Sichere PDF-Dokumente durch digitale Signaturen

soft Xpansion GmbH & Co. KG

Inhaltsverzeichnis

1. Digitale Welt 1
2. Digitale Signatur 1
3. Rechtliche Rahmenbedingungen und Aufgaben einer digitalen Signatur 2
4. Öffentliche und private Schlüssel, Zertifikate 3
5. Signaturen erstellen und überprüfen 3
6. Signieren im PDF-Format 6
7. Vertraulichkeit von Informationen durch die digitale Signatur? 8
8. PDF Xpansion-Produkte für Signierung und Überprüfung von Signaturen 8
9. soft Xpansion Smart Card Crypto Provider 9

1. Digitale Welt

In den letzten zwanzig Jahren hat Papier als wichtigster Informationsträger an Bedeutung verloren. Nach Meinung von Fachleuten ist es denkbar, dass Papierdokumente in nicht allzu ferner Zukunft nur noch eine Rolle als Kopien von digitalen Originaldokumenten spielen könnten. Diese Vision ist heute bereits in einigen Bereichen Realität: so erhält man als Kunde von vielen Mobilfunkanbietern oder Internetprovidern seine Rechnungen standardmäßig per E-Mail als elektronisches Dokument (PDF-Datei) und muss die Zusendung auf Papier zusätzlich beantragen oder in einigen Fällen gar zusätzlich bezahlen.

Digitale Dokumente haben im Vergleich zum Papier unter vielen Gesichtspunkten unwiderlegbare Vorteile, zum Beispiel längere Haltbarkeit, schnellere Übertragung, Schutz von natürlichen Ressourcen. Traditionelle Papierdokumente hatten hingegen bisher einen ganz anderen Vorteil, den digitale Dokumente lange Zeit nicht ausgleichen konnten: auf ihnen können die eigenhändige Unterschrift einer Person oder der Stempel eines Unternehmens oder einer Behörde platziert werden, um die Echtheit des Dokuments oder einer Willenserklärung zu bescheinigen. Aber dieser Vorteil verliert durch den technischen Fortschritt im Bereich der digitalen Unterschrift (Signatur) immer mehr an Bedeutung.

2. Digitale Signatur

Digitale Unterschriften dienen bei der elektronischen Kommunikation zum Beispiel über E-Mail dazu, sicheres und rechtsverbindliches Handeln zu ermöglichen. Sie werden unter anderem verwendet, wenn im Prozess des Unterzeichens von Dokumenten ganz auf die eigenhändige Unterschrift auf Papier verzichtet werden soll. Aber wie muss eine solche digitale Unterschrift konkret ausgestaltet sein, damit sie rechtsverbindliches elektronisches Handeln ermöglicht? Wie können Unternehmen, die den Versand ihrer geschäftlichen Dokumente weiter digitalisieren möchten sicherstellen, dass die Empfänger diesen Dokumenten genauso vertrauen wie den althergebrachten Papierdokumenten? Wie kann der Empfänger einer Mobilfunk-Rechnung sicher sein, dass das per E-Mail zugegangene Dokument tatsächlich von seinem Provider stammt? Oder wie überprüft ein Kunde, ob die Nachricht über eine Rückrufaktion für den neuen PKW tatsächlich vom Hersteller stammt?

Technisch betrachtet wird eine digitale Signatur durch die Kombination eines so genannten elektronischen Zertifikats mit einem digitalen Schlüsselpaar (siehe weiter unten den Abschnitt **„Öffentliche und private Schlüssel, Zertifikate“**) realisiert. Bei Verwendung einer

digitalen Signatur werden Zertifikat und öffentlicher Schlüssel zusammen mit dem unterzeichneten Dokument versandt. Persönliche Zertifikate und Software-Schlüssel können zum Beispiel auf Smart Cards oder auf speziellen USB-Geräten (eTokens) gespeichert werden. Um eine digitale Unterschrift mit Hilfe einer Smart Card zu erstellen, ist ein spezielles Karten-Lesegerät erforderlich, das mit dem Computer verbunden ist. Darüber hinaus werden auch Tastaturen angeboten, in die das Lesegerät bereits integriert ist. Für die Verwendung eines USB-Geräts muss ein USB-Anschluss am Computer vorhanden sein.

3. Rechtliche Rahmenbedingungen und Aufgaben einer digitalen Signatur

In vielen Ländern gelten mittlerweile Gesetze und weitere rechtliche Grundlagen, die die digitale Unterschrift erlauben und die Voraussetzungen regeln, unter denen diese der eigenhändigen Unterschrift gleichgestellt ist. In Deutschland müssen seit dem 1.07.2004 per E-Mail versandte Rechnungen laut Signaturgesetz (SigG) und der Signaturverordnung (SigV) mit einer so genannten qualifizierten Signatur digital unterschrieben werden, um als Äquivalent einer Papierrechnung akzeptiert zu werden.

Warum muss eine per E-Mail versandte Rechnung laut Gesetz digital unterschrieben werden, während eine Papier-Rechnung auch ohne Unterschrift gültig ist? Der Grund liegt in den Besonderheiten des Datenaustausches über elektronische Wege: zum einen können wir nicht sicher sein, dass unser Kommunikationspartner, also zum Beispiel der Versender der Rechnung per E-Mail, tatsächlich derjenige ist, der er zu sein vorgibt (Problem der Identität des Gegenüber). Zum anderen besteht die Gefahr, dass die Rechnung auf dem Weg vom Versender zum Empfänger verändert wurde (Problem der Integrität des Inhalts).

Eine digitale Signatur erfüllt vor diesem Hintergrund für eine definierte Datenmenge, für ein elektronisches Dokument oder für einen Teil davon grundsätzlich folgende Zwecke:

Authentifizierung (Nachweis der Identität einer Person) - die digitale Signatur dient zum einen der Feststellung, ob der Verfasser beziehungsweise der Versender eines Dokuments tatsächlich der ist, der er zu sein erklärt. Dabei wird die eindeutige Identifizierung des Verfassers dadurch erreicht, dass seiner Person ein so genannter geheimer Schlüssel zugeordnet ist, der zusammen mit der Signatur in das digital unterzeichnete Dokument eingefügt wird.

Unleugbarkeit - weiter ermöglicht die digitale Signatur zu verhindern, dass der Versender einer Nachricht zu einem späteren Zeitpunkt abstreitet, die Nachricht versandt zu haben. Der Empfänger einer Nachricht kann so den Absender rechtskräftig feststellen (lassen) und dies zum Beispiel vor Gericht verwenden. Sobald allerdings der ursprüngliche Inhaber des geheimen Schlüssels die alleinige Kontrolle über diesen verliert, muss umgehend eine Sperrung des Zertifikats erfolgen, mit dem digital unterzeichnet wird. Ab der Sperrung sind alle digitalen Signaturen, die vorgeblich von diesem Verfasser kommen, verdächtig. Wird dann die Urheberschaft eines bestimmten signierten Dokuments geleugnet, so bedeutet dies gleichzeitig, dass der geheime Schlüssel auch für alle weiteren Signiervorgänge nicht mehr verwendet werden kann.

Nachweis der **Integrität von Inhalten (Dokumenten)** – häufig kommt es bei der digitalen Kommunikation darauf an, dass darauf vertraut werden kann, dass ein Dokument nach Unterzeichung nicht verändert wurde. Durch die Verschlüsselung eines Dokuments wird zwar dessen Inhalt in eine nicht im Klartext lesbare Zeichenfolge umgewandelt. Aber die meisten Verschlüsselungsverfahren verhindern nicht, dass der verschlüsselte Inhalt verändert werden

kann. Im Falle einer zusätzlichen digitalen Signierung wird die Unterschrift hingegen ungültig, wenn eine Änderung am signierten Dokument erfolgt.

Verwendung von (qualifizierten) Zeitstempeln - wenn die digitale Unterschrift mit einem qualifizierten Zeitstempel (§2 Nr. 14 SigG) versehen ist kann zuverlässig nachvollzogen werden, wann ein Dokument erstellt, unterzeichnet und gegebenenfalls modifiziert wurde, zu welchen Zeitpunkt also originale, unveränderte Daten vorgelegen haben. So kann auch unter dem zeitlichen Aspekt die zuvor erwähnte Unleugbarkeit gewährleistet werden. Nachträgliche Vor- oder Rückdatierungen von Nachrichten und Daten können so ausgeschlossen werden.

Die Verwendung von Zertifikaten, elektronischen Schlüsseln und Zeitstempeln setzt natürlich voraus, dass die sie herausgebenden Unternehmen oder Institutionen selbst vertrauenswürdig sind. In Deutschland müssen sich die entsprechenden Dienstanbieter bei der Bundesnetzagentur, einer zum Bundesministerium für Wirtschaft und Technologie gehörenden Bundesbehörde akkreditieren, bevor sie qualifizierte Zertifikate und Zeitstempel ausstellen dürfen. Für akkreditierte Dienstanbieter wird dann angenommen, dass sie vertrauenswürdig sind.

Die Zertifizierungsdiensteanbieter heißen auf internationaler Ebene Certificate Authority (CA), die Zeitstempel-Anbieter (ZSA) werden als Timestamping Authority (TSA) bezeichnet.

4. Öffentliche und private Schlüssel, Zertifikate

Digitale Signaturen basieren auf der Verwendung von zwei elektronischen Schlüsseln, die als ein Schlüsselpaar zusammengehören. Mit einem so genannten privaten oder geheimen Schlüssel, der nur dem Unterzeichner oder Versender einer Nachricht bekannt sein darf (auch nicht dem Zertifizierungsdiensteanbieter, ZDA!), werden Inhalte unterzeichnet bzw. verschlüsselt. Das mit dem privaten Schlüssel verbundene Zertifikat bescheinigt die Identität des Verfassers, sofern der ZDA vertrauenswürdig ist, und ist somit mit einem elektronischen Ausweis vergleichbar. Mit seinem Gegenstück, dem öffentlichen Schlüssel, werden die Identität des Verfassers und die Integrität der versandten Nachrichten im Rahmen der Entschlüsselung überprüft. Der öffentliche Schlüssel darf im Gegensatz zum privaten Schlüssel allgemein bekannt sein, damit die Überprüfung erfolgen kann. Aus diesem Grund wird das verwendete Verschlüsselungsverfahren als asymmetrisches kyrptografisches Verfahren bezeichnet. Die beiden Schlüssel sind durch das mathematische Verfahren ihrer Erstellung miteinander verknüpft, aber der private Schlüssel kann dennoch nicht aus dem öffentlichen abgeleitet (berechnet) werden. Bei Daten, die mit einem privaten Schlüssel signiert bzw. verschlüsselt wurden, können die Signaturen nur mit dem korrespondierenden öffentlichen Schlüssel entschlüsselt und verifiziert werden. Technische Details erläutert der folgende Abschnitt.

Auch das von Dienstanbieter ausgestellte Zertifikat selbst wird elektronisch signiert. Es gibt auch Zertifikate, die nur innerhalb eines Unternehmens Anwendung finden. Diese sind dann in der Regel auf Servern des Unternehmens abgelegt.

5. Signaturen erstellen und überprüfen

Welche technischen Prozesse laufen nun beim digitalen Signieren und bei der Überprüfung einer Signatur konkret ab? Zunächst einmal muss vorausgeschickt werden, dass die

Erstellung einer digitalen Signatur mittels Verschlüsselung sämtlicher Daten einer Nachricht aus drei Gründen unpraktisch ist:

- Das Datenvolumen der Signatur entspräche dem des Originaldokuments, so dass sich das Datenvolumen insgesamt verdoppelt und viel Speicherplatz beziehungsweise Bandbreite bei Übertragung beansprucht wird
- Die Verschlüsselung ist langsam und erhöht die Prozessorbelastung, so dass die Performance des Netzwerks und der verwendeten Computer gegebenenfalls deutlich reduziert wird
- Durch das erhöhte Datenvolumen der Signatur wird die Gefahr von kryptoanalytischen Angriffen erhöht

In der Praxis werden die zu signierenden Daten eines Dokuments oder einer Nachricht deshalb in einen so genannten Hashwert umgerechnet. Der Hashwert ist eine Zahlenwert und damit eine Kurzfassung der Nachricht, die im nächsten Schritt dann signiert wird. Hashing oder eine Hashfunktion dient also dazu, digitale Zusammenfassungen von Daten zu erstellen. Diese Zusammenfassungen nennt man auch Message Digests oder kryptografische Prüfsummen. Sie haben üblicherweise eine Länge von 128 bis 160 Bit und enthalten ein eindeutiges und individuelles digitales Identifizierungsmerkmal für jede Nachricht. Das heißt: nur identische Nachrichten haben denselben Hashwert. Jede noch so kleine Änderung an der Nachricht liefert einen veränderten Hashwert. Bereits eine Änderung von einem Bit reicht hier aus.

Zwei der am weitesten verbreiteten Algorithmen für die Erstellung von Message Digests sind heute MD5 und SHA-1. MD5 berechnet einen Message Digest von 128-Bit Länge und wurde von der RSA Data Security Inc. entwickelt. SHA-1 hat eine Länge von 160 Bit und wurde von der National Security Agency, dem Geheimdienst der USA, entwickelt. Wegen des längeren Hashwerts wird allgemein angenommen, dass der SH1-Algorithmus eine größere kryptografische Sicherheit als MD5 bedeutet. Darüber hinaus ist SH1 nicht anfällig für einige Angriffe, die auf MD5 geführt werden können.

Die Technik bei der Verwendung von Zeitstempeln (siehe Abschnitt 3) ist dieselbe wie bei der Signierung von Daten. Der aus den Originaldaten der Nachricht oder des Dokuments berechnete Hashwert wird ebenfalls an einen dafür akkreditierten Diensteanbieter (ZSA) gesandt. Dieser verknüpft den (Originaldaten-) Hashwert mit einem Zeitstempel und generiert einen neuen Hashwert aus den verknüpften Daten. Der resultierende ZS-Hashwert (Zeitstempel-Hashwert) wird mit dem privaten Schlüssel des ZSA digital signiert. Zeitstempel, ZS-Hashwert und privater Schlüssel des ZSA werden dann an die Person, Unternehmung oder Institution zurückgesandt, die den Zeitstempel angefordert hat.

Die folgenden beiden Abbildungen zeigen die technischen Abläufe beim Signieren (Abbildung 1) und beim Überprüfen einer Signatur (Abbildung 2):

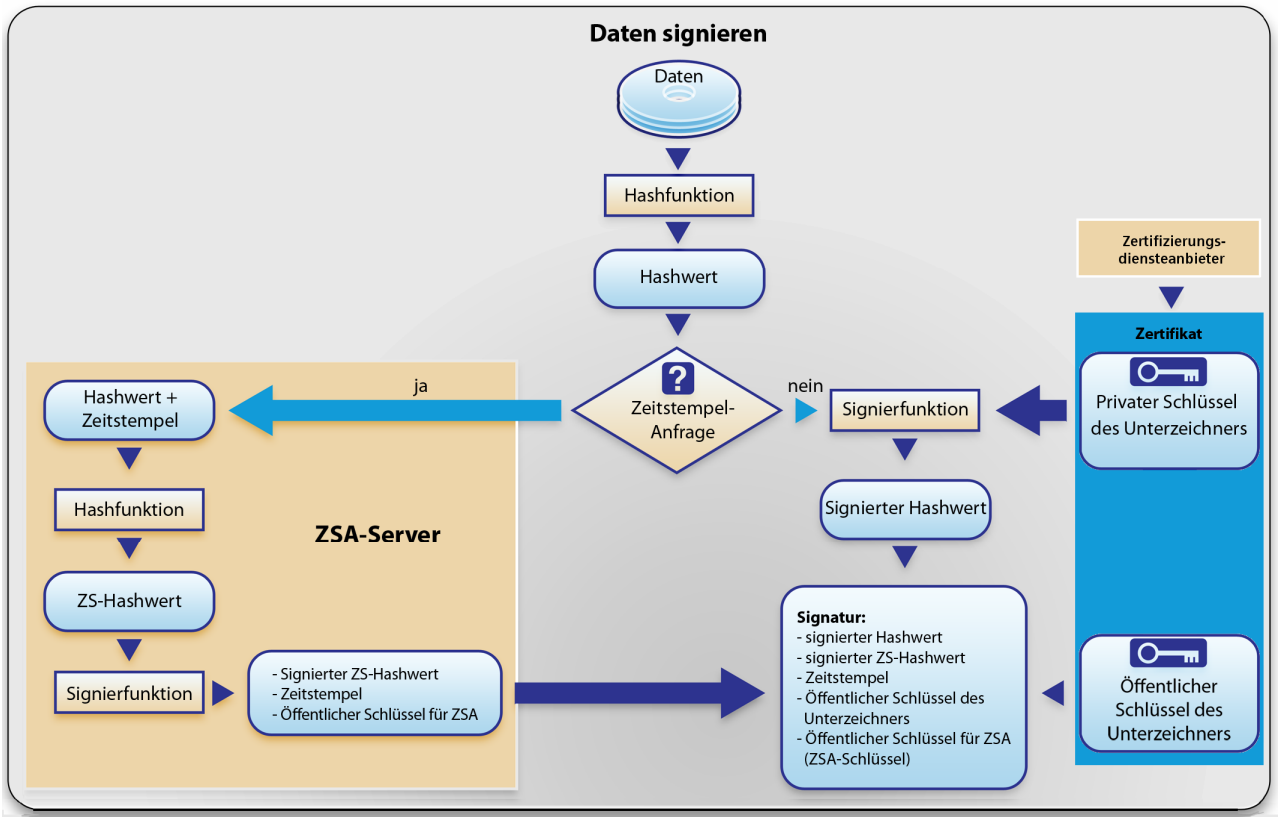

Abbildung 1. Signieren von Daten

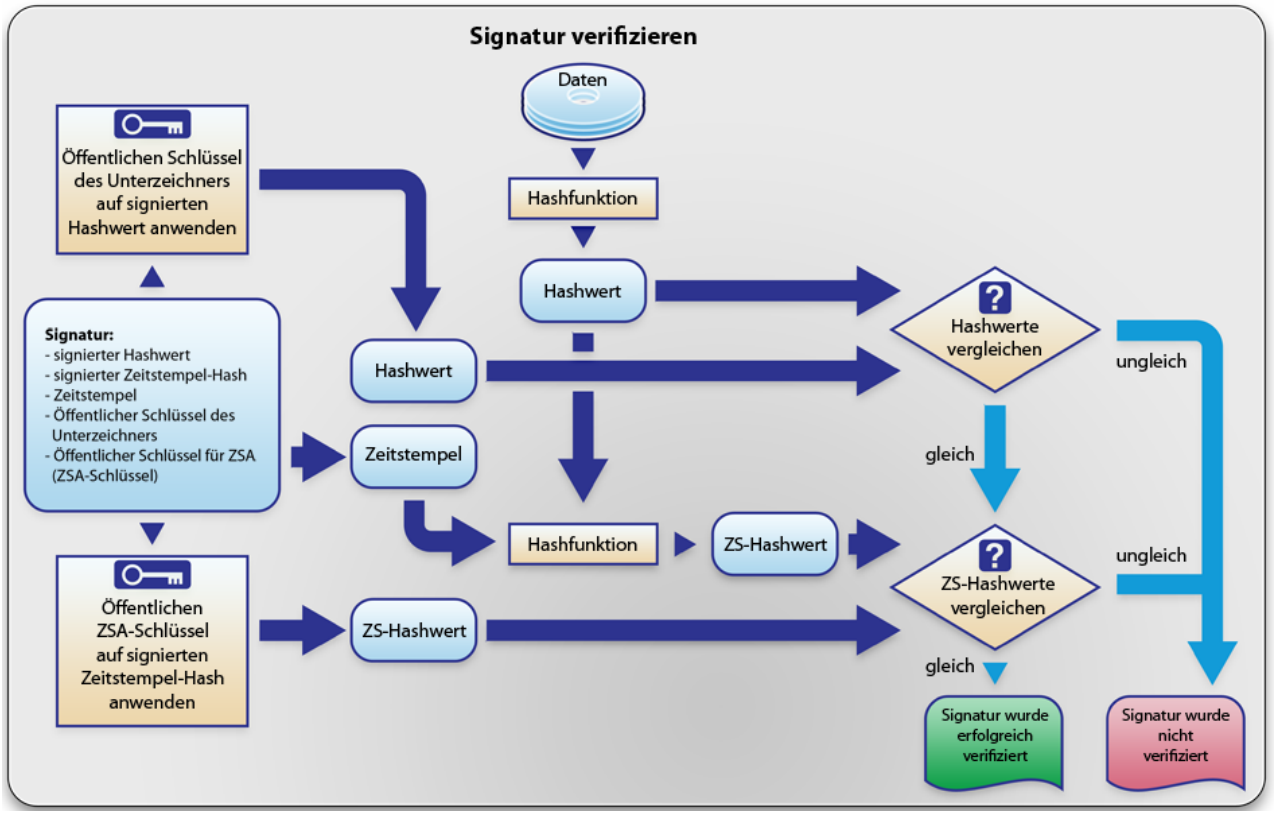

Abbildung 2. Überprüfung einer Signatur

6. Signieren im PDF-Format

Grundsätzlich kann also jedes elektronische Dokument digital unterschrieben werden und es besteht die Möglichkeit, die Unterschriften zu verifizieren. Ein elektronisches Dokument ist normalerweise eine separate Datei oder ein Datensatz in einer Datenbank. Aber auch die die digitale Signatur selbst ist ein Datensatz der gespeichert werden muss. Nicht alle Dateiformate erlauben es, „fremde" Daten - was elektronische Signaturen aus Sicht der eigentlichen Dokumente sind - in das Dokument zu integrieren. In diesen Fällen muss die Signatur als eine separate Datei immer zusammen mit dem Dokument versandt und aufbewahrt werden.

Einige Dateiformate erlauben hingegen die direkte Integration von digitalen Signaturen, und zwar Adobes PDF und Microsofts XPS oder XML-basierte Formate. Da sich das PDF-Format erstens als Quasi-Standard für den Austausch und für die Archivierung von elektronischen Dokumenten etabliert hat (XPS ist ein noch relativ junges Format) und da es zweitens speziell für den Bereich der digitalen Signaturen gesonderte Spezifikationen bereit hält, wird PDF für das elektronische Signieren in der Praxis immer häufiger verwendet.

Das PDF-Format bietet flexible und vielfältige Möglichkeiten, die eine Verwendung von digitalen Signaturen sowohl für den Softwareentwickler als auch für den dem Endanwender attraktiv machen.

Wie eine einzelne digitale Signatur in einer PDF-Datei verankert wird zeigt Abbildung 3a.

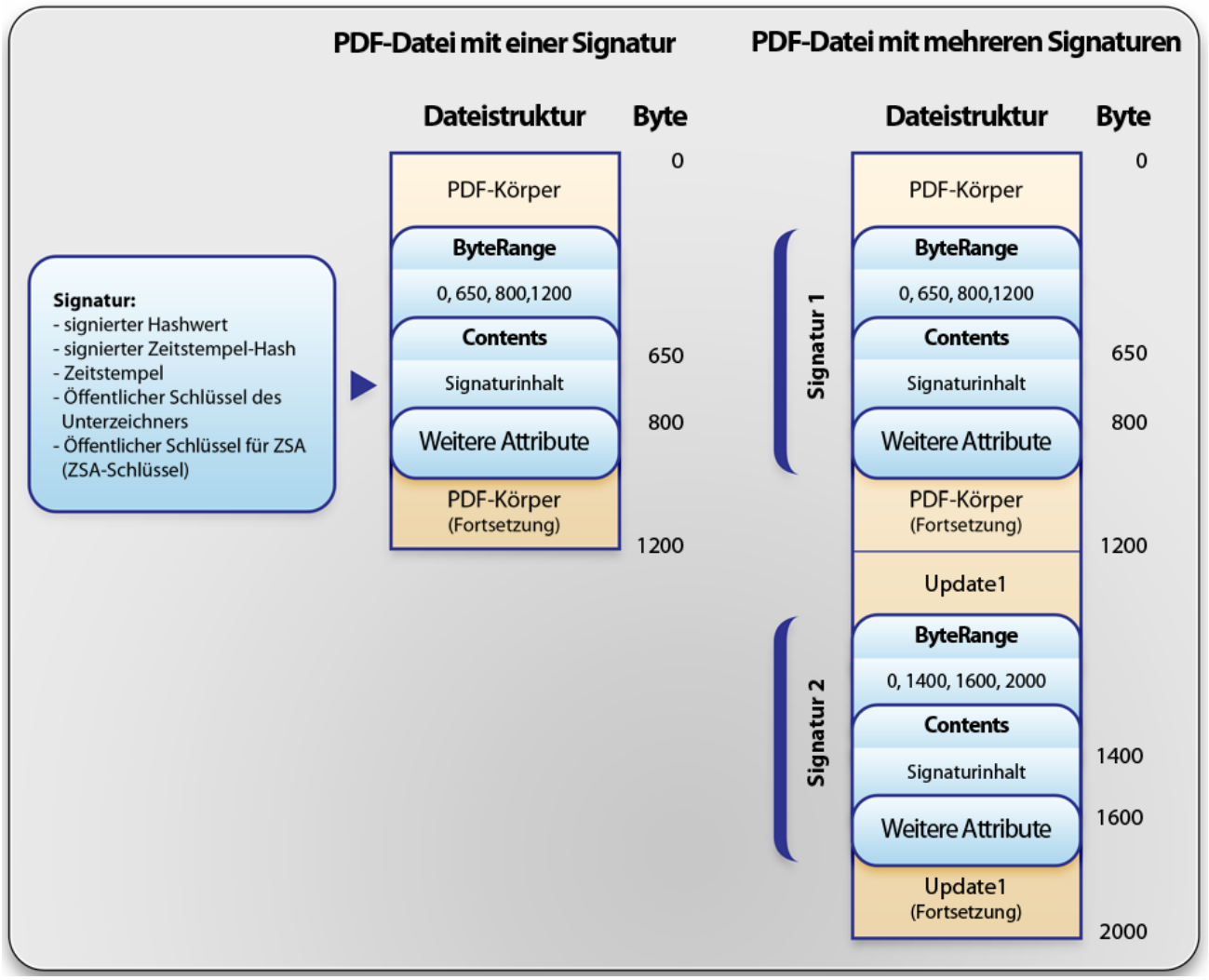

Abbildung 3 a) und b). Signieren einer PDF-Datei

Das ByteRange-Attribut definiert, welcher Inhalt der PDF-Datei durch die Hashfunktion in einen Zahlenwert umgerechnet werden soll. Dies ist üblicherweise der komplette Inhalt der Datei oder der Nachricht, mit Ausnahme der Signatur selbst. Das Contents-Attribut beinhaltet die wichtigsten Signatur-Bestandteile wie die Hashwerte und den öffentlichen Schlüssel. Weitere Attribute sind spezielle technische Eigenschaften, die in der Adobe PDF-Spezifikation beschrieben sind und vom Softwareentwickler berücksichtigt werden müssen.

Die Signatur in der PDF-Datei kann zum einen eine komplett vom System berechnete, rein mathematisch erstellte Signatur sein. Sie kann aber auch auf biometrischen Merkmalen wie einer handschriftlichen Signatur, einem Fingerabdruck oder einem Scan der Netzhaut basieren. Dabei sollte es so sein, dass PDF-Produkte die Zusammenarbeit von unterschiedlichen Signaturprogrammen erlauben: eine mit einer Anwendung 1 des Verfassers 1 signierte PDF-Datei muss mit einer anderen Anwendung 2 eines anderen Verfassers überprüfbar sein.

Mehrfachsignaturen im PDF-Dokument können mittels so genannter inkrementeller Updates realisiert werden.

Inkrementelle Updates fügen alle Modifikationen an das Ende der Datei an, so dass die ursprünglichen Daten unberührt bleiben. Somit ist es relativ einfach, einzelne oder alle

Updates rückgängig zu machen, um eine bestimmte Dateiversion zu erhalten. Und im Falle von mehrfach signierten Dokumenten kann man so sowohl die originalen Inhalte der Person, die zuvor signiert hat als auch seine eigenen Vermerke (das Update) signieren und damit bestätigen.

Abbildung 3b zeigt schematisch die Struktur einer mehrfach signierten PDF-Datei.

Der Adobe Reader unterstützt die folgenden Signaturstandards:
- PKCS#1 (RSA-Verschlüsselung und SHA1-Digest-Algorithmus)
- PKCS#7 (RSA-/DSA-Verschlüsselung sowie SHA1-, SHA256-, SHA384- und SHA512-Digest-Algorithmen)
- PKCS#7 detached (RSA, DSA-Verschlüsselung und SHA1-, SHA256-, SHA384-, SHA512-Digest-Algorithmen)

7. Vertraulichkeit von Informationen durch die digitale Signatur?

Wie bereits erwähnt können bei einer elektronisch signierten E-Mail oder PDF-Datei die Identität des Verfassers und die Integrität der Nachricht überprüft werden. Dies bedeutet jedoch nicht, dass automatisch auch die Nachricht selbst so verschlüsselt wird, dass Unbefugte sie nicht lesen können. Vielmehr wird in der Regel die unverschlüsselte Originalnachricht neben der Signatur, dem Zertifikat und dem Hashwert der Nachricht übermittelt. Moderne Software-Produkte bieten deshalb zusätzliche Funktionen, mit denen auch die Nachricht selbst verschlüsselt werden kann.

8. PDF Xpansion-Produkte für Signierung und Überprüfung von Signaturen

Smart Card Crypto Provider – Softwarebibliothek, die digitale Signaturen und Datenkodierung mit weit verbreiteten Smart Cards ermöglicht. Sie unterstützt die Signaturkarten wichtiger Hersteller wie Deutsche Post, D-Trust, TeleSec, sowohl für die Signierung von PDF-Dateien als auch für andere Zwecke, zum Beispiel für die Autorisierung von PC- und Netzwerkanwendern.

PDF Direct & Quick View – Softwarebibliothek, die es Entwicklern ermöglicht, digitale Dokumente im PDF-Format direkt in ihre Anwendung zu integrieren. Der Name der Bibliothek steht für die beiden Haupteinsatzbereiche in der Anwendung von Drittentwicklern oder Systemintegratoren:

- PDF Direct - ermöglicht die Erstellung von PDF-Dokumenten aus existierenden Dokumenten in beliebigen Dateiformaten (Konvertierung in das PDF-Format), die Erstellung von PDF-Dokumenten aus in einer Anwendung generierten Daten (Berechnungsergebnisse, Kontostände, Berichte usw.) sowie das Speichern solcher Dokumente als PDF-Datei oder in einer Datenbank
- PDF QuickView - ermöglicht das Laden eines PDF-Dokuments aus einer PDF-Datei oder aus einer Datenbank sowie die Darstellung der Dokumentenseiten oder von Metadaten in den Porgrammfenstern der Drittentwickler-Anwendung

Freeware: PDF Quick Reader – ein kostenloses Programm, mit dem PDF-Dateien geöffnet, angezeigt, signiert, gespeichert und ausgedruckt werden können.

9. soft Xpansion Smart Card Crypto Provider

Vor dem Hintergrund der rechtlichen Vorgaben (Signaturgesetz, Signaturverordnung) und eines in Zusammenarbeit von Vertretern aus allen betroffenen Bereichen erstellten Rahmenwerks für die Verwendung von digitalen Unterschriften werden schon seit längerem Softwareprodukte entwickelt, die bei der Verarbeitung digitaler Dokumente, zum Einsatz kommen. Die **Smart Card Crypto Provider**-Bibliothek ist ein solches Produkt. Sie erleichtert die Implementierung von digitalen Unterschriften in Geschäftsprozesse, ermöglicht die digitale Signaturen und Datenkodierung mit weit verbreiteten Smart Cards. Sie unterstützt die Signaturkarten wichtiger Hersteller wie Deutsche Post, D-Trust, TeleSec, sowohl für die Signierung von PDF-Dateien als auch für andere Zwecke, zum Beispiel für die Autorisierung von PC- und Netzwerkanwendern.

Die Verwendung von Smart Card-Zertifikaten für die Verschlüsselung und Entschlüsselung wird vereinfacht. Tiefer gehende Kenntnisse über die technischen Abläufe beim Unterzeichnen von Dokumenten sind mit der **Smart Card Crypto Provider**-Bibliothek nicht erforderlich.

Die Bibliothek kann schnell und mit geringem Aufwand mit einer Anwendung verknüpft werden. Über die Schnittstelle der Bibliothek wird das passende Zertifikat aus der Liste verfügbarer Zertifikate ausgewählt. Dabei erfolgt der Verschlüsselungs-/ Entschlüsselungsvorgang über die von Microsoft® für Programmierer zur Verfügung gestellte Verschlüsselungs-Applikations-Schnittstelle, die **„Crypto API"**.

Die Bibliothek unterstützt alle aktuellen Windows®-Plattformen: Windows® Vista, Windows® XP, Windows® Server 2003, Windows® 2000.

Die Bibliothek erfordert außer den installierten Hardwaretreibern, beispielsweise für das Kartenlese-Gerät, keine weiteren Komponenten. Sie kann mit allen Kartenlesern verwendet werden, die den PC/SC-Standard unterstützen.