellen.

Das im Beispiel vereinfacht beschriebene Verfahren hätte so allerdings noch einen großen Nachteil: Bob, der den Schlüssel von Alice ja kennen muss, um die Signatur zu überprüfen, könnte mit diesem Schlüssel natürlich auch selbst Nachrichten signieren, die dann von Alices Nachrichten nicht zu unterscheiden wären.

Dieses Problem löst man durch sogenannte asymmetrische Signierverfahren. Asymmetrisch deshalb, weil zum Erstellen und Überprüfen nicht ein und derselbe Schlüssel benötigt wird. Man benutzt stattdessen ein Paar aus zwei zusammengehörigen, jedoch verschiedenen Schlüsseln: Der Unterzeichner verfügt über einen privaten, nur ihm bekannten Signaturschlüssel, mit dem er seine Signaturen erstellt; der andere Teil des Schlüsselpaars ist ein öffentlicher Schlüssel, mit dem es nicht möglich ist, Daten zu signieren, wohl aber kann mit ihm die Echtheit der mit dem geheimen Schlüssel erstellten Signatur überprüft werden.

Ein Empfänger kann also die Echtheit der Signatur leicht überprüfen, sofern er den öffentlichen Schlüssel des Unterzeichners kennt. Damit kommt die Signatur der eigenhändigen Unterschrift auf Papier recht nahe: Wer weiß, wie die Unterschrift einer Person aussieht, kann zwar leicht die Echtheit der Unterschrift feststellen, er kann sie aber nicht ohne Weiteres kopieren.

teil des unkomplizierten Verfahren ist, dass die reale Identität des Schlüsselpaar-Inhabers nicht gesichert ist, solange man nicht auf sicherem Wege aus einer vertrauenswürdigen Quelle den entsprechenden öffentlichen Schlüssel zum Überprüfen der Signaturen eines Unterzeichners erhalten hat.

Konkret heißt das, dass der Unterzeichner beispielsweise seinen öffentlichen Schlüssel auf der eigenen Website angeben müsste. Erst mit dieser Zusatzinformation könnte dann der Empfänger sicher sein, dass die empfangene signierte Datei auch wirklich von dem angegebenen Unterzeichner stammt – vorausgesetzt, er ist sich sicher, dass die Website auch wirklich echt ist.

Das Problem der fortgeschrittenen elektronischen Signatur ist also, dass sie, für sich genommen, keine Aussage über die wirkliche Identität des Unterzeichners erlaubt. Genau diese Schwachstelle wird mit der aufwändigeren, qualifizierten elektronischen Signatur beseitigt.

Die qualifizierte elektronische Signatur (QES): Unterschrift mit Ausweis-Charakter

Für die qualifizierte elektronische Signatur werden die Anforderungen, die für die fortgeschrittene Signatur gelten, um zwei Merkmale erweitert: Sie muss gemäß § 2 Nr. 3 SigG zusätzlich *„auf einem [...] qualifzierten Zertifikat beruhen und [...] mit einer sicheren Signaturerstellungseinheit erzeugt werden“*.

Der entscheidende Unterschied ist hier das „qualifzierte Zertifikat“: eine Bescheinigung, ausgestellt von einer vertrauenswürdigen Stelle, dass der betreffende öffentliche Schlüssel tatsächlich der angegebenen Person gehört. Der Zertifikataussteller überprüft dazu die Identität der Person, die von ihm ein Schlüsselpaar zum Signieren elektronischer Daten erhält.

Die geforderte „sichere Signaturerstellungseinheit“ besteht im Normalfall aus einem Kartenlesegerät und einer Chipkarte und einer dazu zugehörenden PIN. Durch Eingabe der PIN am Kartenlesegerät wird auf dem Chip der Karte die Signatur erzeugt und dann erst an den Computer gesendet. Der private Schlüssel verlässt somit also nie die Karte und ist auf diese Weise zusätzlich gegen Ausspionieren geschützt.

Das Zertifikat, das für die qualifizierte Signatur benötig wird, hat jedoch noch einen Vorteil – zumindest für einige Berufsgruppen, so zum Beispiel beeidigte bzw. ermächtige Übersetzer: In das Zertifikat können Informationen über eine regulierte Berufsbezeichnung eingetragen werden. Somit kann man sich durch die qualifizierte Signatur gleichzeitig als Urkundenübersetzer ausweisen.

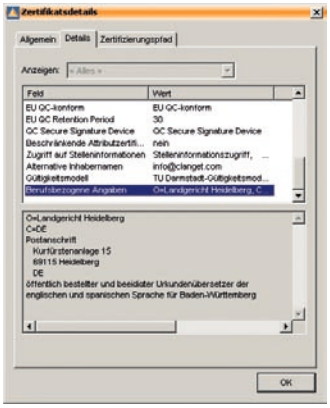
Eine qualifizierte elektronische Signatur erstellen – so geht's:

1: Erwerb eines Zertifikats

Als erstes benötigen Sie ein Zertifikat in Form einer Signaturkarte. Unternehmen, die solche Zertifikate ausstellen, müssen ihre Tätigkeit bei der Bundesnetzagentur anzeigen und werden von dieser überwacht. Mittlerweile gibt es in Deutschland recht kostengünstig Signaturkarten von verschiedenen Anbietern, meist im Set mit dem nötigen Kartenleser. Eine aktuelle Liste findet sich auf der Website der Bundesnetzagentur (bundesnetzagentur.de). Drei große Anbieter sind die Bundesdruckerei (D-Trust), die Sparkassen (S-Trust) und die Deutsche Post (Signtrust). Die Kosten für die Anschaffung belaufen sich bei den meisten Anbietern auf rund 150 EUR, hinzu kommt eine jährliche Zertifikatsgebühr von etwa 50 EUR.

Um eine Signaturkarte zu bekommen, füllen Sie auf der Website des Ausstellers einen Antrag aus, den Sie dann ausdrucken und per Post versenden. Außerdem müssen Sie mit einem Formular zur Identitätsüberprüfung zu einer angegebenen Stelle (Notar, Postident o.ä.) und sich dort mit Ihrem Personalausweis oder Reisepass ausweisen.

Falls Sie sich Ihre Beeidigung bzw. Ermächtigung in das Zertifikat eintragen lassen möchten, füllen Sie das entsprechende Feld „berufsbezogenes Attribut“ aus (maximal 120 Zeichen, Leerzeichen mitgezählt, Umlaute und „ß“ zählen aus technischen Gründen doppelt). Klären Sie am besten im Vorfeld mit dem Landgericht, wie die Bezeichnung genau einzutragen ist. Der Zertifikataussteller sendet dann ein Formular zur Bestätigung an das zuständige Landgericht. Es ist sinnvoll, bei Ihrem Antrag schon einen Ansprechpartner des Gerichts anzugeben, am besten informieren Sie diesen schon vorher, da die Bestätigungsprozedur für die meisten Gerichte Neuland ist.



Nach der Bestätigung Ihrer Identität und der Berufsbezeichnung erhalten Sie nach einigen Tagen per Post Chipkarte, PIN, Software und Lesegerät. Nach Installation und PIN-Aktivierung können Sie Ihre erste qualifizierte Signatur erstellen.

2. Erstellen von PDF-Dateien mit qualifzierter Signatur

Die gängigen Signierprogramme bieten meist mehrere Möglichkeiten, Dateien zu signieren. Zum einen gibt es Plugins für gängige Tools wie MS Word oder Adobe Acrobat; einige Anwendungen wie OpenOffice bieten zudem eigene, kompatible Signierfunktionen.

Ein universeller und zudem einfacherer Weg ist das Erstellen und Signieren über einen virtuellen Drucker. Bei der Installation der Signiersoftware OpenLiMiT unter Windows wird beispielsweise gleich auch ein virtueller Drucker installiert, der unter dem Namen „OpenLiMiT PDF-Producer" in der Druckerauswahl aller Programme erscheint. Sie können also aus jeder Anwendung ein PDF erstellen und dieses dann mit der Signiersoftware elektronisch unterschreiben. Dazu stecken Sie einfach Ihre Signaturkarte in den Kartenleser und geben über die Tastatur des Kartenlesers Ihre PIN ein. Der Kartenleser generiert damit die Signatur und bettet diese in die PDF-Datei ein. Jetzt müssen Sie die signierte Datei nur noch speichern; der ganze Vorgang dauert weniger als eine Minute.

Die qualifizierte elektronische Signatur ersetzt zwar vollständig die eigenhändige Unterschrift, dennoch ist es ratsam, einmal die eigene Unterschrift und den Stempelabdruck einzuscannen und immer unter den Übersetzungen einzufügen, bevor man diese elektronisch signiert.

Achten Sie außerdem beim Signieren darauf, dass Ihr „berufsbezogenes Attribut" in die Signatur eingeschlossen (mitsigniert) wird und dass eine in das PDF eingebettete Signatur erstellt wird und keine separate Signaturdatei.

3. Überprüfen von qualifizierten Signaturen

Zum Überprüfen der qualifzierten Signatur gibt es etliche kostenlose Programme; der Vorgang ist unkompliziert und die Bedienung selbsterklärend. Man öffnet die zu prüfende Datei in einem Validierungsprogramm, klickt gegebenenfalls noch auf einen Button – und das Ergebnis wird angezeigt.

Die Überprüfung mit dem Adobe Reader ist leider nicht immer erfolgreich, hauptsächlich, weil zwar die Signatur, nicht aber das Zertifikat überprüft wird. Behörden, Notare und Gerichte werden sich davon wohl nicht verwirren lassen, da auch sie schon elektronische Dokumente ausstellen und verwalten – auf der Grundlage der qualifizierten elektronischen Signatur. Private Empfänger hingegen könnten bei Fehlermeldungen in Adobe Reader – trotz gültiger qualifizierter Signatur – allerdings misstrauisch werden. Insofern sollte man sich überlegen, ob man nicht einer elektronisch signierten Übersetzung gleich immer noch eine zusätzliche Seite im PDF mit Informationen und Links zu Validierungssoftware anfügt.

Fazit

Fortgeschrittene und qualifizierte elektronische Signaturen beruhen auf demselben Prinzip eines Schlüsselpaars aus privatem und öffentlichen Schlüssel. Die fortgeschrittene elektronische Signatur ist kostengünstig, ohne Registrierung schnell verfügbar und für viele Zwecke ausreichend. Die qualifizierte Signatur ist zwar aufwändiger, erlaubt jedoch durch das Zertifikat und den jederzeit online abrufbaren öffentlichen Schlüssel einen sicheren Rückschluss auf die Identität des Unterzeichners.

Es kommt auf den Einzelfall an, welche Signatur als Ersatz für die eigenhändige Unterschrift zu wählen ist. Für die Vorlage von elektronischen Dokumenten bei Behörden, Notaren und Gerichten ergibt sich jedoch oft aus Verwaltungsvorschriften zwingend die Notwendigkeit, eine qualifizierte Signatur einzusetzen. Wo die Schriftform gesetzlich vorgeschrieben ist, kann nach § 126a BGB nur die qualifzierte elektronische Signatur an deren Stelle treten. In einigen Dolmetschergesetzen (z.B. Bayern, Schleswig-Holstein) ist zudem explizit geregelt, dass eine beglaubigte Übersetzung, wenn sie elektronisch ausgestellt wird, mit einer qualifizierten Signatur zu versehen ist.

Weblinks

Qualifizierte Signatur: de.wikipedia.org/wiki/QES
Signaturgesetz: www.dejure.org/gesetze/SigG
Bundesnetzagentur: www.bundesnetzagentur.de

Zertifikatanbieter (sog. Trustcenter)

Liste mit Zertifikatanbietern: nrca-ds.de/ZDAliste.htm
Signtrust (Deutsche Post): www.signtrust.de
S-Trust (Sparkassen): www.s-trust.de
D-Trust (Bundesdruckerei): www.d-trust.net/index.php

Software zum Überprüfen elektronischer Signaturen

OpenLiMiT Reader – www.openlimit.com
Secrypt digiSeal Reader – www.secrypt.de
Sign Live! CC validation client – www.intarsys.de

Oliver Clanget

Oliver Clanget hat deutsche, englische und spanische Sprach- und Literaturwissenschaft (Gymnasiallehramt) an der Universität Heidelberg studiert. Er ist staatlich geprüfter Übersetzer und in Baden-Württemberg für die Sprachen Englisch und Spanisch öffentlich bestellt und beeidigt. Seit 2007 ist er als freiberuflicher Technischer Übersetzer und Urkundenübersetzer in Heidelberg tätig. info@clanget.com