Die zertifizierte Signatur im praktischen Einsatz

VON
10.5.2004 | Ratgeber - Internetrecht, Computerrecht

Mehr zum Thema: Internetrecht, Computerrecht Rubrik, Elektronische, Signatur, E-Mail, Schriftform

Authentizität und Integrität

Grundlage der elektronischen Signatur ist die Verschlüsselungstechnologie. Ganz wichtig für die folgenden Gedanken ist die Trennung des zertifizierten Signierungsverfahrens von der Verschlüsselungstechnologie. Signieren und Verschlüsseln von E-Mails sind zwei voneinander unabhängige Verfahren, die zwar sinngemäß sehr eng verknüpft sind, jedoch unterschiedliche Zwecke verfolgen. Es sei bemerkt, dass im Bereich der elektronischen Signaturen zwischen den asymmetrischen und symmetrischen kryptografischen Verfahren unterschieden wird, ohne hier weitere Einzelheiten ausführen zu wollen. Dienste wie Pretty Good Privacy (PGP) oder GNUPG (Open Source Software) verwenden seit Jahren erfolgreich das asymmetrische kryptografische Verfahren zur Verschlüsselung von E-Mails nebst Anlagen. Dabei wird die Nachricht vom Versender anhand eines dem Empfänger eindeutig zugewiesenen und öffentlich abrufbaren Schlüssels, dem (**public key**) verschlüsselt. Diese Nachricht kann dann vom Empfänger mit einem zweiten, dem privaten Schlüssel (**privat key**) entschlüsselt werden. Das Verfahren funktioniert auch in die entgegengesetzte Richtung, indem eine Nachricht mit dem privaten Schlüssel verschlüsselt und vom Empfänger mit dem öffentlichen Schlüssel des Absenders entschlüsselt wird.

Voraussetzung dafür, dass Kommunikationspartner Erklärungen austauschen können, ist lediglich, dass ein Schlüssel öffentlich über das World Wide Web auf einem Server zugänglich ist. Entscheidend ist in diesem Zusammenhang, dass es derzeit technisch ausgeschlossen ist, den privaten Schlüssel aus dem öffentlichen Schlüssel zu errechnen. Der private Schlüssel darf natürlich niemals versendet werden, weil genau dann die Gefahr des Missbrauchs bestünde. Bei den so eben beschriebenen Diensten handelt es sich um Angebote, die den Kommunikationspartnern in erster Linie Vertraulichkeit bieten. Mit **Vertraulichkeit** ist gemeint, dass es für Dritte ausgeschlossen sein soll, den Inhalt der ausgetauschten Daten zur Kenntnis zu bringen.

Vornehmlicher Sinn und Zweck der elektronischen Signatur im Sinne des Signaturgesetzes (SigG) ist es, **Authentizität und Integrität** zu gewährleisten. Der Empfänger einer E-Mail darf /kann/muss sich darauf verlassen können, dass eine signierte E-Mail mit dem empfangenen Inhalt genauso vom Absender abgegeben wurde, wie sie beim Empfänger angekommen ist. Wenn eine Datei oder eine E-Mail signiert werden soll, erzeugt die Hard- und Software aus den zu signierenden Daten den so genannten Hash-Wert. Der Hash-Wert ist als digitaler Fingerprint zu verstehen – ein praktisch einmaliger Wert. Aus dem Hash-Wert können die Daten nicht rekonstruiert werden. Werden die Daten nur geringfügig verändert, ändert sich auch der Hash-Wert. Sollen die Daten versendet werden, wird der errechnete Hash-Wert mit dem privaten – oder falls bekannt – mit dem öffentlichen Schlüssel des Empfängers asymmetrisch verschlüsselt und als Anlage an die elektronische Nachricht und den Daten angefügt. Selbstverständlich ist die Technik der elektronischen Signatur dazu in der Lage, die eigentlichen Daten und nicht nur den Hash-Wert „nebenbei“ zu verschlüsseln, um als Plus zu Authentizität und Integrität auch Vertraulichkeit zu erzeugen.

Jetzt Impressum erstellen

Seiten in diesem Artikel:

Diskutieren Sie diesen Artikel

Kommentar schreiben

Das könnte Sie auch interessieren

Gesetzgebung
Neues Signaturgesetz in Kraft