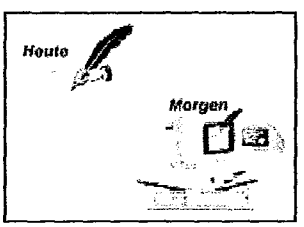
BSI-Kurzinformation

Elektronische Signatur

1. Einsatzgebiete und Anforderungen im Überblick



Elektronische Netze und Kommunikationswege ermöglichen es, Informationen über weite Strecken in kurzer Zeit auszutauschen. Dies umfasst auch rechtlich relevante Dokumente, wie z. B. Angebote, Bestellungen oder Rechnungen im **E-Business** oder Anträge und Bescheide im **E-Government**.
Dabei werden an die übertragenen Informationen zwei wesentliche Anforderungen gestellt: Erstens muss der Empfänger der Daten zweifelsfrei feststellen können, wer der Absender ist (Authentizität und Nichtabstreitbarkeit) und zweitens muss ausgeschlossen werden, dass die Daten durch die Beteiligten, oder durch Dritte unbemerkt manipuliert oder verfälscht werden können (Integrität).
Beide Anforderungen können durch den Einsatz der **elektronischen Signatur** erfüllt werden: Mit Hilfe von kryptographischen Verfahren macht die elektronische Signatur jede Manipulation oder Verfälschung an den Originaldaten für den Empfänger sofort erkennbar. Durch eine sichere Zuordnung der eingesetzten kryptographischen Schlüssel zum Kommunikationspartner lässt sich außerdem der Urheber einer signierten Nachricht zweifelsfrei feststellen. Weiterhin können elektronische Signaturen auch eingesetzt werden, um einen Zeitpunkt festzuhalten, zu dem die Daten in einer bestimmten Form vorgelegen haben (**Zeitstempel**). Diese Funktionen sind vor allem wichtig, wenn die elektronisch getätigten Transaktionen rechtlich verbindlich und damit beweisbar sein sollen. Für sichere Rechtsgeschäfte im Internet sind **elektronische Signaturen** also unverzichtbar. Für bestimmte Handlungen im elektronischen Rechtsverkehr können Formerfordernisse den Einsatz elektronischer Signaturen sogar verbindlich vorschreiben.
Elektronische Signaturen schützen nicht davor, dass Unbefugte Einblick in Daten erhalten. Bei vertraulichen Daten ist deshalb zusätzlich zur elektronischen Signatur eine Verschlüsselung erforderlich.

2. Signaturgesetz

Elektronische Signaturen können mit verschiedenen Verfahren auf unterschiedlichen Sicherheitsniveaus realisiert werden. Um hier eine Orientierung zu geben und um festlegen zu können, welchen Beweiswert elektronische Signaturen im konkreten Einzelfall haben, definiert in Deutschland das Signaturgesetz (SigG) [3] verschiedene Arten der elektronischen Signatur:

Abbildung 1: Arten der elektronischen Signatur

Einfache elektronische Signaturen (§ 2 Nr. 1 SigG) dienen dazu, den Urheber einer elektronischen Nachricht zu kennzeichnen, z. B. durch das Abspeichern einer eingescannten Unterschrift. Für einfache elektronische Signaturen sind keine Anforderungen bezüglich ihrer Sicherheit oder Fälschungssicherheit definiert, so dass diese Signaturen nur einen sehr geringen Beweiswert haben. Für besonders werthaltige Transaktionen kommen sie in aller Regel nicht in Frage.

Für **fortgeschrittene elektronische Signaturen** (§ 2 Nr. 2 SigG) gelten höhere Anforderungen: Sie müssen eine Manipulation der Daten erkennbar machen, sich eindeutig einer natürlichen Person zuordnen lassen, die Identifizierung dieser Person erlauben und es ermöglichen, dass nur diese Person die erforderlichen Mittel zur Signaturerzeugung unter ihrer alleinigen Kontrolle halten kann. Insofern verfügen fortgeschrittene elektronische Signaturen grundsätzlich über einen etwas höheren Beweiswert. Die tatsächliche Sicherheit einer fortgeschrittenen elektronischen Signatur hängt jedoch von den eingesetzten Signaturverfahren, den verwendeten Software- und Hardwarekomponenten und nicht zuletzt von der Sorgfalt der Anwender bei der Signaturerstellung ab. Im Streitfall muss der Anwender daher im Zweifel beweisen, dass die Signatur tatsächlich in diesem Sinne sicher erzeugt wurde.
Anders verhält sich dies bei der **qualifizierten elektronischen Signatur** (§ 2 Nr. 3 SigG), für deren Echtheit ein Anscheinsbeweis streitet. Bei dieser höchsten Sicherheitsstufe der elektronischen Signatur wird die Signatur ihrem Urheber über ein qualifiziertes Zertifikat (§ 2 Nr. 7 SigG) zugeordnet. Durch das qualifizierte Zertifikat, das von einem vertrauenswürdigen Zertifizierungsdiensteanbieter (§ 2 Nr. 8 SigG) (ZDA) signiert wird, wird die Zusammengehörigkeit zwischen dem öffentlich bekannten Signaturprüfschlüssel, der zur Prüfung der Signatur verwendet wird (vgl. Abschnitt 3), und der Identität des Signaturschlüsselinhabers belegt. Der Zertifizierungsdiensteanbieter garantiert, dass die Angaben im qualifizierten Zertifikat und die Auskünfte seiner Verzeichnis- und Zeitstempeldienste korrekt sind und er die Anforderungen gemäß Signaturgesetz und Signaturverordnung [4] erfüllt. Dazu gehört, dass der ZDA die sensiblen Zertifizierungsdienste in einer besonders geschützten Umgebung betreibt (Trust Center). Außerdem klärt der ZDA den Anwender über seine Sorgfaltspflichten im Umgang mit der Signatur auf. Zertifizierungsdiensteanbieter unterliegen der Aufsicht durch die Bundesnetzagentur (BNetzA) und müssen dort im Rahmen ihrer Betriebsaufnahme und Betriebsanzeige Nachweise, Belege und Erklärungen einschließlich eines Sicherheitskonzepts einreichen, die die Erfüllung der gesetzlichen Anforderungen gemäß Signaturgesetz und Signaturverordnung dokumentieren.
Qualifizierte elektronische Signaturen sind wegen ihres hohen Sicherheitsniveaus in der Regel der handschriftlichen Unterschrift gleichgestellt und können grundsätzlich im Rechtsverkehr ebenso wie diese eingesetzt werden. Sollten Zweifel an der Sicherheit einer qualifizierten elektronischen Signatur auftreten, kann eine Überprüfung anhand des bei der BNetzA hinterlegten Sicherheitskonzeptes Klarheit verschaffen. Zertifizierungsdiensteanbieter können eine solche Prüfung auch schon vor der Aufnahme des Betriebes, also insbesondere unabhängig von einem konkreten Streitfall, durchführen und sich dadurch akkreditieren lassen. Beim Einsatz einer qualifizierten elektronischen Signatur mit Anbieterakkreditierung besteht deshalb für die Anwender ein hohes Maß an Rechtssicherheit. Die aktuelle Liste der bestätigten Produkte für die Ausführung der qualifizierten Signatur und der Zertifizierungsdiensteanbieter mit Betriebsanzeige bzw. mit Anbieterakkreditierung kann auf derWebseite der BNetzA [2] eingesehen werden. Die Anforderungen an die verschiedenen Arten von Signaturen und an die Zertifizierungsdiensteanbieter sowie deren Anbieterakkreditierung sind im Signaturgesetz und in der Signaturverordnung geregelt.

3. Funktionsweise

Fortgeschrittene und qualifizierte elektronische Signaturen basieren heute auf Verfahren der asymmetrischen Kryptographie. Solche Verfahren verwenden ein Paar aus zwei zusammengehörigen kryptographischen Schlüsseln.

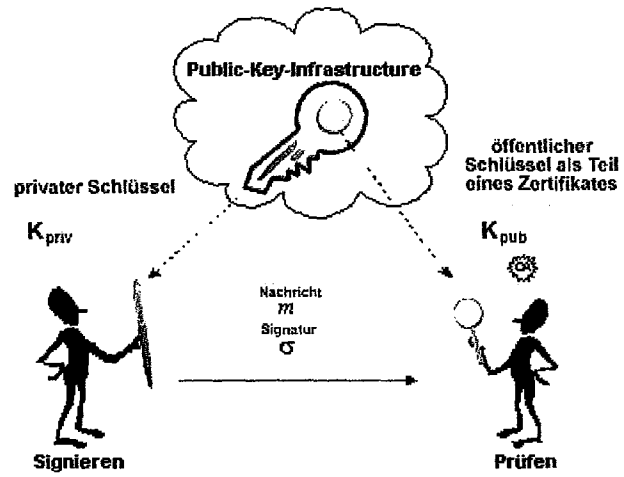


Abbildung 2: Signatursystem

Einer dieser Schlüssel wird als sogenannter **privater Schlüssel** (Kpriv) zur Signaturerzeugung verwendet und vom Signaturersteller geheim gehalten, so dass kein Unbefugter mit diesem Schlüssel Signaturen erstellen kann. Der andere Schlüssel wird als öffentlicher Schlüssel (Kpub) allen Kommunikationspartnern zur Verfügung gestellt und dient der Überprüfung der Signatur. Das kryptographische Verfahren stellt sicher, dass eine Signatur, die sich mit dem öffentlichen Schlüssel prüfen lässt, nur mit dem zugehörigen privaten Schlüssel erstellt worden sein kann und deshalb dem Inhaber dieses Schlüssel zugerechnet werden muss.
Die Veröffentlichung der **öffentlichen Schlüssel** aller Kommunikationspartner in einem telefonbuchartigen Verzeichnis und die Zuordnung dieser Schlüssel zu Personen übernimmt der Zertifizierungsdiensteanbieter. Dazu erhebt er die erforderlichen Daten und prüft die Identität des Schlüsselinhabers. Diese Daten werden dann für den Fall der qualifizierten elektronischen Signatur in einem qualifizierten Zertifikat (vgl. Abschnitt 2) mit dem öffentlichen Schlüssel verbunden, wobei diese Verknüpfung durch eine Signatur des Zertifizierungsdiensteanbieters vor Manipulationen geschützt ist. Das elektronische Zertifikat hat eine feste Gültigkeitsdauer und kann vom Schlüsselinhaber über eine Hotline gesperrt werden, wenn z. B. die sichere Verwahrung des zugehörigen privaten Schlüssels nicht mehr gegeben ist. Gesperrte Zertifikate werden im Verzeichnisdienst des Zertifizierungsdiensteanbieters gekennzeichnet. Die Gesamtheit der Systeme und Prozesse zur Ausgabe und Verwaltung der Zertifikate fasst man unter dem Begriff " Public-Key-Infrastruktur" zusammen.

4. Sicherheit

Qualifizierte elektronische Signaturen erfüllen eine Reihe von besonderen Sicherheitsanforderungen, die eine Fälschung solcher Signaturen mit den verfügbaren technischen Mitteln ausschließen.
Dies betrifft zunächst die eingesetzten kryptographischen Verfahren, deren Sicherheit laufend vom Bundesamt für Sicherheit in der Informationstechnik bewertet wird [1]. Für qualifizierte elektronische Signaturen dürfen nur solche Verfahren eingesetzt werden, die eine Manipulation oder Fälschung von Signaturen nach dem Stand der Technik ausschließen.
Ein weiteres wesentliches Sicherheitskriterium ist der Schutz des privaten Schlüssels. Damit dieser Schlüssel nicht in die Hände Dritter geraten kann, wird er bei qualifizierten elektronischen Signaturen in einer so genannten sicheren Signaturerstellungseinheit (§ 2 Nr. 10 SigG) – z. B. einer besonders gesicherten Chipkarte (vgl. Abbildung 3) – gespeichert, wo auch die Signaturerzeugung erfolgt. Der Chipkartenhersteller muss dabei in einem **Prüf- und Bestätigungsverfahren** nachweisen, dass ein Auslesen des Schlüssels aus der Chipkarte nicht möglich ist und dass der Signaturalgorithmus auf der Chipkarte sicher implementiert ist.

Auch für die Schlüsselerzeugung gelten entsprechende Auflagen an die dabei eingesetzten

Abbildung 3: Signaturerstellungseinheit

technischen Komponenten, damit keine Kopien des privaten Schlüssels angefertigt werden können.
Zertifizierungsdiensteanbieter, die qualifizierte Zertifikate ausgeben, müssen weitere hohe Sicherheitsanforderungen erfüllen, z. B. bei der persönlichen Identifizierung der Signaturschlüsselinhaber, durch den Einsatz zuverlässigen und geschulten Personals und durch die Sicherstellung der Erreichbarkeit ihres Verzeichnisdienstes. Beim Verlust der Karte oder bei anderen Sicherheitsvorfällen kann der Signaturanwender sein Zertifikat jederzeit – also rund um die Uhr – über eine Hotline sperren lassen. In einer gesetzlich vorgeschriebenen Unterrichtung werden die Signaturanwender über den richtigen Umgang mit der Chipkarte informiert.
Alle Sicherheitsmaßnahmen des Zertifizierungsdiensteanbieters müssen in einem **Sicherheitskonzept** dokumentiert und bewertet werden. Weil die Zertifizierungsdiensteanbieter bei qualifizierten Zertifikaten der Aufsicht durch die Bundesnetzagentur unterliegen, müssen sie ihr Sicherheitskonzept dort hinterlegen. Bei der freiwilligen Akkreditierung erfolgt außerdem eine unabhängige Prüfung des Sicherheitskonzeptes.
Die Aufbewahrungsfristen für die Antragsunterlagen, die elektronischen Daten und die Zertifikate liegen für angezeigte ZDA bei fünf und für akkreditierte ZDA bei 30 Jahren. Hierdurch wird die Nachprüfbarkeit elektronisch signierter Dokumente innerhalb üblicher Aufbewahrungsfristen sichergestellt. Durch die Nachsignatur von archivierten Dokumenten und Signaturen kann die Beweiskraft von qualifizierten elektronischen Signaturen auch längerfristig erhalten werden.

5. Anwendungsmöglichkeiten im Einzelnen

Die qualifizierte elektronische Signatur kann im Rechtsverkehr unter Privaten bereits seit dem Inkrafttreten von § 126a BGB im Jahre 2001 als **Äquivalent zur Schriftform** eingesetzt werden. Besondere Bedeutung erlangt sie jedoch im öffentlichen Bereich: Während im Privatrechtsverkehr der Grundsatz der Formfreiheit gilt, sieht das öffentliche Recht für Anträge und Bescheide regelmäßig die Schriftform vor, so dass insbesondere Anträge einer Unterschrift bedürfen. Hinzu kommt, dass bei der elektronischen Ausstellung von Bescheiden der Integrität des Inhalts wie auch der Authentizität des Ausstellers wegen der mit ihnen verbundenen Rechtswirkung eine besondere Bedeutung zukommt.
Ein erster Anwendungsbereich der qualifizierten elektronischen Signatur ist hierbei die elektronische Übermittlung von Rechnungen nach § 14 Absatz 3 UStG: Um der erhöhten Gefahr eines Umsatzsteuerbetruges durch leichtere Fälschbarkeit elektronischer Rechnungen entgegenzuwirken, berechtigen elektronisch ausgestellte Rechnungen einen Unternehmer nur dann zum Vorsteuerabzug, wenn sie mit einer qualifizierten elektronischen Signatur versehen sind.
Im Rahmen des ELSTER-Projekts [9] wurde durch die Entwicklung einer neuen Sicherheitsplattform für das Online-Portal (ElsterOnline) nunmehr auch die Möglichkeit geschaffen, Steuererklärungen sowie die seit 01.01.2005 grundsätzlich zwingend elektronisch abzugebenden Umsatz- und Lohnsteuervoranmeldungen mit einer elektronischen Signatur zu versehen.
Im elektronischen Rechtsverkehr innerhalb und mit Justizbehörden wurde durch das FormAnpG [6] vom 13.07.2001 zunächst die elektronische Form für Schriftsätze zugelassen. Durch das JKomG [7] vom 22.03.2005 ist nunmehr auch die Zustellung gerichtlicher Entscheidungen in elektronischer Form sowie die elektronische Aktenführung in der Justiz möglich. Weitere Anwendungsbereiche im behördlichen Umfeld sind beispielsweise das Rechnungswesen in derSozialversicherung, Patentanmeldungen beim DPMA sowie das Einwohnermeldewesen.

6. Interoperabilität

Zertifizierungsdienste für qualifizierte elektronische Signaturen werden am Markt von einer Reihe von Zertifizierungsdiensteanbietern (vgl. Abschnitt 2) angeboten. Dabei ist es natürlich wünschenswert, dass ein Signaturanwendungsprogramm mit den Chipkarten möglichst aller Anbieter zusammenarbeitet, damit die Anwender nicht für jede Anwendung eine eigene Chipkarte benötigen. Um dieses Ziel zu erreichen und gleichzeitig die Verbreitung von elektronischen Signaturen in der Praxis weiter zu fördern, wurde im Jahr 2003 das Signaturbündnis gegründet. Die Mitglieder des Signaturbündnisses, die sowohl private Anbieter als auch Behörden mit E-Government-Anwendungen umfassen, haben sich auf die Einhaltung gemeinsamer Standards zur Interoperabilität verpflichtet.

Eine zentrale Rolle nimmt dabei der Standard ISIS-MTT [5] ein, bei dem international anerkannte Standards zu eindeutigen Profilen für Zertifikate, Zertifizierungsdienste und Signaturformate zusammengefasst wurden.

7. Internationale Anerkennung

Die Regelungen des Signaturgesetzes beruhen auf der EU-Richtlinie [8]. Daher bestehen in den EU-Staaten weitgehend übereinstimmende Regelungen zum Einsatz und zu den Rechtswirkungen elektronischer Signaturen einschließlich der gegenseitigen Anerkennung und dem grenzüberschreitenden Einsatz.
Nach § 23 Absatz 1 SigG sind Zertifizierungsdiensteanbieter aus anderen Mitgliedsstaaten daher inländischen Anbietern gleichgestellt, sofern sie die sachlichen Voraussetzungen der EU-Richtlinie erfüllen. Darüber hinaus ist auch die Gleichstellung von Zertifizierungsdiensteanbietern eines Drittlandes möglich, sofern bestimmte Anforderungen erfüllt sind.

Weitere Informationen erhalten Sie unter:

1. Bundesamt für Sicherheit in der Informationstechnik http://www.bsi.bund.de/esig/index.htm
2. Bundesnetzagentur: elektronische Signatur http://www.bundesnetzagentur.de/enid/gz.html
3. Gesetz über Rahmenbedingungen für elektronische Signaturen und zur Änderung weiterer Vorschriften, vom 16.05.2001, BGBl. 2001 I Nr. 22, S. 876 ff. geändert durch Art. 1 G v. 04.01.2005 (BGB1. 2005 I Nr 1, S. 2 ff.)
4. Verordnung zur elektronischen Signatur vom 16.11.2001, BGBl. 2001 I Nr. 59, S. 3074 ff, geändert durch Art. 2 G v. 04.01.2005 (BGB1. 2005 I Nr. 1, S. 2 ff.)
5. T7 e.V. und TeleTrusT e.V. : ISIS-MTT-Spezifikation, Version 1.1, März 2004, via http://www.isis-mtt.de
6. Gesetz zur Anpassung der Formvorschriften des Privatrechts und anderer Vorschriften an den modernen Rechtsgeschäftsverkehr vom 13.07.2001, BGBl. 2001 I Nr. 35, S. 1542 ff.
7. Gesetz über die Verwendung elektronischer Kommunikationsformen in der Justiz vom 22.03.2005, BGBl. I Nr. 18, S. 837 ff.
8. Richtlinie 1999/93/EG des Europäischen Parlaments und des Rates vom 13.12.1999 über gemeinschaftliche Rahmenbedingungen für elektronische Signaturen, via http://europa.eu.int/eur-lex/pri/de/oj/dat/2000/l_013/l_01320000119de00120020.pdf
9. ELSTER – die elektronische Steuererklärung, https://www.elster.de

Die zitierten Gesetzestexte sind unter http://bundesrecht.juris.de abrufbar