Hannes Federrath • Freie Universität Berlin • feder@inf.fu-berlin.de

Verläßlichkeit digitaler Signaturen

Während die mathematischen Operationen beim Erzeugen digitaler Signaturen nach dem heutigen Stand der Forschung als sicher bezeichnet werden können, sind die technischen Geräte, auf denen Dokumente signiert und getestet werden, weitaus unsicherer. Das Fälschen von Signaturen gelingt nicht etwa deshalb, weil die kryptographischen Funktionen unsicher sind, sondern deren Umsetzung und Einbettung in die zur Signatur verwendete Soft- und Hardware.

Grundlagen digitaler Signaturen

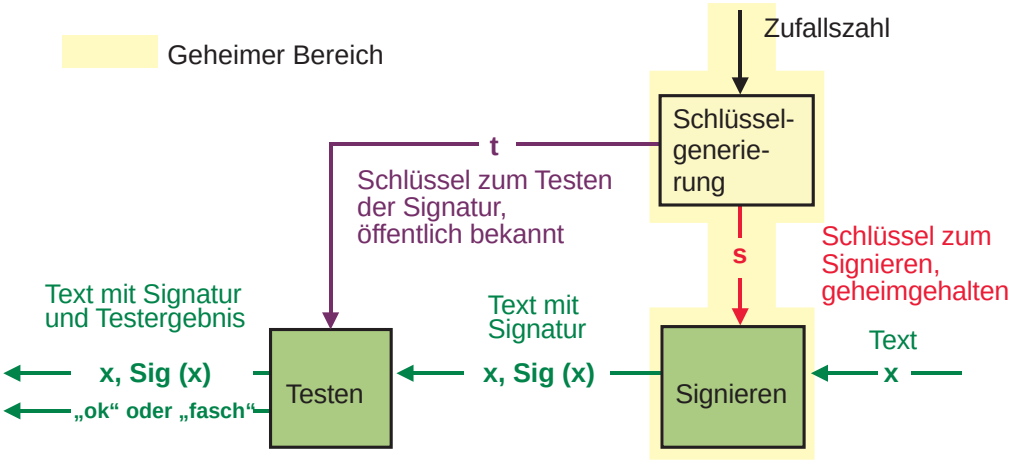
Digitale Signaturen basieren auf kryptographischen Funktionen. Beim Signieren werden digitale Dokumente mit einer digitalen Signatur versehen, die Jedem die Möglichkeit gibt, die Echtheit, d.h. Unverfälschtheit und Authentizität des Dokuments zu überprüfen. Zum Signieren des Dokuments besitzt der Signierer einen privaten Schlüssel, den nur er kennen darf. Die Signatur wird durch eine kryptographische Operation erzeugt, in die das Dokument und der private Schlüssel eingehen. Zum Überprüfen (Testen) eines Dokuments dient ein öffentlich bekannter Schlüssel, den jeder kennen darf. Aus dem öffentlichen Testschlüssel kann der private Signierschlüssel nicht abgeleitet werden. Der Test ist eine kryptographische Operation, in die das Dokument und der Testschlüssel eingehen.

Digitale Signaturen sind dann sicher, wenn es einem Fälscher mindestens **unmöglich** ist,

- die kryptographischen Funktionen zu knacken,
- den Signierschlüssel einer Person unberechtigt zu erfahren,
- dem Signierer ein Dokument unterzuschieben, das er gar nicht signieren wollte oder das er womöglich nie vorher gesehen hat,
- dem Tester vorzugaukeln, daß ein Dokument echt ist, obwohl es gefälscht ist.

Digitale Signaturen sind jedoch mehr als nur kryptographische Funktionen. Digitale Signaturen umfassen ebenfalls organisatorische und technische Komponenten. Dazu zählen:

- **Die Schlüssel müssen sicher erzeugt und aufbewahrt werden.** Der Signierer muß sich sicher sein, daß sein Signierschlüssel niemals einer anderen Person oder Organisation bekannt wird.
- **Die Authentizität des öffentlichen Testschlüssels**, d.h. die Zugehörigkeit des Testschlüssels zu einer bestimmten Person **muß** für des Tester **überprüfbar sein**. Die Zusammengehörigkeit von Testschlüssel und Person wird durch ein digitales Zertifikat be-



Die Operationen zum Berechnen und Testen einer digitalen Signatur

stätigt. Der Tester muß darauf vertrauen, daß der Aussteller des Zertifikats, eine sog. Zertifizierungsstelle, sich von der Identität einer Person überzeugt hat und niemals gefälschte oder irrtümlich falsche Zertifikate ausstellt.

– **Die technischen Geräte, mit denen die Dokumente vor dem Signieren angesehen und** gelesen und anschließend die **digitalen Signaturen erzeugt** und getestet **werden, muß** für den Signierer bzw. Tester vertrauenswürdig sein und außerdem **sicher sein gegen Manipulationen** und Ausforschung durch Fremde.

Die sichersten heute käuflichen Systeme zum Erzeugen digitaler Signaturen bestehen aus einem Chipkartenleser, der an den Computer angeschlossen wird, einer Software, die auf einem Standardbetriebssystem abläuft, und aus einer Chipkarte, die den privaten Signierschlüssel und die kryptographische Signieroperation enthält.

Diese Systeme erfüllen die oben genannten Anforderungen nicht vollständig. Das bedeutet, ein Fälscher ist ggf. in der Lage, digital signierte Dokumente zu erzeugen, die nicht von der Person stammen, der der Testschlüssel zugeordnet ist.

Manipulationsmöglichkeiten

Die Hauptgründe für diese Unsicherheiten sind:

– Chipkarten bieten nur eine begrenzte Sicherheit gegen Ausforschung und Manipulation. Es ist deshalb nicht auszuschließen, daß der Signierschlüssel doch aus der Chipkarte ausgelesen werden kann. Chipkarten stellen einen Kompromiß von Sicherheit und Handhabbarkeit dar.

– Die Signierschlüssel werden häufig in sogenannten Trust Centern erzeugt und anschließend auf die Chipkarte geladen. Es ist eine Frage des Vertrauens, ob das Trust Center eine Kopie des Signierschlüssels behält oder nicht. Gesetze können das Aufbewahren einer Kopie zwar verbieten, besser wäre es jedoch, wenn der Signierschlüssel direkt auf der Chipkarte erzeugt wird. Damit ersparen sich Trust Center, Gesetzgeber und Kunden eine Menge Ärger.

– Während der Signierer bei der eigenhändigen Unterschrift das unterzeichnete Dokument gegenständlich vor sich hat, gibt er beim Erzeugen der digitalen Signatur seinem Computer die Anweisung, eine bestimmte Datei oder einen im Speicher vorhandenen Datensatz durch die kryptographische Signieroperation bearbeiten zu lassen. Ein zu signierendes Dokument wird zunächst am Bildschirm des Computers betrachtet und anschließend an die Chipkarte übertragen, damit dort die digitale Signatur erzeugt wird. Es ist nicht auszuschließen, daß die Datenübertragung zwischen Computer und Chipkarte durch ein fremdes Programm auf dem Computer oder gar das Betriebssystem selbst verfälscht wird. Das bedeutet, die bei der Chipkarte ankommenden Daten stimmen nicht mit denen überein, die der Computerbildschirm zuvor angezeigt hat. Ein besonders bösartiges fremdes Programm könnte sogar die Dokumente vor der Sendung an die Chipkarte ersetzen, so daß der Benutzer ein Dokument signiert, das er nie zuvor gesehen hat.

– Die Signieroperation auf der Chipkarte wird dann ausgeführt, wenn der Benutzer durch Eingabe einer PIN bestätigt hat, daß die Signieroperation ausgeführt werden soll. Ein bösartiges fremdes Programm könnte die Eingabe der PIN abfangen und somit beliebig viele Signieroperationen auf der Chipkarte ausführen lassen.

Sichere digitale Signaturen

Die beiden letzten Manipulationsmöglichkeiten lassen sich dadurch beseitigen, daß das Signiergerät nicht nur den privaten Schlüssel und die Signieroperation, sondern über eine eingebaute Tastatur, einen eingebauten Bildschirm und ein manipulationssicheres Spezialbetriebssystem verfügt. Bevor der Benutzer das Dokument signiert, betrachtet er es am Bildschirm des Signiergerätes und löst über die eingebaute Tastatur die Signieroperation aus. Solange der Benutzer dem Signiergerät vertraut, das Signiergerät den Signierschlüssel erzeugt, die Software korrekt arbeitet und es keine Manipulationsmöglichkeiten von außen gibt, sind die erzeugten digitalen Signaturen sicher. Ein solches Gerät ist deutlich teurer als eine Software, ein Chipkartenleser und eine Chipkarte. Es ist aber unumgänglich, wenn sichere digitale Signaturen erzeugt werden sollen.

Fazit

Digitale Signaturen sind nur komplexitätstheoretisch sicher, d.h. die Wahrscheinlichkeit, daß ein Fälscher in der Lage ist, ein signiertes Dokument zu erzeugen oder den privaten Schlüssel zu finden, ist sehr klein, aber wird nie Null.

Der begrenzten Sicherheit von Chipkarten, Betriebssystemen und Computern sollte dadurch Rechnung getragen werden, daß die mit ihr erzeugten digitalen Signaturen eine Art Haftungsbegrenzung aufweisen. Keinesfalls sollte man in den Glauben verfallen, daß eine Beweislastumkehr (d.h. der Signierer beweist im Streitfall, daß er die Signatur nicht erzeugt hat) in jedem Fall möglich ist. Über kurz oder lang werden Experten in Streitfällen Gutachten vorlegen, daß es doch möglich ist, Signaturen ohne das Wissen des Signierers zu erzeugen.