Folge 6 von 8

Signet und die zweite Welle der Digitalisierung (als sie noch nicht so hieß; etwa 2004)

Eberhard von Faber

September 2019

Private und geschäftlicher Vorgänge elektronisch (am Computer) zu erledigen, daran haben wir uns heute schon gewöhnt – auch wenn jetzt erst (2019) die große Digitalisierung beginnen soll. Doch auch schon davor wurde Software im privaten und geschäftlichen Umfeld in großem Stil verwendet. Anfang der 2000er Jahre ermöglichte ein Produkt der Firma Adobe, elektronische PDF-Formulare direkt am Computer auszufüllen, abzuspeichern und natürlich zu versenden. Ich fand solcherart „intelligente Dokumente" ungemein praktisch, denn sie lösten eine Reihe von Problemen: Die oft aufwendige Schulung der Mitarbeiter für eine neue Software konnte weitgehend entfallen, wenn der Geschäftsprozess vorher mittels Papierformularen organisiert wurde, da die elektronischen Versionen absolut identisch aussehen konnten. Außerdem war es möglich, die eingegebenen Daten aus einem solchen Formular elektronisch auszulesen und zum Beispiel in eine Warenwirtschaftssoftware wie SAP zu übertragen. Damit konnten Firmen, die verschiedene Softwaresysteme verwenden, elektronisch miteinander kommunizieren und ihre Geschäftsprozesse medienbruchfrei miteinander verbinden. Dadurch könnten viel Papier und manuelle Tätigkeit eingespart werden, wie es das papierlose Büro und die Digitalisierung versprechen. Als Voraussetzung dafür müsste das Ganze natürlich sicher sein. D.h., Fälschungen der über das unsichere Internet übertragenen Formulare müssten erkannt und der Absender eindeutig identifizierbar sein. Deshalb mussten die PDF-Formulare von Adobe und weitere Office-Anwendungen wie E-Mail um Funktionen wie elektronische Unterschrift und Verschlüsselung erweitert werden. Und das sollte ein einfach zu bedienendes Produkt leisten, das am Ende „Signet" getauft wurde.

Das Folgende ist ein Anschauungsbeispiel dafür, dass die Integration einer harmlos aussehenden Sicherheitsfunktion wie der elektronischen Unterschrift weit mehr verlangt, als nur ein Stück Software mit dem Code der Kryptofunktion.[1] Das gilt insbesondere für ein Produkt für Endanwender. Der Artikel enthält keine firmeninternen Informationen. Alle Details in dem Fallbeispiel sind Stand der Technik oder gängige Praxis.

1 Goldgräberstimmung und das Signaturgesetz

In der IT-Sicherheit gilt, dass nichts stärker wirkt, als ein Gesetz. Natürlich hatten die Sicherheitsleute immer Angst, dass sich im potentiell unsicheren Internet kaum ein wirkliches Geschäft entwickeln würde. Jedenfalls dachten wir in den späteren 1990er Jahren so. Aber auch danach galt die mangelnde IT-Sicherheit als ein Grund für die schleppende „Digitalisierung", also die Nutzung von Software für Geschäfts- und Verwaltungsabläufe.[2] Um den Jahrtausendwechsel und Anfang der 2000er Jahre setzte man große Hoffnung in die elektronische Unterschrift (digitale Signatur), weil es eine gesetzliche Regelung gab. Das Signaturgesetz bestimmte über die Risikoverteilung bzw. stellte die Anbieter davon frei, wenn bestimmte Auflagen erfüllt waren. Das ist das, was Innovationen und wirtschaftliche Aktivität brauchen. Und so gab es viele

---

1 Für Fachleute: Kryptographie sichert zwar Daten, verlagert das Problem von Integrität und Vertraulichkeit aber auf die Schlüssel und erfordert daher ein entsprechendes Schlüsselmanagement. Das macht die Systeme häufig sehr kompliziert, auch wenn diese Funktionen wie im Fall „Signet" für den Anwender nicht auf den ersten Blick sichtbar sind.

2 Später gab es die gleiche Diskussion bezüglich „Cloud-Computing". Hier war die Unsicherheit bezüglich der IT-Sicherheit nachweislich ein Hemmschuh für die Verbreitung dieser Technologie.

Unternehmensgründungen, Projekte und natürlich zahlreiche pressewirksame Auftritte, um die neue Technologie bekannt zu machen.

Der Auslöser, warum ich mich damit beschäftigen sollte, hatte damit zu tun und war aber, wie fast immer, in der Suche nach Geschäftsmöglichkeiten begründet. Und dazu musste das Produkt einen wirklichen Mehrwert bieten (siehe Abb. 1).

CHIP AKTUELL

Adobe Acrobat

PDF als Killer-Applikation für digitale Signatur

Obwohl es längst Lösungen dafür gibt, war bei der elektronischen Signatur bislang nur Zögern und Abwarten angesagt: Behörden, Banken und erst recht Privatleute wollten davon nichts wissen. Adobe-Geschäftsführer Fritz Fleischmann hat dafür eine einfache Erklärung: „In den vergangenen Jahren hat hier eine Killer-Applikation oder ein universeller Client gefehlt." Trotz hoher Sicherheitsbedürfnisse habe sich keine der vorhandenen Lösungen durchsetzen können.

Die Kombination aus einem PDF-Dokument und der digitalen Signatur könnte das nach Adobes Vorstellungen bald ändern. Der kostenlose Acrobat Reader ist bereits weit verbreitet. Wäre das PDF-Dokument mit einer elektronischen Signatur versehen, könnte der Empfänger unter anderem feststellen, ob die Datei wirklich vom angegebenen Absender stammt und ob sie manipuliert wurde.

Neben dem sehr bekannten Dateiformat bietet Adobes Lösung den Vorteil, dass mit allen gängigen Smartcards eine digitale Signatur erzeugt werden kann. Nötig sind dafür ein Lesegerät und zusätzliche Software zum Signieren, die Openlimit liefert. Der Preis dafür ist noch offen.

T-TeleSelec Signet: Chipkarte, Lesegerät und Software im Paket von der Telekom. Preis: 130 Euro.

Derzeit erfüllen Adobes Acrobat und der Acrobat Reader die Anforderungen des strengen deutschen Signaturgesetzes nicht. Daran wird gerade gearbeitet: Die Sicherheitsevaluierung läuft; Adobe rechnet damit, dass das Bundesamt für Sicherheit in der Informationstechnik (BSI) bis Mitte des Jahres ein Zertifikat ausstellt, das eine so genannte qualifizierte digitale Signatur erlaubt – die dann rechtsgültig ist.

Auf dieses O.K. wartet auch die Telekom: T-Systems bietet bereits ein Komplettpaket für 130 Euro an, das dann per Upgrade auch die qualifizierte digitale Signatur für PDF-Dokumente bieten soll. Neben der Datensicherheit sind die Kosten ein Argument fürs digitale Signieren. Das Dokumenten-Management auf Papier kostet Verwaltungen und Industrie pro Formularvorgang 30 bis 60 Euro.

Info: www.adobe.de
www.openlimit.com

54 | CHIP | APRIL 2005

Abb. 1: Viele Hoffnungen

Aber wie verkauft man IT-Sicherheit? Das war damals schon nicht ganz einfach. Kunden erwarteten zu Recht, dass die Produkte, die sie kauften, sicher waren. Da war nicht viel Raum für Extras. Natürlich gab es Ausnahmen und reichlich wachsende Märkte auch im Bereich IT-Sicherheit. Betreiber mittlerer und großer IT-Infrastrukturen und IT-Anwendungen brauchten Sicherheitskomponenten für deren Absicherung wie z.B. Firewalls. Auch hatten sich alle Marktteilnehmer daran gewöhnt, Geld für einen Schutz vor Schadsoftware auszugeben und geschäftliche Anwender nutzten auch Verschlüsselungslösungen zur sicheren Datenübertragung. Was die Geschäftsführung wollte, war ein Massenprodukt – am besten für Konsumenten und kleine Gewerbetreibende, denn deren Zahl ist beträchtlich. Nun waren Ideen gefragt. Es genügte nicht, ein Produkt eines Herstellers etwas zu veredeln. Nur eigene Wertschöpfung oder Alleinstellungsmerkmale ermöglichen hohe Gewinnspannen. Ein IT-Sicherheitsprodukt für den PC von jedermann wäre dafür eine gute Wahl. Es fanden sich schnell Zulieferer, die als Mitstreiter äußerst hilfreich waren.

2 Die Idee: medienbruchfreier Workflow (mit Signatur)

Ende der 1990er Jahre war die Computertechnik allgemein verbreitet und deren Vernetzung soweit fortgeschritten, dass die Industrie die Automatisierung ihrer nun elektronischen Geschäftsprozessen massiv vorantrieb. Allerdings waren viele der Computeranwendungen im Wesentlichen auf eine Firma beschränkt bzw. auf diese zentriert. Das lag daran, dass (dem Client-Server-Paradigma folgend) die Anwendung (Software für die geschäftliche Anwendung) auf einem Server lag. Bestimmte Nutzer hatten die Möglichkeit, auf diese zentrale, auf dem Server befindliche Anwendung zuzugreifen. Dies entsprach dem damaligen Entwicklungsstand, hat sich aber bis heute oft nur unwesentlich geändert. Die Nutzer gehören in der Regel der Firma an, die die Anwendung entwickeln ließ bzw. zur Verfügung stellt und nutzt. Zusätzlich gibt es einzelne Nutzer, die Aufgaben bei Zulieferern, Partnern oder Kunden wahrnehmen. Doch das ist eher die

Ausnahme und ändert nichts an der Tatsache, dass die Anwendung auf eine Firma zentriert ist. Doch schon damals waren lineare, voneinander unabhängige Wertschöpfungsketten eher die Ausnahme als die Regel. Wertschöpfungs*netzwerke* waren in vielen Branchen schon damals das eher vorherrschende Modell. Und solche Netzwerke sind zum Teil sehr dynamisch. D.h., Kooperationen, Verträge und Projekte werden geschlossen, aber auch schnell wieder durch andere ersetzt. Dies betrifft aber nicht nur die Zulieferer, Partner oder Kunden „der Firma" selbst. Vielmehr ist „die Firma" auch Teil eines Wertschöpfungsnetzwerkes und z.B. Lieferant in einem anderen Netzwerk. Das bedeutet aber, dass dem Modell „*eine* Anwendung *einer* Firma mit mehreren festen Nutzern" Grenzen gesetzt sind.

Weil die Wertschöpfungskette nicht an der Unternehmensgrenze haltmacht, muss auch der elektronische Geschäftsprozess weiterreichen. Dieser ersten Einsicht muss eine zweite folgen. Der eben beschriebene Bezug auf eine Firma lässt sich nicht dadurch flexibilisieren, dass sich alle Mitstreiter auf eine zentrale Super-Anwendung einigen und diese nutzen. Dazu sind die Branchen und ihre Märkte zu dynamisch und viele Mitstreiter sind untereinander eben auch Konkurrenten. Die Digitalisierung, die damals e-Business hieß, versprach auch damals schon Wettbewerbsvorteile. Sonst hätte man sie nicht vorangetrieben. Was also war zu tun?

Lange bevor Computer Einzug hielten, wurden für die ersten standardisierten Vorgänge Formulare genutzt. Diese wurden von der Firma Adobe in elektronische Dokumente überführt, die am Computer ausgefüllt werden konnten, aber optisch ganz genau wie ihre papiernen Originale aussahen. Das erleichterte Umstieg und Einführung enorm. Und natürlich konnte der im elektronischen Formular gespeicherte Inhalt auch per Software ausgelesen und z.B. in SAP übertragen werden. Wenn sich die Systeme bzw. Anwendungen der beiden Vertragspartner verstanden, also die gleiche Daten- bzw. Formularstruktur verwendeten, konnte der Arbeitsablauf medienbruchfrei erfolgen. D.h., der Absender befüllte ein elektronisches Formular des Empfängers und der Empfänger extrahierte die Daten des Absenders nach Prüfung des Formulars. Doch da lag das Problem: Denn auf dem Kommunikationsweg lag das potenziell unsichere Internet.

Hier kommen die IT-Sicherheit und die Chipkarte ins Spiel.

3 Adobe integriert die elektronische Signatur mittels Chipkarte

Die Idee mit den Formularen war gut. Aber die Software wurde von der US-amerikanischen Firma Adobe hergestellt. Wir versuchten also, Adobe mit ins Boot zu holen. Es war nicht nötig, Adobe von der digitalen oder elektronischen Signatur zu überzeugen. Sie hatten diese ja selbst integriert. Wir wollten aber die gesetzliche, rechtssichere digitale Signatur haben. Und hier waren deutsche bzw. europäische Auflagen zu erfüllen, deren Erfüllung mit erheblichen Investitionen und Folgekosten verbunden waren.

Die USA waren weit weg und US-amerikanische Firmen sahen die Welt aus ihrer Perspektive. Da gab es keine gesetzliche, rechtssichere digitale Signatur. Ich hatte zwei Termin mit dem Geschäftsführer von Adobe, bei denen es darum ging, welche Bedeutung die Gesetzgebung in Deutschland bzw. Europa für Adobe hat. Eines der Anwendungsbeispiele war das folgende: Für den Nachweis der ordnungsgemäßen Entsorgung von gefährlichen, überwachungsbedürftigen Abfällen sind bis zu sieben rechtsverbindliche Unterschriften erforderlich. Die Nachweise müssen weitergegeben und archiviert werden. Die Folge ist Papier mit zum Teil sechs Durchschlägen, ein hoher Aufwand für Abfallerzeuger, Abfallbeförderer und Abfallentsorger. Mit Adobe-Formularen und der gesetzlichen, rechtssicheren digitalen Signatur geht das viel besser.

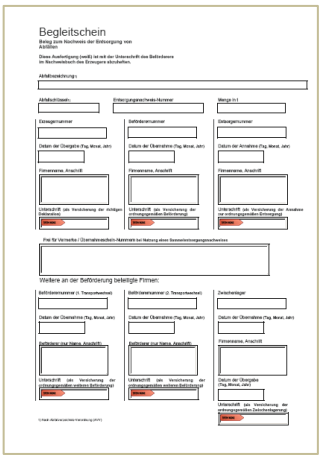
Begleitschein

Abb. 2: Entsorgungsnachweis

Eine andere, einfachere technische Lösung ist nicht möglich, aufgrund nationaler Regelungen und dem Recht der Europäischen Union. Abb. 2 zeigt den digitalen Entsorgungsnachweis, den man am Ende rechtssicher digital unterschrieben konnte.

4 Die „Story“ für den Anwender

Es ist erwähnt worden, dass das zu entwickelnde Produkt einen möglichst großen Anwenderkreis haben sollte. Deshalb mussten andere Anwendungen auch für den Privatkunden her. Viele Voraussetzungen existierten dafür schon. Viele Emailprogramme unterstützten bereits die Schnittstelle S/MIME für die Integration von Verschlüsselung und Signatur. Es mussten nur noch die entsprechenden Softwarekomponenten geschaffen werden. Dafür gab es Partnerfirmen, die dies bewerkstelligten. Eine weitere Herausforderung war es, alle Komponenten zur Zulassung für die rechtssichere Version der digitalen Signatur zu führen, die im Rechtsdeutsch „qualifizierte“ elektronische Signatur bzw. Unterschrift heißt. Eine vom Gesetz geforderte zusätzliche Software war die Anzeigekomponente („Viewer“). Man sollte ja genau das angezeigt bekommen, was man dann rechtsgültig unterschrieb.

Abb. 3 zeigt drei Anwendungsgebiete, die Signet unterstützte. Sichere Email und elektronische Formulare sind bereits erwähnt worden. Über die Windows-Druckfunktion konnte man Dateien erzeugen, die auch digital signiert oder verschlüsselt wurden. Das gleiche funktionierte im Windows-Explorer (Dateimanager). Eine Zugabe war die Anwendung „elektronischer Leitzordner“, bei dem es sich um das Softwarepaket ELO Office handelte. Dies war ein vollständiges Dokumentenmanagementsystem samt Archivierung.

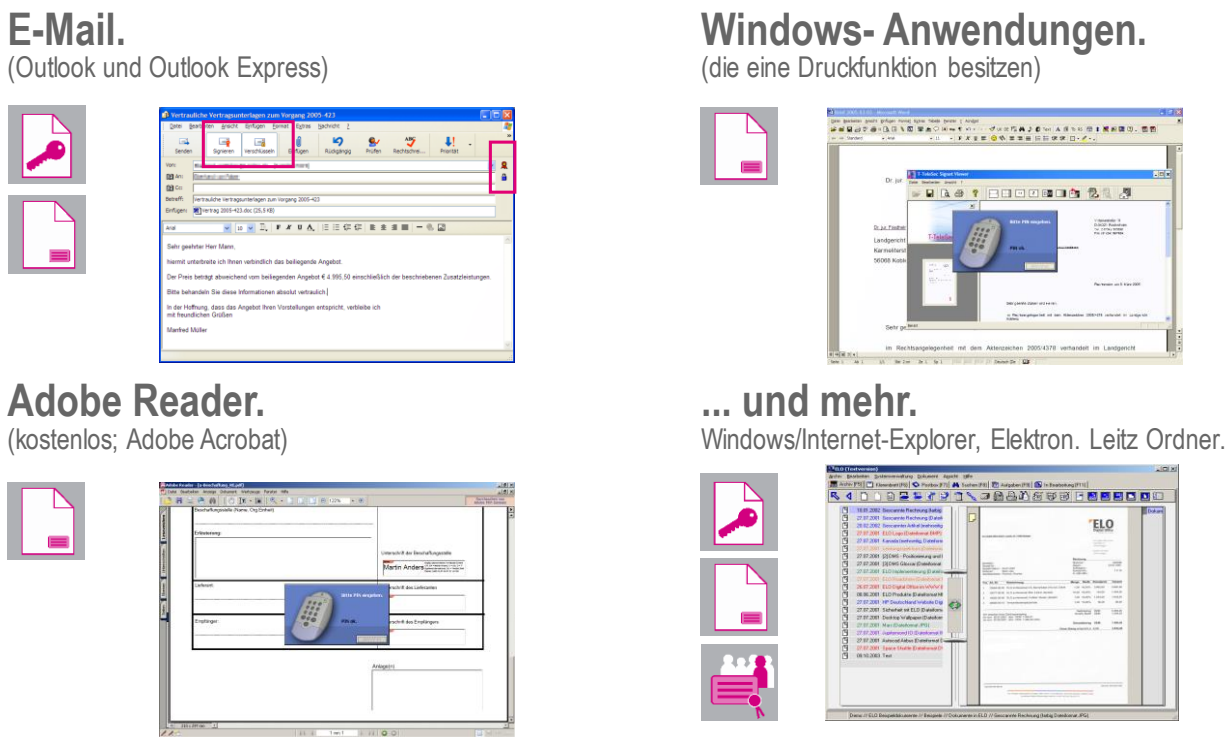

Abb. 3: Desktop-Anwendungen für Verschlüsselung, Signatur und Authentifizierung (siehe Icons)

Ein Hauptproblem des Produktes bestand darin, dem Anwender die Funktionalität und ihren Effekt nahezubringen. Signatur und Verschlüsselung sind nicht unbedingt für jeden sofort verständlich. Noch heute wird der Weg zur Verbreitung für viele dadurch versperrt, dass Begriffe wie Zertifikat und privater Schlüssel verwendet werden. Manchmal wird den Anwendern auch Kryptographie zugemutet. Das musste man anders machen. Wenn jemand eine Camping-Kühlbox kauft, wird ihm auch nicht erklärt, wie ein Peltier-Element funktioniert.

Doch ganz ohne ein Verständnis der Technologie geht es auch nicht. Das kleine Handbuch, dass ich geschrieben habe, hat etwa 60 Seiten und erklärt Installation und Nutzung ganz ohne Rückgriff auf Kryptographie. Erst im Anhang (Glossar) gibt es die Einträge „RSA“ und „Schlüsselpaar“, damit die technisch Vorgebildeten sehen können, dass Signet wie alle derartigen Lösungen auf dem RSA-Algorithmus und einer Public-Key-Infrastructure (PKI) aufbauen.

Die Erklärung von „PKI ohne Kryptographie“ basiert für die Signatur auf der Darstellung in Abb. 4. Man muss ja wissen, wann man die Chipkarte braucht und wann irgendwelche Daten (über den Ersteller) zu kontrollieren sind.

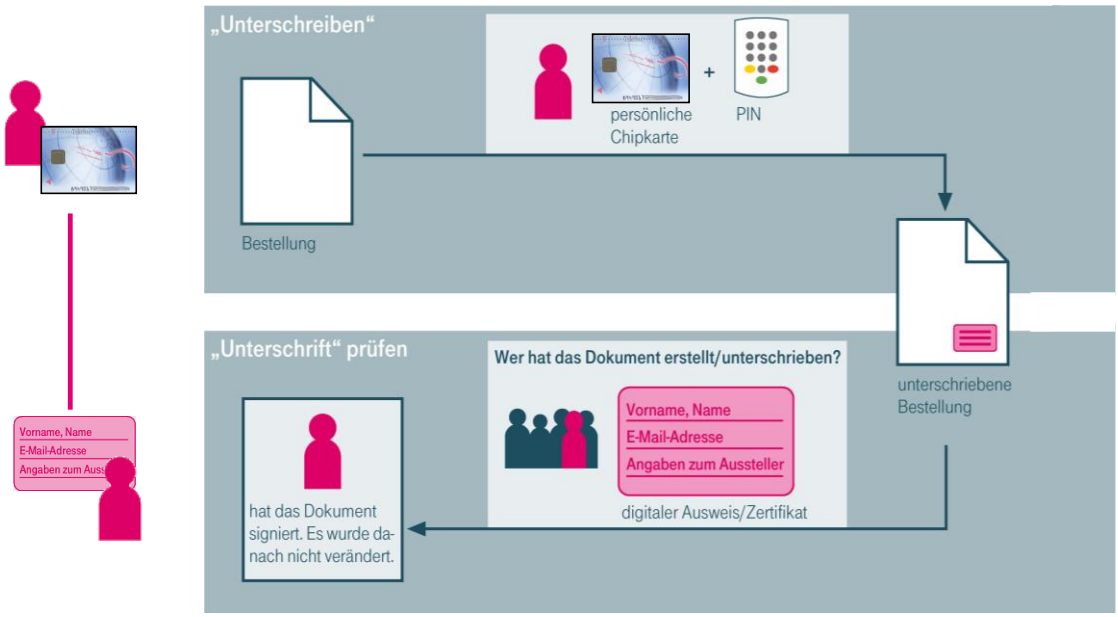

Abb. 4: Basistechnologie digitale Signatur: Integritätsschutz und Autorisierung einer Nachricht

Die Beschreibung hebt darauf ab, dass für den kritischen bzw. zu schützenden Vorgang immer die Chipkarte und die PIN benötigt werden. Bei der Anwendung „Unterschreiben/Signatur“ ist es die Erstellung der Signatur, die ja fälschungssicher sein soll. Bei der Anwendung „Verschlüsselung“ geht es darum, dass nur der berechtigte Empfänger in der Lage sein darf, den verschlüsselten Inhalt zu entschlüsseln. Deshalb muss nun der Empfänger die Chipkarte und die PIN einsetzen. Dieser Vorgang ist in Abb. 5 dargestellt.

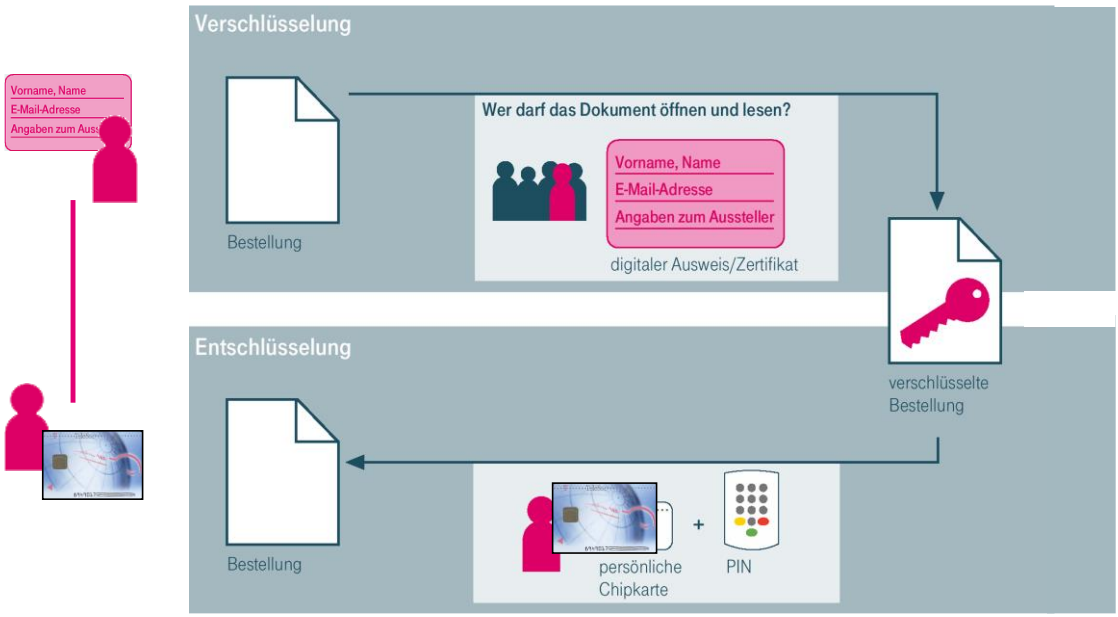

Abb. 5: Basistechnologie Verschlüsselung: hocheffizient und sicher durch kryptographische Verfahren

Den bei Fachleuten (leider) gebräuchlichen Begriff „Zertifikat“ habe ich durch „digitalen Ausweis“ ersetzt. Ein normaler Sichtausweis bestätigt, dass ein Name, eine Mitgliedschaft, ein Konto oder dergleichen (steht auf dem Ausweis) zu einer Person (sie ist abgebildet) gehört. Eine Behörde oder eine andere autorisierte Autorität bestätigt diesen Zusammenhang als Aussteller des Sichtausweises. Deshalb ist der Aussteller ebenfalls angegeben. Derjenige, der den Ausweis in Augenschein nimmt, kann für sich entscheiden, ob er dem Aussteller traut. Wenn nicht, ist der ganze Sichtausweis für ihn bedeutungslos und der Inhaber hat das Nachsehen. Die Parallelen zum digitalen Ausweis (Zertifikat) sind in unseren elektronischen Anwendungs-

fällen eklatant. Dieser Datensatz, den Windows oder eine andere Software anzeigt, bestätigt die Zugehörigkeit einer Person (Name, Email usw.) zu einer Chipkarte (Instrument für die Signatur und die Entschlüsselung).[3] Der Aussteller hat beides hergestellt. Ein Feld im digitalen Ausweis (Zertifikat) enthält den Namen des Ausstellers. Es ist dort auch angegeben, unter welche Voraussetzung die Chipkarte und der digitale Ausweis (Zertifikat) herausgegeben wurden und dass dazu eine Registrierung erforderlich war und wie diese abläuft und was im Einzelnen dabei geprüft wird. Auch bei einem Personalausweis und Reisepass (Sichtausweis) muss man sich ja beim Aussteller persönlich „registrieren“ (bzw. erfassen) lassen.

5 Marktforschung: Fokusgruppen

Aber werden die geschäftlichen und privaten Anwender diese Story verstehen? Werden sie den Nutzen verstehen und als den ihren ansehen? Werden sie Geld dafür auszugeben bereit sein? Werden sie in der Lage sein, das Produkt sachgerecht zu verwenden? Welches sind die möglichen und erfolgversprechenden Vertriebswege? Das alles sind Fragen, die man beantworten muss, bevor man hoffnungsfroh investiert und ein Produkt auf den Markt bringt. Ist also unser Produkt mit der Signatur von PDF-Formularen die erhoffte „Killer-Applikation“ (Abb. 1), die der Technologie und dem Geschäft damit zum Durchbruch verhilft?

Die Antworten müssen die klassischen Methoden der Marktforschung liefern. Man nutzt eine Marktforschungsagentur, die sogenannte Fokusgruppenbefragungen durchführt. Sie wählt eine Gruppe von Endverbrauchern und eine Gruppe von Gewerbetreibenden, denen Signet in deren Räumlichkeiten in der Münchner Innenstadt vorgestellt wird. Dabei kann ich durch einen halbdurchlässigen Spiegel beobachten, wie der Leiter des Markttests Signet vorstellt, durch die Funktion führt und Fragen stellt. Nur einmal muss ich eingreifen, als irgendetwas nicht funktioniert bzw. der Vorführende nicht zurechtkommt. Das Ergebnis stimmt uns nicht euphorisch, aber die Marktforschungsagentur betont vor Ort und in ihrem Bericht, dass das Produkt gut aufgenommen und eindeutig nicht durchgefallen sei.

6 Umsetzung

Die Umsetzung ist aufwendiger und viel zeitraubender, als ich dachte. Zwar wird die Software von Partnerfirmen erstellt. Dennoch sind viele Abstimmungen notwendig. Es geht um Funktionen, Bedienfreundlichkeit, Gestaltung der Oberfläche, Firmenlogos, Rechte, Verträge, Kosten und vieles andere mehr. Ein weiteres großes Thema ist der Zeitplan. Insbesondere die für die Zulassung nach Signaturgesetz notwendigen Sicherheitsbegutachtungen erfordern viele Abstimmungen, denn nach der Begutachtung kann nichts mehr geändert werden.

Bei der Beschaffung der Chipkartenleser muss eine objektive Auswahl getroffen werden. Ein Hersteller wirft seinen Leser mit Wucht an die Wand, um mir die Robustheit des Gerätes zu demonstrieren. Auch bei der Auswahl des Lesers geht es um Kosten, Logos, Lieferzeiten u.v.a.m. Lieferzeiten können zu einem Problem werden, wenn das Produkt z.B., wie in der Branche üblich, zur CeBIT fertig und dort vorgestellt werden soll. Wurde das Produkt dort angekündigt, muss es in größeren Stückzahlen auch verfügbar sein.

Ein weiterer Aufgabenbereich beim „Produktmanagement“ für Signet umfasst die Erstellung von Verpackung, Bedienungsanleitung und Begleit- und Werbematerial sowie die eigentliche Herstellung und die Vertriebswege samt Logistik. Von der Bedienungsanleitung war schon die Rede; sie kann natürlich auch dann erst fertig sein, wenn die Software halbwegs stabil ist. Die Anleitung enthält ja zum Beispiel auch Screenshots und soll die Bedienung ja eingängig beschreiben und auf möglich Fallstricke hinweisen. Layout und Druck übernimmt bzw. organisiert eine beauftragte Agentur. Das gleiche gilt für die Verpackung (siehe Abb. 6) und die CD mit der Software. Aber Inhalte und die Texte muss ich entwickeln. Wir entwickeln vier

[3] Kryptographisch wird die öffentliche Komponente des Schlüsselpaars zugeordnet. Die zur öffentlichen Komponente gehörende private Schlüsselkomponente befindet sich auf der Chipkarte und kann vom Inhaber der Chipkarte, die durch eine PIN geschützt ist, verwendet werden.

Icons, die den Funktionalitäten des Produktes entsprechen. Alles muss außerdem bestimmten Konzernvorgaben entsprechen, damit das Produkt gleich als eines des Herstellers erkannt wird.

Abb. 6: Das fertige Produkt: Chipkarte, Leser, Handbuch, Software, Registrierung

Bezüglich der Verpackung muss noch ein zusätzliches Problem gelöst werden. Signet soll in den stationären Handel. Es wird befürchtet, dass Kunden das Produkt kaufen und dann zu Hause oder im Büro enttäuscht feststellen, dass sie es nicht gleich nutzen können. Diese Tücke liegt in der Natur von Signatur und Verschlüsselung, die ja nicht ohne den digitalen Ausweis auskommen. Dieser Datensatz liegt dem Produkt natürlich nicht bei, sondern wird nach der notwendigen Registrierung erst erzeugt. Und die Registrierung des Nutzers muss persönlich erfolgen – im Interesse einer hohen Sicherheit und weil es das Signaturgesetz so fordert. Auf diese Hürde muss der Kunde aufmerksam gemacht werden – vor dem Kauf. Wir entscheiden uns für eine kompliziertere Kartongestaltung. Man kann den vorderen Deckel wie bei einem Buch aufschlagen, ohne dass der Karton geöffnet werden muss. Hier sieht man die Chipkarte, und es gibt den Hinweis, wie die Chipkarte zur persönlichen Chipkarte des Nutzers wird und dass man dann einen digitalen Ausweis (Zertifikat) bekommt. Auf der rechten Umschlagseite steht eine Anleitung in vier Schritten: Registrierung des Anwenders/Kunden, Erstellung des digitalen Ausweises beim Trust Center und Installation des Produktes sowie Laden des digitalen Ausweises durch den Anwender/Kunden. Dadurch dass Chipkarte herausnehmbar in der vorderen Klappe untergebracht ist, kann die Registrierung beim Händler erfolgen, ohne dass alles ausgepackt werden muss.

Das führt uns zu einem „unsichtbaren“ Teil des Produktes, den Trust-Center- oder PKI-Services. Dazu gehören Erzeugung der Schlüsselpaare, Herstellung der Chipkarten, Verarbeitung der Registrierungsdaten sowie Erstellung und Versand des digitalen Ausweises. Hinzu kommen Sperrfunktionen mit entsprechenden Internet-Auskunftsdiensten über die Gültigkeit bzw. Sperre der digitalen Ausweise. Letztere haben ähnlich wie die meisten Sichtausweise eine Gültigkeitsdauer und müssen nach Ablauf erneuert werden. Werden sie gesperrt, weil z.B. ein Missbrauch zu befürchten ist, so muss die Software vor der Verwendung prüfen können, ob der digitale Ausweis noch gültig ist. Außerdem gibt es ein Teilnehmerverzeichnis, in dem man ähnlich wie in einem Telefonbuch nachschlagen kann, um den digitalen Ausweis eines Teilnehmers zu bekommen. Auf diese Weise kann man ad-hoc einem Teilnehmer eine verschlüsselte Nachricht schicken und prinzipiell ist jeder Teilnehmer in der Lage, elektronische Unterschriften (Signaturen) jedes Teilnehmers zu prüfen. So wird die sichere Kommunikation im Internet optimal unterstützt.

Ich habe später selbst Testkäufe gemacht bzw. versucht, um festzustellen, vor welchen Problemen ein Kunde steht und wie ihm geholfen wird. Aber der Verkauf bzw. die dafür notwendigen Informations- und Werbematerialien mussten auch erstellt werden. So habe ich Flyer getextet und drucken lassen, Pressemitteilungen

geschrieben und verteilt, Handreichungen (für Vertriebsmitarbeiter) und Präsentationen (für Geschäftskunden) erstellt und vieles andere mehr.

7 Der Erfolg hat viele Gesichter

Die CeBIT im März 2004 vor voll mit „Signet“, so kam es mir jedenfalls vor. Alle beteiligten Partnerunternehmen einschließlich Adobe zeigten das Produkt auf ihren Ständen. Es gab viele Termine, Fotos und Urkunden. – Die aus Sicht der beteiligten Unternehmen wichtigste Urkunde ist die Bestätigung, dass Signet die Anforderungen des Signaturgesetzes erfüllt.

Das Ganze war für mich keine reine „Produktmanagementaufgabe“. Irgendwie war ich in vielen Bereichen zugleich Auftraggeber, Entwickler, Gestalter, Vermarkter usw. Viel musste bzw. habe ich selbst gemacht. Aber am Ende waren es all die großartigen Partnerfirmen und ihre engagierten Vertreter, die dieses Unterfangen zum Erfolg geführt haben. Manche, aber nicht alle Logos findet man auf der Verpackung des Produktes.

Über den „Produktmanager“

Spätestens nach Erreichen des Teenager-Alters habe ich angefangen, elektronische Geräte zu „basteln“. Anfangs half mein Vater mit Bauplänen, oder ich nutzte Bausätze. Doch schon bald stand die Entwicklung eigener Geräte im Vordergrund. Schon früh war mir klar, dass ich Elektrotechnik studieren und dann in der Forschung und Entwicklung (F&E) arbeiten wollte. Allerdings hat mich auch die Physik interessiert, so dass ich beides studierte und danach auf dem Gebiet der Theoretischen Physik promovierte. Danach ging ich in die Industrie und arbeitete dort fortan auf dem Gebiet der IT-Sicherheit in sehr unterschiedlichen Bereichen und mit unterschiedlichen Verantwortlichkeiten. Die Entwicklung von Signet fällt in die Zeit, in der ich als Stabsleiter der Geschäftsführung für Strategie und Geschäftsentwicklung verantwortlich war. Heute entwickle ich für einen großen IT-Konzern Methoden, Prozesse und Standards zur Absicherung einer großtechnischen, weit verteilten und komplexen IT-Produktion.

Bildnachweis: Quelle für Abb. 1 ist die Zeitschrift Chip. Alle anderen Abbildungen können mit Hilfe des Produktes T-TeleSec Signet der Firma T-Systems gewonnen werden.