DuD
Datenschutz und Datensicherheit

Zu einem prinzipiellen Problem digitaler Signaturen

Dirk Fox

Das am 1. August 1997 in Kraft getretene Signaturgesetz (SigG) wurde inzwischen durch die seit dem 1. November 1997 gültige Signaturverordnung (SigV) und Maßnahmenkataloge des BSI konkretisiert. Für ein zentrales, prinzipielles Problem enthalten jedoch bisher weder die Signaturverordnung noch die Maßnahmenkataloge eine geeignete Regelung: das der Darstellung digital signierter Daten. Der vorliegende Beitrag gibt ein Beispiel für einen Angriff unter Ausnutzung unterschiedlicher Darstellungsmöglichkeiten derselben Daten: Trotz einer erfolgreichen Prüfung einer digitalen Signatur unter einer Bitfolge kann ein Empfänger eine andere Nachricht sehen als der Signierer.

Dipl.-Inform.
Dirk Fox

ist Security Consultant der r³ security engineering ag, Karlsruhe.
Schwerpunkte: Kryptologie, insbesondere digitale Signatursysteme, Zertifizierungsinfrastrukturen, Sicherheit in Rechnernetzen.
E-Mail: fox@r3sec.de

Einleitung

Mit der Verabschiedung von Signaturgesetz (SigG, Art. 3 IuKDG) und Signaturverordnung (SigV) hat die Bundesregierung die Rahmenbedingungen für den praktischen Einsatz digitaler Signaturen im elektronischen Geschäftsverkehr geschaffen.

Neben der noch überwiegend in der Entwicklung befindlichen Integration des Mechanismus „digitale Signatur“ in Standard-Anwendungsprogramme, dem Aufbau Signaturgesetz-konformer Sicherungsinfrastrukturen und der Entwicklung geeigneter Signierkomponenten gibt es auch noch einige für Anwender und Hersteller wichtige und bisher nicht befriedigend gelöste offene Fragen. Dazu zählen insbesondere die Gestaltung der Signier- und Prüfkomponente sowie der Darstellungskomponente – in einer Weise, die auch einem nichtkundigen Anwender eine leichte Bedienbarkeit erlaubt, nach ITSEC zertifiziert ist, zu niedrigen Kosten vertrieben werden kann und keine Fälschungsmöglichkeiten bietet.

SigV und SigG sehen daher die Erstellung eines Maßnahmenkatalogs durch das Bundesamt für Sicherheit in der Informationstechnik (BSI) in enger Diskussion mit Vertretern der Industrie und wissenschaftlichen Experten vor, der Empfehlungen für den Einsatz und die Realisierung geeigneter Komponenten enthalten soll und im Bundesanzeiger zu veröffentlichen ist.

Eine 300 Seiten starke erste Fassung der Maßnahmenkataloge wurde am 18. November 1997 vom BSI vorgelegt.[1] Sie wurden nach erheblichen Einwänden von Industrievertretern jedoch noch einmal einer vollständigen Überarbeitung unterzogen. Inzwischen wurden von der Regulierungsbehörde im Umfang erheblich reduzierte Fassungen zu den § 12 Abs. 2 (Version 2.0a vom 25. März 1998) und § 16 Abs. 6 SigV (Version 1.0 vom 3. März 1998) publiziert; endgültige Fassungen sollen noch folgen.

1 Unfälschbarkeit

Damit digitalen Signaturen im elektronischen Rechtsverkehr zukünftig eine ähnlich hohe Beweiskraft zugemessen wird wie heute eigenhändigen Unterschriften, muß eine digitale Signatur die Unverfälschtheit und Urheberschaft von Daten zweifelsfrei gegenüber (unparteiischen) Dritten belegen können.

Um dies erreichen zu können, müssen die verwendeten Techniken dreierlei ausschließen:

- Niemand außer dem berechtigten Inhaber des Signierschlüssels darf eine gültige digitale Signatur erzeugen können (Authentizität).
- Jede nachträgliche Veränderung digital signierter Daten oder einer digitalen Signatur ist zweifelsfrei feststellbar (Integrität).
- Kein Signierer darf später glaubhaft abstreiten können, daß er eine digitale Signatur geleistet hat (Nicht-Abstreitbarkeit).

1.1 Technische Aspekte

Technisch meint der Vorgang des „digitalen Signierens“, daß mit einem geheimen Signierschlüssel zu einer gegebenen Bitfolge *m* ein Wert *s* (die digitale Signatur) berechnet wird. Mit Hilfe eines öffentlichen Prüfschlüssels kann dann nachgewiesen werden, daß *s* und *m* zusammengehören.

Die Veränderung auch nur eines einzigen Bits in *m* oder *s* führt dazu, daß diese Prüfung fehlschlägt. Das kryptographische Verfahren, mit dem eine solche digitale Signatur bestimmt wird, muß so sicher sein, daß es praktisch unmöglich ist, gültige

[1] http://www.bsi.bund.de, Version 1.0

digitale Signaturen ohne Kenntnis des geheimen Signierschlüssels zu erzeugen.[2]

Genügt ein digitales Signatursystem diesen technischen Anforderungen, gilt es in kryptographischer Hinsicht als unfälschbar.

1.2 Organisatorische Aspekte

Kryptographische Unfälschbarkeit eines digitalen Signatursystems bedeutet jedoch keineswegs, daß in der Praxis jede Signaturfälschung ausgeschlossen ist. Denn ein Fälscher könnte z.B.

- den geheimen Signierschlüssel erfahren (bspw. durch Auslesen oder Analyse einer Chipkarte [WoFo_97])
- dem Signierer Daten seiner Wahl unbemerkt unterschieben (siehe die provet-Simulationsstudie „Rechtspflege“ [HaBi_93, Pord_93]) oder
- ein falsches Schlüsselzertifikat erschleichen, das seinem Schlüssel eine fremde Identität zuordnet [Zies_97].

Durch geeignete organisatorische und technische Maßnahmen, von denen sich einige in den Maßnahmenkatalogen finden, lassen sich diese und ähnliche andere Fälschungsversuche verhindern. Spätestens die in der Signaturverordnung geforderte Prüfung der Komponenten nach genormten Sicherheitskriterien (ITSEC) sollte Mängel aufdecken, die solche Fälschungen ermöglichen.

2 Semantik

Übersehen wird jedoch häufig, daß eine erfolgreiche Fälschung keineswegs erfordert, daß die signierten Daten, die Signatur selbst oder die Signier- bzw. Darstellungskomponente manipuliert werden.

Denn eine digitale Signatur ist lediglich ein Nachweis für die Integrität und Authentizität einer bestimmten Bitfolge. Sie garantiert also nur die „syntaktische“ Unverfälschtheit dieser *Daten* – nicht aber die „semantische“ Unverfälschtheit der *Information*. Denn ob beispielsweise eine lediglich ein Bit lange Nachricht „Ja“ oder „Nein“ bedeutet, hängt von der für die Darstellung erforderlichen *Interpretation* dieses digital signierten Bits ab.

Ist diese Interpretation nicht eindeutig, dann hilft auch eine digitale Signatur nicht weiter: In diesem Fall ist (für den Empfänger und einen unparteiischen Dritten) unentscheidbar, ob der Signierer die Bedeutung „Ja“ oder „Nein“ siginiert hat.

Die tatsächliche Rechtsverbindlichkeit einer digitalen Signatur steht und fällt daher nicht nur mit der mathematischen und praktisch-technischen Unfälschbarkeit eines digitalen Signaturverfahrens, sondern auch mit der Eindeutigkeit der *Darstellung* der signierten Daten.

Wie aber eine digital signierte Bitfolge für die Darstellung interpretiert wird, hängt insbesondere von der verwendeten *Kodierung* und dem speziellen *Format* der Daten ab.[3]

3 Darstellungen

Weder die Signaturverordnung noch die Maßnahmenkataloge schreiben eine bestimmte Kodierung oder ein Datenformat vor. Dahinter scheint die Überzeugung zu stehen, daß man es in der Praxis in der Regel mit ausreichend langen Bitfolgen zu tun haben wird, die über eine hinreichende Redundanz verfügen, um (gezielte oder ungewollte) Fehlinterpretationen bei der Darstellung signierter Daten auszuschließen.

3.1 Doppeldeutigkeit

Tatsächlich ist es sehr unwahrscheinlich, z.B. zu einer vorliegenden digital signierten Datei eine zweite Darstellungs-Interpretation zu *finden*, die unter einer gängigen Darstellungskomponente einen abweichenden, dennoch sinnvollen Inhalt anzeigt (z.B. ein Text-Dokument, das in einem Graphik-Programm als Bild erscheint). Dies wäre jedoch für eine passive Signatur-„Fälschung“ der beschriebenen Art erforderlich.

Hingegen ist es sehr wahrscheinlich, daß es gelingt, eine Datei (aktiv) zu *erzeugen*, die unter zwei verschiedenen Darstellungskomponenten zwei unterschiedliche und jeweils sinnvolle Darstellungen besitzt. Kann ein Fälscher nun jemanden dazu bewegen, diese Datei digital zu signieren, kann er abhängig von der Darstellungskomponente zwei inhaltlich unterschiedliche, gültig digital signierte Dokumente vorlegen.

Eine solche aktive Signatur-„Fälschung“ mag auf den ersten Blick unwahrscheinlich erscheinen. In der Praxis läßt sich ein solcher Fall jedoch sehr leicht konstruieren: Schließt man mit einer Person einen von beiden Parteien digital signierten Vertrag, bei dem das Vertragsdokument eine solche Zweideutigkeit aufweist, kann ein Vertragspartner später ein digital signiertes Dokument mit abweichendem Inhalt vorlegen.

Da wahrscheinlich viele digital signierte Bitfolgen in einem anwendungsspezifischen Format vorliegen und daher neben den in einer bestimmten Kodierung dargestellten Zeichen auch Steuerzeichen, Reste gelöschter Daten oder Makro-Anweisungen (in allen Textverarbeitungen üblich) enthalten werden, ist es z.B. möglich,

- durch Änderung der Datei-Kennung (unter DOS/Windows z.B. „*.doc“ in „*.txt“) unterschiedliche Darstellungen der Daten (z.B. Steuerzeichen als Text) zu erzwingen,
- Fehler in der Format-Konvertierung einer bestimmten Darstellungskomponente auszunutzten,
- spezielle Anzeige-Optionen (wie die Darstellung von „verborgenem Text“ oder eine nahezu unsichtbare Farbwahl einzelner Zeichen) zum Verstecken bestimmter Textteile einzusetzten.

Diese Liste läßt sich zweifellos noch erweitern.

Grundsätzlich läßt es sich auch bei Vorkehrungen gegen bekannte „Tricks“ dieser Art nicht sicherstellen, daß es keine weiteren, ähnlichen Möglichkeiten gibt.

3.2 Beispiel

Angesichts der Komplexität heutiger Anwendungsprogramme dürfte es in der Praxis häufig noch wesentlich einfacher sein, geringfügige Unterschiede in den Implementierungen desselben Anwendungsprogramms für unterschiedliche Betriebssysteme auszunutzen.

Ein besonders hübsches Beispiel für eine solche Darstellungs-„Fälschung“ bietet das Textverarbeitungsprogramm MS-Word. Unterschreibt man einen unter WinWord (Version 6.0a) erstellten Vertragstext folgenden Inhalts (siehe auch Abb.):

„Hiermit verpflichte ich mich zur ¼jährlichen Zahlung von DM 10.000,- über 3 Jahre.“,

dann reduziert sich diese Verpflichtung unter „Word for Macintosh“ (Version 5.1 und 6.0.1) auf ein Viertel dieser Summe, denn dort erscheint:

[2] Zur Sicherheit digitaler Signatursysteme siehe Fox, DuD 2/97, S. 69 ff. [Fox_97].

[3] Natürlich fließen in die Bedeutung auch inhaltliche Interpretationen des Betrachters ein. Dies ist aber eine Dokumenten allgemein eigene Mehrdeutigkeit.

„Hiermit verpflichte ich mich zur jährlichen Zahlung von DM 10.000,- über 3 Jahre."

Das Sonderzeichen „¼" (das Word bei der Standardeinstellung in Extras/Optionen/AutoFormat „Brüche durch Sonderzeichen" automatisch einfügt) von Word 6.0a wird von Word for Macintosh 6.0.1 als „_" interpretiert.

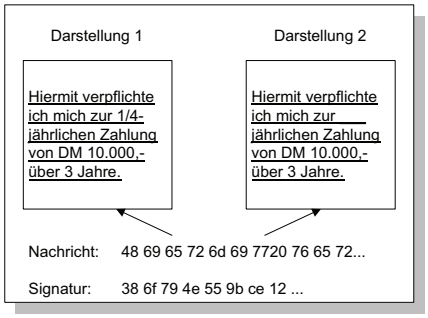

Abb.: Unterschiedliche Darstellung desselben Dokuments

Je nach Interesse des Vertragspartners läßt sich auf diese Weise (ohne jeden Programmieraufwand) durch Wahl des Textverarbeitungsprogramms eine Zahlungsverpflichtung vervierfachen bzw. auf ein Viertel reduzieren.

4 Lösungsweg

Einen wirkungsvollen Schutz vor solchen Darstellungs-„Fälschungen" erreicht man nur durch die Festlegung von Format und Kodierung der digital signierten Daten. Dafür gibt es prinzipiell drei Wege:

- Erstens kann die für ein digital signiertes Dokument zu verwendende Darstellungskomponente (und damit auch Format und Kodierung der Daten) zwingend vorgeschrieben werden.

Diese Komponente könnte mehrere Darstellungsformate beherrschen und würde unzulässige Formate und Kodierungen abweisen. Sie könnte zusätzlich als ein „*tamper resistent*"-Device ausgelegt werden und so außerdem Angriffe verhindern, die eine Manipulation der Darstellungskomponente voraussetzen.

Entscheidende Nachteile dieser Lösung sind jedoch der erforderliche erhebliche regulative Eingriff sowie die hohen Kosten für Hersteller und damit auch den Nutzer. Daher würde eine solche Lösung die Integration von digitalen Signaturen in Standard-Anwendungen erheblich erschweren, wenn nicht gar verhindern.

- Zweitens ließe sich die Kodierung digital signierter Daten allgemein und systemunabhängig festlegen.

Das ISO-OSI-Modell sieht in der Darstellungsschicht von Kommunikationssystemen zur plattformunabhängigen Kodierung von Daten die „Abstract Syntax Notation One" (ASN.1) vor [ISO_87]. Sie erlaubt eine eindeutige Kodierung beliebig strukturierter Daten durch eine „Tag-Length"-Darstellung (Feldtyp-Länge). Auf diese Weise wäre die Kodierung digitaler Daten eindeutig; Zweifelsfälle wie das oben genannte Beispiel würden nicht auftreten.

Allerdings müßten Daten für das digitale Signieren geeignet umkodiert werden; dabei gingen unweigerlich auch Informationen (wie z.B. Formatierungsangaben) verloren.

- Schließlich könnte im Format einer digitalen Signatur ein Feld vorgesehen sein, daß das verwendete Format und die Kodierung angibt.

Will man verbreitete Kodierungen wie bspw. die gängiger Textverarbeitungssysteme unterstützen, ließe sich das verwendete Format in den digital signierten Daten vermerken. Dazu ist allerdings eine allgemein gültige, bspw. von der Regulierungsbehörde geführte Format- und Kodierungsliste erforderlich, in der Dokumentenformate registriert und einem bestimmten festen Format- und Kodierungs-Bezeichner zugeordnet werden.

Fazit

Das angeführte Beispiel zeigt, daß bei der Betrachtung der Sicherheit (Unfälschbarkeit) digitaler Signaturen auch die Formatdarstellung und die Kodierung der signierten Daten berücksichtigt werden müssen. Will man primitive Darstellungs-„Fälschungen" wie in dem vorgestellten Beispiel vermeiden, die zudem der Vertrauenswürdigkeit des Mechanismus „digitale Signatur" erheblichen Schaden zufügen können, erscheint die Einführung eines zentralen, von der Regulierungsbehörde geführten und authentischen „Format- und Kodierungs-Registers" unausweichlich.

Dank

Für hilfreiche Diskussionen zu diesem Thema danke ich insbesondere Birgit Pfitzmann und Michael Waidner, die das schöne Beispiel aus leidvoller Word-Erfahrung beisteuerten, sowie Rüdiger Grimm und Jobst Biester.

Literatur

[Fox_97] Fox, Dirk: *Fälschungssicherheit digitaler Signaturen*. DuD 2/97, S. 69-74.

[HaBi_93] Hammer, Volker; Bizer, Johann: *Beweiswert elektronisch signierter Dokumente*. Datenschutz und Datensicherung (DuD), 12/93, S. 689-699.

[ISO_87] International Organization for Standardization (ISO): *Specification of Abstract Syntax Notation One (ASN.1)*. International Standard ISO 8824, Genf, 15. Dezember 1987.

[Pord_93] Pordesch, Ulrich: *Risiken elektronischer Signaturverfahren*. Datenschutz und Datensicherung (DuD), 10/93, S. 561-569.

[WoFo_97] Wohlmacher, Petra; Fox, Dirk: *Hardwaresicherheit von SmartCards*. DuD 5/1997, S. 260-265.

[Zies_97] Zieschang, Thilo: *Sicherheitsrisiken bei der Schlüsselzertifizierung*. DuD 6/1997, S. 341-343.