Zeitschrift: Comtec : Informations- und Telekommunikationstechnologie = information and telecommunication technology

Herausgeber: Swisscom

Band: 78 (2000)

Heft: 5

Artikel: Sicherheit und Nachweisbarkeit im E-Commerce

Autor: Keller, Peter

DOI: https://doi.org/10.5169/seals-876437

Exploration Programmes:
Corporate Technology Explores Future Telecommunications

Sicherheit und Nachweisbarkeit im E-Commerce

Ein hoher Grad an Sicherheit bei EDV-Infrastrukturen und Kommunikationskanälen (Internet) sowie eine hohe rechtliche Beweislage von elektronischen Aktionen und Transaktionen sind Grundbedingungen für die Verbreitung von E-Commerce. Durch die heute einsetzbaren Sicherheitsmechanismen und -elemente sowie durch die Beanspruchung von diversen sicherheitsbezogenen Diensten wird ein genügend hoher Grad an Sicherheit erreicht. Die rechtliche Beweislage von elektronischen Verträgen oder Transaktionen ist unter Verwendung von hochwertigen digitalen Signaturen und Zeitstempeln nicht schlechter als bei Papierverträgen mit handschriftlichen Unterschriften. Der Artikel erläutert ausserdem ein paar spezielle Sicherheitsaspekte bezüglich der Langzeitarchivierung von elektronischen Dokumenten und des Erhalts des Beweiswerts von digitalen Signaturen über lange Zeit hinweg.

Das Explorationsprogramm «Cards and Security»
- erarbeitet Konzepte für neue Sicherheitsprodukte und Produkte mit hohen Sicherheitsanforderungen wie beispielsweise Finanztransaktionsdienste und
- leistet einen Beitrag dazu, dass Verluste durch Sicherheitslücken verhindert werden und dass die Kosten durch sichere Prozesse gesenkt werden können.

Mit ihren Explorationsprogrammen erforscht Corporate Technology Telekommunikationstechnologien und neue Dienstmöglichkeiten mit einem Langzeitfokus von zwei bis fünf Jahren. Zudem erlaubt das in diesen Aktivitäten aufgebaute Wissen eine aktive Unterstützung von Innovationsprojekten der Geschäftseinheiten.

Das Explorationsprogramm «Security and Cards» verfolgt die Themen
- Schutz der Infrastruktur von Swisscom vor Attacken (Hacking), Missbrauch oder Betrug,
- neue sicherheitsbezogene Dienste,
- Untersuchung von neuen Sicherheitstechnologien wie Smart Cards oder biometrische Authentifikationsverfahren,

In der neuen «E-Economy» sind zuverlässige Telekommunikationsinfrastruktur und sichere Dienste eine Notwendigkeit. Die Sicherheit von Swisscom-Diensten und deren Schutz vor böswilligen Aktionen und Betrug sind deshalb von grossem Interesse. In diesem Zusammenhang stellt sich auch die Frage, wie das Potential von Smart Cards als Teil des Kundengateway für Finanztransaktionsdienste ausgebaut werden kann.

PETER KELLER, BERN

mit dem Ziel, Konzepte einerseits von Schutzmassnahmen und andrerseits von neuen Diensten zu erarbeiten.
Der vorliegende Artikel befasst sich mit demjenigen Teil des Explorationsprogramms, der die Konzeption von neuen sicherheitsbezogenen Diensten zum Inhalt hat. Die Ziele des Artikels sind das Aufzeigen der aktuellen Situation bezüglich Sicherheit und Verbindlichkeit des E-Commerce, die Sensibilisierung für die notwendigen neuen Sicherheitsfunktionen und -dienste sowie das Aufzeigen von wichtigen Aspekten im Umgang mit den neuen Sicherheitsfunktionen. Im Vordergrund stehen sicherheitsbezogene und juristische Aspekte im Umgang mit Zertifikaten, digitalen Signaturen, Zeitstempeln und elektronischen Verträgen. Die dargelegten Sachverhalte wurden im Wesentlichen im Rahmen des Explorationsprojekts «Interdomain Trusted Third Party Services (ITS)» erarbeitet.

Ausgangslage und Sicherheitsanforderungen

Mehr und mehr Informationen werden statt auf Papier in elektronischer Form bearbeitet, gespeichert und übermittelt. Darunter befinden sich auch etliche vertrauliche oder schützenswerte Informationen, vor allem wenn es um E-Commerce geht. Diverse Routineabläufe, ob firmeninterne oder solche mit Partnern, Lieferanten oder Kunden, werden automatisiert und elektronisch abgewickelt. Der Umfang und die Arten von E-Commerce-Funktionen wachsen ständig und entwickeln sich von der einfachen Werbung, der Information, der Kontaktaufnahme und dem Einkaufen zu immer heikleren und komplizierteren Funktionen in der gesamten Wertschöpfungskette. Dabei werden vor allem mehr und mehr Business-to-Business-Prozesse elektronisch abgewickelt.
Es ist offensichtlich, dass in diesem Umfeld die Sicherheit, Verbindlichkeit und Beweisbarkeit von elektronischen Abläufen, Transaktionen und Informationen eine Bedingung ist. In Bild 1 sind die verschiedenen Aspekte zusammengefasst, die entweder einzeln oder zusammen erfüllt sein müssen.

Sicherheitsbasisfunktionen

Die Gesamtsicherheit eines Systems oder Systemverbunds hängt immer von der Sicherheit der einzelnen Elemente ab. Darum müssen sowohl die Infrastruktu-

Die Aspekte der Informationssicherheit auf einen Blick

«Sicherheit» ist ein Überbegriff und bezieht sich jeweils auf einen oder mehrere der folgenden Sicherheitsanforderungen:
- Vertraulichkeit: Gewissheit, dass übermittelte oder gespeicherte Informationen nur von befugten Personen, Maschinen oder Computerprozessen gelesen werden können.
- Authentifikation: Erlangen der Gewissheit, dass der Kommunikationspartner auch wirklich derjenige ist, für den er sich ausgibt.
- Authentizität: Gewissheit bezüglich des Ursprungs einer Information oder bezüglich ihres Wahrheitsgrades.
- Integrität: Gewissheit, dass einer Information bei der Übertragung oder Speicherung nichts hinzugefügt, nichts gelöscht und nichts verändert wurde.
- Beweisbarkeit bzw. Nichtabstreitbarkeit: Die Fähigkeit, eine bestimmte Aktion oder einen bestimmten Sachverhalt über eine gewisse Zeit hinweg beweisen zu können oder, vom anderen Standpunkt aus gesehen, nicht abstreiten zu können. Der Grad der Beweisbarkeit einer Aktion oder eines Sachverhalts definiert den Beweiswert.
- Verfügbarkeit: Die Zeitspanne, während der auf Informationen oder Funktionen zugegriffen werden kann, oder die Geschwindigkeit, mit der auf Informationen oder Funktionen zugegriffen werden kann.

Wichtig zu bemerken ist, dass es 100%ige Sicherheit nicht gibt (wie in unserer physikalischen Umwelt) und dass Sicherheit immer relativ ist, das heisst, dass es wenig Sinn macht zu sagen, «es ist sicher». Präziser ist, «bezüglich dieses Sicherheitsaspektes ist es sicher bis zu diesem Grad».

Bild 1. Was bedeutet Informationssicherheit?

ren aller beteiligten Partner adäquat geschützt werden wie auch die diversen Kommunikationskanäle zwischen den Partnern. Die *Zugriffskontrolle* ist ein Mechanismus zur Sicherstellung der Vertraulichkeit, Integrität und Verfügbarkeit von Informationen. Dabei können verschiedene *Authentifikationsmittel* eingesetzt werden wie Passwörter, Secur-ID, Streichlisten, Public-Key-Verfahren oder biometrische Erkennungsmerkmale wie Fingerabdrücke, Augenbilder oder Stimmen.

Viele heute eingesetzte und die meisten neu entwickelten Sicherheitsfunktionen basieren auf *kryptografischen Mechanismen.* Bei *symmetrischen Algorithmen* wird für die Ver- und Entschlüsselung derselbe Schlüssel verwendet, der darum vorgängig zwischen den beiden Kommunikationspartnern auf eine sichere Art und Weise ausgetauscht werden muss. Bei *asymmetrischen Algorithmen* werden für die Ver- und Entschlüsselung je verschiedene Schlüssel verwendet: Die beiden Schlüssel, Public und Private Key genannt, bilden ein Schlüsselpaar und sind komplementär zueinander. Dabei bleibt der Private Key immer geschützt im Besitz seines Inhabers, wogegen der Public Key frei verteilt wird. Asymmetrische Algorithmen werden darum auch Public/Private-Key-Verfahren genannt. Der interessierte Leser findet detailliertere Grundlagen dieser Mechanismen in [1] bis [4], im Intranet oder im Internet.

Bild 2. Inhalt des Schlüsselzertifikats.

Verschlüsselung

Die wichtigsten Anwendungen kryptografischer Mechanismen sind die Verschlüsselung von Daten und die Herstellung und Überprüfung von digitalen Signaturen. *Verschlüsselung* ist ein Mittel zum Erreichen der Übertragungsvertraulichkeit oder der Informationsspeicherung. Dabei werden die Daten so verändert, dass ein Nichtberechtigter, obwohl er eventuell auf sie zugreifen kann, die darin enthaltenen Informationen nicht herausdestillieren kann. Symmetrische Algorithmen sind ein nahe liegender Mechanismus für die Verschlüsselung, aber auch mit Hilfe von asymmetrischen Algorithmen (Public-Key-Verfahren) kann verschlüsselt werden. Dabei werden die Daten vom Absender mit dem Public Key des Empfängers verschlüsselt. Dieser muss also irgendwie Zugang zu diesem Public Key, der nicht sein eigener ist, haben. Dann wird die Meldung an den Empfänger gesendet. Nur dieser kann nun mit Hilfe seines Private Key, den nur er kennt, die Meldung entschlüsseln.

Digitale Signatur

Die wichtigste Anwendung von Public-Key-Verfahren ist die *digitale Signatur.* Sie ist ein Code oder eine Bitsequenz, die an die signierte Information angehängt wird. Sie wird mit Hilfe des Private Key des Signierenden hergestellt und mit Hilfe seines Public Key überprüft (umgekehrtes Public-Key-Verfahren). Nur der Signierende hat Zugriff auf seinen Private Key, was bedeutet, dass nur er die Signatur herstellen kann. Andererseits kann jeder, der Zugriff auf den Public Key des Signierenden hat, die Signatur überprüfen. Digitale Signaturen bewirken die Sicherstellung gleich dreier Sicherheitsanforderungen, nämlich der Authentifikation des Signierenden, der Integrität der signierten Informationen sowie der Beweisbarkeit des Ursprungs der signierten Information (z.B. Transaktionen, Meldungen oder Dokumente). Die digitale Signatur ist also eine sehr mächtige Sicherheitsfunktion. Allerdings ist nicht jede digitale Signatur automatisch von hoher Sicherheitsqualität, wie weiter unten erläutert wird.

Authentifikation

Public-Key-Verfahren können auch für die *Authentifikation* im Rahmen eines Log-ins oder einer Zugriffskontrolle verwendet werden. Dabei stellt der Authentifizierende im Rahmen eines Challenge-Response-Verfahrens sicher, dass der Authentifizierte im Besitz des zu seinem Public Key gehörenden Private Key ist. Wichtig zu bemerken ist, dass ein Inhaber eines Schlüsselpaares seinen eigenen Public Key gar nie selber braucht, sondern nur immer seinen Private Key. Den Public Key verwenden andere beim Versenden von für ihn verschlüsselten Meldungen, beim Überprüfen von seinen digitalen Signaturen oder beim Authentifizieren.

Schlüsselzertifikate

Schlüsselzertifikate (Public Key Certificates) sind elektronische Ausweise, ausgestellt durch eine Zertifizierungsstelle (Certificate Authority/CA), wobei der Unterschied zu herkömmlichen Ausweisen darin besteht, dass statt des Fotos und des Namens des Inhabers (wie bei einem Pass) der Public Key und der Name des Inhabers zertifiziert werden (Bild 2). Im Unterschied zur Identitätskarte ist ein Zertifikat öffentlich, das heisst, es kann frei verteilt und kopiert werden. Durch die digitale Signatur der CA sind Schlüsselzertifikate unfälschbar, das heisst, es ist nicht möglich, den Inhalt eines Zertifikats unbemerkt zu ändern. Darum braucht ein Zertifikat nicht speziell geschützt zu werden. Ein Zertifikat garan-

Bild 3.
Inhalt der Zertifikatssperrliste (Certificate Revocation List, CRL).

tiert die Authentizität des darin enthaltenen Public Key, das heisst, es garantiert die Identität des Inhabers des zum Public Key dazugehörigen Private Key. Die Identität des Zertifikatsinhabers wird dabei durch den im Zertifikat enthaltenen Namen bestimmt. So lösen Zertifikate das Problem, dass einem Public Key nicht anzusehen ist, wer der Inhaber des dazugehörigen Private Key ist. Schlüsselzertifikate vereinfachen darum die drei oben beschriebenen Anwendungen von Public-Key-Verfahren: die Authentifikation gegenüber einem System oder Netz, die Ver- und Entschlüsselung von Daten sowie die Herstellung und Überprüfung von digitalen Signaturen. Dabei ist es aus Sicherheitsgründen ratsam, dass derselbe Inhaber für jede Funktion ein separates Schlüsselpaar und ein separates Zertifikat verwendet. Ein Inhaber kann also mehrere Zertifikate für verschiedene Zwecke haben. Allerdings gibt es erst wenige Produkte, die dies auch unterstützen – die meisten Produkte verwenden dasselbe Zertifikat für alle drei Funktionen.
Es kann vorkommen, dass ein Zertifikat revoziert (aufgehoben) werden muss. Dann nämlich, wenn der dazugehörige Private Key geknackt wurde, wenn der Inhaber die Rechnung für das Zertifikat nicht zahlt, wenn ein Mitarbeiter seine Firma verlässt oder wenn die Angaben im Zertifikat geändert haben (z.B. bei Heirat). Oder es muss suspendiert werden (temporär gesperrt), weil ein Verdacht auf ein Problem besteht. Im Unterschied zur Suspendierung wird eine Revozierung nicht rückgängig gemacht. Ein suspendiertes oder revoziertes Zertifikat wird von der CA in eine *Sperrliste* (Certificate Revocation List, CRL) eingefügt (Bild 3). Die CRL ist wie ein Zertifikat unfälschbar, was deren Veröffentlichung und Verteilung ohne zusätzliche Schutzmassnahmen erlaubt. Wird eine Suspendierung eines Zertifikats rückgängig gemacht, so wird dessen Seriennummer in der nächsten Ausgabe der CRL wieder entfernt. Revozierte Zertifikate bleiben bis zum Zeitpunkt des Ablaufs des Zertifikats in der CRL enthalten. Dann werden deren Seriennummern aus der CRL entfernt. Statt eine CRL herauszugeben, kann eine CA den Revozierungs- oder Suspendierungsstatus ihrer Zertifikate auch online zur Verfügung stellen.
Die Überprüfung eines Zertifikats umfasst mehrere Aspekte:

- Die darin enthaltene digitale Signatur der CA muss überprüft werden.
- Es muss geprüft werden, ob das Zertifikat noch gültig, das heisst, ob es nicht bereits abgelaufen ist.
- Es muss kontrolliert werden, ob das Zertifikat in der gerade aktuellen CRL enthalten ist.
- Der Überprüfer muss sich fragen, ob er der Organisation, die als CA auftritt, vertrauen will, dass sie auch wirklich den richtigen Public Key zertifiziert hat und dass ihr eigener Private Key gut geschützt ist. Dieses Vertrauen muss sich eine CA zuerst verdienen – durch Bekanntheit, durch Etablierung, durch Garantien, durch Sorgfalt, durch sichere und transparente Registrierungs- und Zertifizierungsprozesse, durch die kommunizierte Sicherheit ihrer Infrastruktur, durch Veröffentlichung ihres *Certificate Practise* Statements (CPS, Dienstbeschreibung) und durch Veröffentlichung ihrer *Certification Policy* (Reglement und Sicherheitsmassnahmen).

Zertifizierungshierarchien

Oft verwenden CAs so genannte *Zertifizierungshierarchien*, das heisst Systeme von sich zertifizierenden CAs, wobei zuoberst in der Hierarchie die Root-CA steht (Bild 4). Jede CA hat ihr Schlüsselpaar. Die Root-CA signiert (zertifiziert) den Public Key der unterstellten CA (subordinate CA) usw. Die End-User-CA schliesslich signiert den Public Key des End-User. Jede CA gibt dabei ihr eigenes CPS und allenfalls ihre eigene Certification Policy heraus und veröffentlicht ihre eigene CRL (oder stellt eine Validierungsschnittstelle zur Verfügung).

Querzertifikat

Ein *Querzertifikat* (Cross Certificate) ist ein Zertifikat für einen Public Key einer anderen CA. Das heisst eine CA garantiert für die Authentizität des Public Key einer anderen CA. So können sich CAs ein- oder gegenseitig zertifizieren. Auf diese Weise lassen sich auch Zertifikatshierarchien miteinander verknüpfen, was für einen Überprüfer von Vorteil sein kann, weil er nämlich nicht mehr darum besorgt sein muss, wie er über einen sicheren Kanal (bezüglich Integrität und Authentifikation) an den Public Key der «fremden» CA oder Root-CA gelangt. Diese Anforderung erfüllt das Querzertifikat selber. Querzertifikate werden heute zwar noch kaum verwendet, aber es ist möglich, dass sie in Zukunft häufiger vorkommen werden, sobald sich die diversen CAs etabliert haben werden und die Technologie so weit verbreitet sein wird, dass seitens

der Zertifikatsinhaber Druck auf die CAs ausgeübt wird, sich gegenseitig querzuzertifizieren.

Zertifikatskette

Eine *Zertifikatskette* ist eine Serie von Zertifikaten, von der akzeptierten CA des Überprüfers bis zum End-User-Zertifikat des Überprüften. Diese Ketten lassen sich auch über mehrere CAs oder Zertifizierungshierarchien aufbauen (Bild 5). Ein Überprüfer eines End-User-Zertifikats muss zusätzlich auch jedes einzelne Zertifikat in der Kette überprüfen, inklusive Überprüfung der Signaturen in den Zertifikaten und der aktuellen CRLs aller involvierten CAs. Insbesondere muss er sich fragen, ob er jeder einzelnen CA in der Kette vertraut. Auf gewisse Schritte in diesem Prozess kann dabei allerdings verzichtet werden, wenn der Überprüfer das End-User-Zertifikat oder gewisse CAs in der Kette bereits einmal überprüft und die Gewissheit hat, dass End-User-Zertifikate und CA-Zertifikate seit der letzten Prüfung nicht manipuliert worden sind und nicht suspendiert oder revoziert wurden. Diese Prinzipien gelten für einen Überprüfer von digitalen Signaturen genau gleich wie für den Absender einer vertraulichen Meldung oder für einen Authentifizierenden. Alle müssen den verwendeten Public Key mittels der Überprüfung der Zertifikatskette authentifizieren.

Zeitstempel

Ein *Zeitstempel* wird unter eine bestimmte Information gesetzt und enthält eine digital signierte, korrekte und präzise Zeitangabe, wobei die zeitgestempelte Information mit signiert wird (Bild 6). Ein Zeitstempel besteht also im Wesentlichen aus zwei Komponenten: der Zeitangabe und der digitalen Signatur des Erstellers des Zeitstempels (Zeitstempeldienst). Zeitstempel bewirken den Nachweis des Zeitpunkts einer Transaktion, einer Aktion, des Abschlusses eines Vertrags oder der Existenz eines Dokuments. Oft sind solche Zeitstempel nötig, weil Zeitangaben von Systemuhren entweder unpräzis sein können oder manipuliert werden können und darum relativ einfach bestritten werden können. Ausserdem sind Zeitstempel dort notwendig, wo der Beweiswert von digitalen Signaturen über längere Zeit hinaus erhalten bleiben soll, wie das beispielsweise bei elektronischen Verträgen der Fall sein kann.

Elektronischer Vertrag

Ein *elektronischer Vertrag* (ein Vertragsdokument in elektronischer Form) ist ein Dokument, das von beiden Vertragsparteien mit einem Zeitstempel versehen und dann digital signiert wird. Er besteht also im Wesentlichen aus dem Originaldokument, zwei Zeitstempeln und zwei digitalen Signaturen.
Sende- und Empfangsbestätigungen sind ein wichtiges Element, um den Versand oder den Erhalt von Transaktionen oder Meldungen zu einem späteren Zeitpunkt nachweisen zu können. Oder um sicherzustellen, dass die andere Partei den Versand oder Erhalt einer gewissen Transaktion oder Meldung nicht abstreiten kann. Der Beweiswert von solchen Bestätigungen kann um einiges erhöht werden, wenn sie mit den digitalen Signaturen von Sender bzw. Empfänger und der ransportdienstanbieterin sowie mit einem Zeitstempel versehen sind.

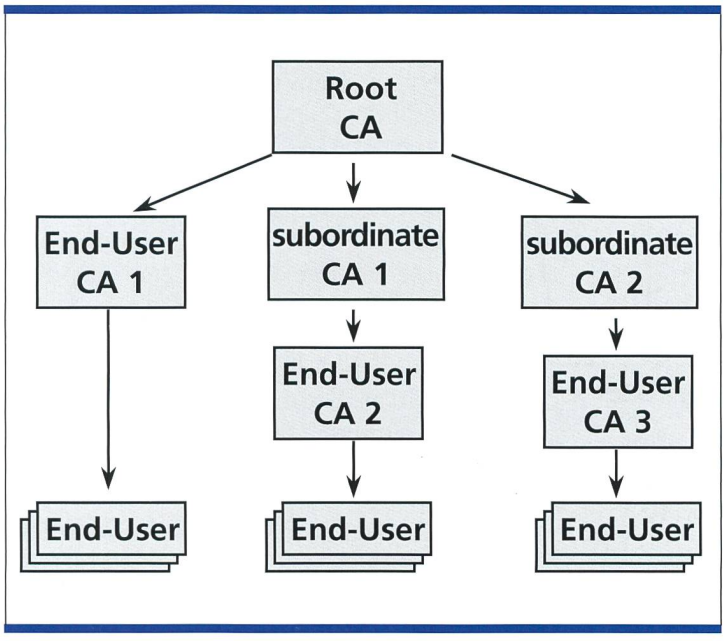

Bild 4. Zertifizierungshierarchien. Die Pfeilrichtung bezeichnet, wer wen zertifiziert, d.h. wer wessen Public Key signiert.

Attributzertifikat

Ein *Attributzertifikat* enthält ein bestimmtes Attribut des Inhabers eines Schlüsselzertifikats, das in Letzterem nicht vorkommt, weil es entweder zu kurzlebig ist oder weil es nicht als Identitätsmerkmal gilt. Ein solches Attribut ist beispielsweise eine Eigenschaft des Inhabers, wie dessen Alter, Zivilstand, Wohnort, Nationalität, Kreditwürdigkeit, Stimmberechtigung, Mitgliedschaft, usw. Oder das Attribut ist eine Zugriffsberechtigung auf bestimmte Daten oder Ressourcen. Das Attributzertifikat bestätigt also nicht wie das Schlüsselzertifikat die Identität des Inhabers, sondern die Richtigkeit der darin enthaltenen Informationen oder dient als Ticket für die Zugriffskontrolle. Es enthält immer eine eindeutige Referenz auf das zum Inhaber gehörende Schlüsselzertifikat (Bild 7). Das Attributzertifikat wird von einer Attribute Certificate Authority herausgegeben, das heisst, mit ihrem Private Key signiert. Die Attribute Certificate Authorities werden in der Regel von anderen Organisationen betrieben als von jenen, die die Rolle der CA einnehmen. So kann zum Beispiel eine Gemeinde als Attribute Certificate Authority für Wohnsitz- oder Zivilstandsangaben walten und eine Firma kann Tickets mit Zugriffsrechten für ihre Mitarbeiter und Handelspartner herausgeben. Allerdings werden Attributzertifikate zurzeit noch sehr wenig eingesetzt.

Sicherheitsdienste von Trusted Third Parties

Für einen effizienten und reibungslosen E-Commerce-Dienst sind neben den diversen Kommunikationsdiensten auch eine Reihe von sicherheitsbezogenen Diensten nötig, die von so genannten Trusted Third Parties (TTPs) angeboten werden. «TTP» ist ein Überbegriff und bezeichnet eine Stelle, an die die Teilnehmer gewisse sicherheitsbezogene Aufgaben delegieren (Bild 8). Eine TTP muss darum das Vertrauen der beteiligten Teilnehmer geniessen. Eine Firma oder Organisation, die als TTP auftritt, kann da-

bei auch mehrere TTP-Rollen gleichzeitig übernehmen.
Eine *Zertifizierstelle* (Certification Authority, CA) ist ein Beispiel einer TTP. Sie garantiert für die Echtheit von Public Keys und stellt zu diesem Zweck Schlüsselzertifikate aus. In der Schweiz besteht mit Swisskey eine solche CA (www.swisskey.ch).
Eine *Registrierstelle* (Registration Authority, RA) arbeitet mit der CA zusammen. Sie registriert und authentifiziert die Inhaber von Private Keys, die dann von der CA zertifiziert werden. In der Regel muss sich der Beantragende eines Zertifikats dabei persönlich bei der RA ausweisen (sonst hat das Zertifikat keinen hohen Sicherheitswert). Bei Firmenzertifikaten muss ein Vertreter der Firma persönlich erscheinen und einen Handelsregisterauszug vorweisen. Um dem Zertifikatsbeantragenden einen langen Weg zur RA zu ersparen, sollte die Stelle, die die Rolle der RA übernimmt, über ein geografisch verteiltes Netz verfügen. Als mögliche Kandidaten für die Rolle der RA bieten sich Bankfilialen, Postfilialen, Swisscom-Shops, Gemeinden oder andere verteilte Infrastrukturen an. In der Schweiz sind bis jetzt die Crédit Suisse, die UBS und die kantonalen Handelskammern als RAs für Swisskey tätig. Post, Swisscom und Handelsregisterämter sind ebenfalls im Gespräch. Im Ausland können Notare als RA für Swisskey beigezogen werden.
Da Zertifikate auch gesperrt werden können, muss jeder Überprüfer eines Zertifikats darum besorgt sein, jeweils in der aktuellen CRL der Zertifizierstelle nachzuschauen, ob das Zertifikat noch gültig ist. Oder er kann die Zertifizierstelle online über den Status des Zertifikats abfragen. Wenn verschiedene Zertifizierstellen im Spiel sind, kann dies allerdings recht mühsam sein. Abhilfe schafft hier ein *Validierungsdienst* für Schlüsselzertifikate, der die Statusinformationen von Zertifikaten verschiedener CAs zusammensucht (online oder über CRLs) und sie über eine einzige Schnittstelle dem Überprüfer online zur Verfügung stellt. Solche Validierungsdienstanbieter sind zurzeit allerdings noch rar.
Wie oben erwähnt sind Zertifikate öffentlich und können frei verteilt werden. Dies ist unter anderem dann nötig, wenn ein Absender einer vertraulichen Meldung diese für den Empfänger verschlüsseln will. Dazu muss er nämlich zuerst an dessen Zertifikat herankommen, weil er die Meldung mit dem Public Key des Empfängers verschlüsseln muss. Zertifikatsinhaber haben also ein Interesse daran, dass ihre Zertifikate so einfach wie möglich zugänglich sind. Eine effiziente Art, dies zu erreichen, ist, einen *Verzeichnisdienstanbieter* zu beanspruchen, der Zertifikate im Internet zur Verfügung stellt. Ein solches Verzeichnis sollte neben den Zertifikaten der Teilnehmer auch solche der Zertifizierstellen selber (CA-Zertifikate) sowie Querzertifikate (Cross Certificates) und CRLs enthalten. ETV als das grösste Verzeichnis in der Schweiz eignet sich hier gut als Anbieter. Entsprechende Pläne stehen zurzeit zur Diskussion.
Sicherheitselemente wie Zertifikate, Schlüssel, Sperrlisten usw. müssen unter Umständen über Jahre oder Jahrzehnte hinweg archiviert werden. Dann nämlich, wenn beispielsweise eine digitale Signatur noch nach Jahren überprüfbar sein soll oder wenn eine verschlüsselte Datei nach Jahren wieder entschlüsselt werden können muss. Dieses Bedürfnis kann ein *Archivdienst* erfüllen. Ein solcher Dienst kann nicht nur Sicherheitselemente speichern, sondern auch Dokumente,

Abkürzungen

CA	Certification Authority (Zertifizierstelle für Schlüsselzertifikate)
RA	Registration Authority (Registrierstelle einer CA)
TTP	Trusted Third Party (Anbieterin von Sicherheitsdienstleistungen)
CRL	Certificate Revocation List (Sperrliste von Schlüsselzertifikaten)
CPS	Certificate Practise Statement (Dienstbeschreibung einer CA)
PKI	Public Key Infrastructure (Überbegriff, der die Zertifizierstellenhierarchie, die verwendeten Zertifikate sowie die zum Umgang mit Zertifikaten notwendigen Zusatzverwaltungsfunktionen umfasst)
ETV	Elektronisches Teilnehmerverzeichnis (Dienst von Swisscom Directories)

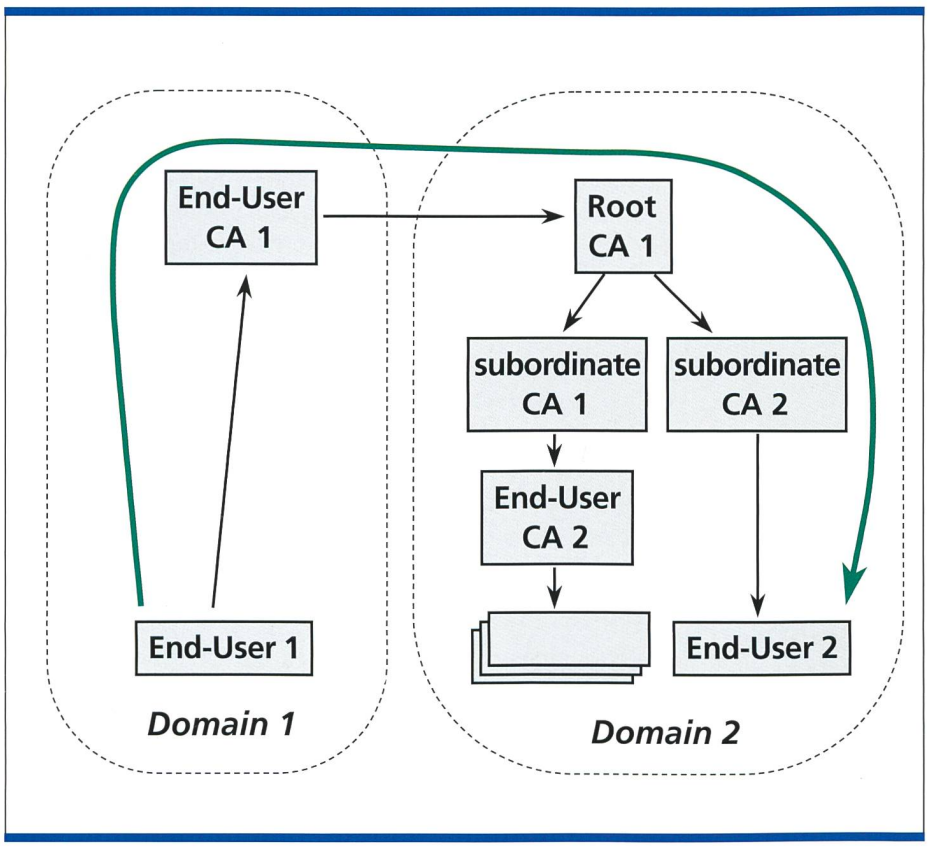

Bild 5. Zertifikatskette. Die Pfeilrichtung bezeichnet, wer wen überprüft.

Belege, Verträge oder Transaktionen. *Attributzertifikatsanbieter* können bestimmte Angaben über Inhaber von Schlüsselzertifikaten validieren und zertifizieren.
Bei vielen Geschäftsbeziehungen in der «Papierwelt» und im Verkehr mit Behörden spielen Notare eine wichtige Rolle. Um solche Dienste auch in der elektronischen Welt zur Verfügung zu haben, braucht es *Notariatsdienste*, die dieselben oder ähnliche Funktionen, wie sie heute auf Papier erbracht werden, auch elektronisch ausführen.
Um Transaktionen, Verträge oder Dokumente für die allfällige spätere Beweisführung korrekt und präzise zu datieren, ist ein von allen Beteiligten akzeptierter *Zeitstempeldienst* nötig (Zeitstempel siehe oben).
Die Herstellung und sichere Verwaltung von kryptografischen Schlüsseln ist eine relativ komplexe und heikle Aufgabe, für die nicht überall das notwendige Know-how vorhanden ist. Hier können verschiedene Schlüsselverwaltungsdienste einspringen. *Schlüsselgenerierungsdienste* generieren hochwertige kryptografische Schlüssel und verteilen sie auf eine sichere Art und Weise an ihre Inhaber. *Schlüsselhinterlegungsdienste* archivieren geschützte Kopien von Schlüsseln, sodass sie auch nach einem Verlust wiederhergestellt werden können. *Chipkartenpersonalisierungsdienste* speichern Schlüssel auf Chipkarten, wo sie bezüglich Zugriffssicherheit am besten aufgehoben sind.

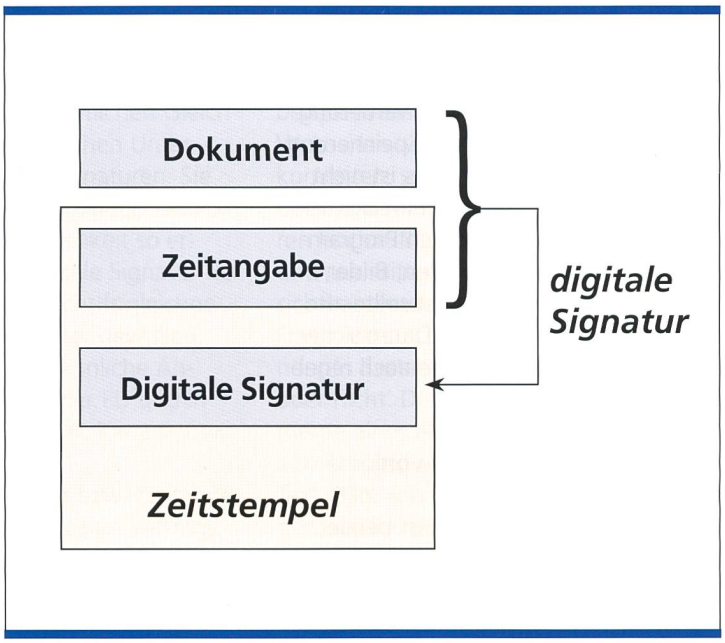

Bild 6. Inhalt und Herstellung eines Zeitstempels.

Qualität und Beweiswert von digitalen Signaturen, Zertifikaten und Zeitstempeln

Das neue elektronische Medium Internet bringt ausser der schnelleren Kommunikation und den neuen Möglichkeiten auch neue Gegebenheiten bezüglich Sicherheit, Verbindlichkeit, Nachweisbarkeit und Art der Beweisführung vor Gericht mit sich. Ein solcher Aspekt ist die sicherheitstechnische Qualität von digitalen Signaturen. Im Allgemeinen ist der Beweiswert einer digitalen Signatur umso höher, je höher auch deren technische Qualität ist. Diese hängt von einer ganzen Reihe von Punkten ab. Der wichtigste ist die Stärke der eingesetzten kryptografischen Mechanismen, das heisst konkret die Robustheit der Hashfunktion und des asymmetrischen Algorithmus sowie die verwendete Schlüssellänge und der Zufallsgrad des Schlüsselpaares. Weitere Punkte sind der Grad des Schutzes des verwendeten Private Key vor unerlaubtem Zugriff sowie der Grad der Gewissheit, dass der Signierende niemand anderem Zugriff auf seinen Private Key gab. Ausserdem darf der Signierende zu einem möglichst hohen Grad nicht abstreiten können, dass er zum Zeitpunkt der digitalen Signatur im Besitz des Private Key war.
Diese letzte Anforderung wird im Wesentlichen durch die Qualität des Schlüsselzertifikats erfüllt. Diese wiederum hängt einerseits von sämtlichen Qualitätsmerkmalen der digitalen Signatur der CA ab, also von denselben Merkmalen wie eben beschrieben. Andererseits hängt die Qualität eines Zertifikats auch wesentlich von der Qualität der angewendeten Registrier-, Identifikations- und Zertifizierungsprozesse der CA und RA ab. Hier sind vor allem die Methode und der Grad der Sorgfalt bei der Identifikation des Zertifikatsinhabers durch die RA ausschlaggebend sowie die Frage, wie sichergestellt wurde, dass diejenige Person, die von der RA identifiziert wurde, ein und dieselbe Person war, die sich als Besitzerin des Private Key ausgab.
Die Qualität von Zeitstempeln hängt ebenfalls von einer Reihe von Kriterien ab. Wiederum ist die Qualität der digitalen Signatur des Zeitstempeldienstanbieters sowie die Qualität von dessen Schlüsselzertifikat zu berücksichtigen. Das wichtigste Kriterium ist aber die Präzision und Manipulationssicherheit der verwendeten Uhr bzw. Uhren.

Langzeitarchivierung von elektronischen Dokumenten

Gewisse geschäftlich relevante Dokumente wie Buchungsbelege müssen in der Schweiz per Gesetz zehn Jahre lang aufbewahrt werden. Und auch sonst besteht der Bedarf, Informationen unter Umständen jahrzehntelang zu archivieren (Patientendaten, Geschäftsdokumente, Patentschriften, Zertifikate usw.). Dadurch dass die Informationen nun elektronisch statt auf Papier oder Mikrofilm vorliegen, müssen neue Aspekte berücksichtigt werden. Der erste ist die Verfügbarkeit der Informationen. Diese ist gleich in mehreren Punkten gefährdet. So kann beispielsweise ein invertiertes Bit auf einer Festplatte das ganze Dokument korrumpieren, das dann unter Umständen entweder gar nicht oder nur mit erheblichem Aufwand wieder hergestellt werden kann. Noch wahrscheinlicher sind aber Probleme mit Dateiformaten und Datenträgern, Probleme, die durch die rasante Entwicklung von Hard- und Software noch verstärkt werden. Wer ist heute noch in der Lage, Lochstreifen aus den 60er-Jahren, Magnetbänder aus den 70er-Jahren oder 5¼-Zoll-Disketten aus den 80er-Jahren zu lesen? Und auch wenn er es könnte, wer hat noch das richtige Programm, um die Datei im alten Format überhaupt öffnen zu können? Und selbst wenn sogar dies der Fall wäre, würde dieses alte Programm nur auf einem damaligen Betriebssystem laufen. Dieses wiederum läuft sehr wahrscheinlich auf der heute verfügbaren Hardware nicht mehr. Wir

sehen – die einzige Möglichkeit, ohne erheblichen Aufwand alte Dateien auch noch nach Jahrzehnten öffnen zu können, ist die regelmässige Konvertierung in aktuelle Formate und die Speicherung auf aktuelle Datenträger. Dies ist nicht immer einfach. Vor allem wenn Dokumente Elemente von anderen Programmen beinhalten, wie Grafiken, Bilder, Videos usw. Ein Archivdienst sollte also nicht nur bemüht sein, die Daten sicher aufzubewahren, sondern sie auch regelmässig konvertieren.

Bild 7. Inhalt eines Attributzertifikats.

Erhalt des Beweiswertes von digitalen Signaturen

Nicht nur die Verfügbarkeit ist bei der Langzeitarchivierung ein Thema, sondern auch die Erhaltung des Beweiswerts von digital signierten Dokumenten. Dieser Beweiswert wird nämlich im Verlaufe der Jahre immer schwächer, weil die zum Zeitpunkt der Signatur verwendeten kryptografischen Schlüssel und Algorithmen je länger, je unsicherer werden. Wenn ein Angreifer nämlich eine frisch erstellte digitale Signatur knacken will, dann ist das sicher sehr schwierig. Aber unter dem Aspekt der immer noch rasant wachsenden Rechenleistung von Computern ist es wahrscheinlich, dass er nach ein paar Jahren des ständigen Durchprobierens aller Möglichkeiten irgendwann zum Ziel kommt. Und dann ist der Beweiswert einer digitalen Signatur stark vermindert, weil deren Fälschungssicherheit unter anderem darauf basiert, dass nur der Inhaber des damals verwendeten Private Key die digitale Signatur herstellen konnte und niemand anders. Darum muss ein Signaturmechanismus (d.h. die Hashfunktion sowie der asymmetrische Algorithmus) so stark sein, dass er unter Berücksichtigung der wachsenden Rechenleistung während der gesamten Zeit von der Herstellung bis zur spätesten Überprüfung mit genügender Gewissheit nicht geknackt werden kann. Wenn also beispielsweise ein signiertes Dokument während zehn Jahren als Beweis dienen soll, so muss die verwendete digitale Signatur zehn Jahre lang halten. Aber selbst das ist nicht genügend. Denn um eine digitale Signatur nach zehn Jahren überprüfen zu können, müssen auch die dazugehörige, zehn Jahre alte Zertifikatskette des Signierenden, inklusive Root Zertifikat, sowie sämtliche zehn Jahre alten, zum Zeitpunkt der Signatur gültigen CRLs aller CAs in der Kette überprüfbar sein. Und da Zertifikate, CA-Zertifikate und CRLs ebenfalls digitale Signaturen enthalten, müssen auch diese Signaturen zehn Jahre lang halten. Das bedeutet aber auch, dass die Zertifikate und die CRLs zusammen mit dem signierten Dokument zehn Jahre lang aufbewahrt werden müssen. Aber dessen nicht genug. Weil nach zehn Jahren wahrscheinlich nicht mehr bekannt sein wird, unter welchen Bedingungen eine CA Zertifikate ausstellte und revozierte, ist es notwendig, auch alle CPS und Certification Policies sicher zu archivieren. Und es muss nach zehn Jahren Software vorhanden sein, die das zehn Jahre alte Signatur- und Zertifikatsformat noch behandeln kann. Digitale Signaturen und Zertifikate kann man nämlich im Unterschied zu Dokumenten nicht konvertieren – dies ergibt sich aus deren Natur. Und das signierte Dokument selber darf auch nicht konvertiert werden, ansonsten die Signatur nicht mehr stimmt – das Dokument wird ja durch die Konvertierung verändert, was bezogen auf die digitale Signatur als Integritätsverletzung gilt. Zu allem Übel muss schliesslich auch noch der Zeitstempel über all die Zeit hinweg sicher bleiben, was wiederum heisst, dass dessen digitale Signatur genügend stark sein muss, um die ganze Zeit durchzuhalten. Sämtliche Sicherheitsfunktionen müssen also so ausgewählt werden, dass deren Robustheit mindestens so lange anhält, wie die Funktionen überprüft werden sollen. Ein möglicher, aber etwas umständlicher Ausweg aus dieser Situation ist die periodisch erneuerte Signierung des Originaldokuments durch dessen Erstunterzeichner, inklusive seiner alten Signaturen, sowie allenfalls konvertierter Kopien des ursprünglichen Dokuments.

Diese Probleme bestehen mit Papier natürlich nicht, aber dafür andere, wie der hohe Platzverbrauch oder die begrenzte Dauerhaftigkeit auf Grund der Papierqualität.

Rechtlicher Stellenwert und Verbindlichkeit digitaler Signaturen und elektronischer Verträge

Der rechtliche Stellenwert von digitalen Signaturen in der Schweiz kann als gut bezeichnet werden. Da das Schweizer Gesetz mit ein paar ganz wenigen Ausnahmen die Formfreiheit für Verträge vorsieht, ist es den Vertragspartnern erlaubt, Verträge schriftlich, mündlich oder eben elektronisch abzuschliessen. Dabei können sie nach freiem Willen digitale Signaturen verwenden, um den Beweiswert eines Vertrags zu erhöhen. Obwohl

Referenzen

[1] Peter Keller, «Kryptographie und Trusted Third Parties», comtec 12/96

[2] Manfred Schmidt, «Kryptographie und Smart Cards», comtec 11/99

[3] SSH Communications Security, «Introduction to Cryptography», www.ssh.fi/tech/crypto/intro.html

[4] RSA Laboratories, «Frequently Asked Questions about Today's Cryptography», www.rsasecurity.com/rsalabs/faq/

die Gerichtspraxis diesbezüglich noch weitestgehend fehlt, gibt es keinen Grund, warum ein Gericht eine digitale Signatur nicht als Beweismittel zulassen sollte. Somit ergibt sich der Beweiswert eines elektronischen Vertrags im Wesentlichen aus dem Beweiswert der beiden im elektronischen Vertrag vorhandenen digitalen Signaturen sowie der darin enthaltenen Zeitstempel.

Es gibt zwar noch immer gewisse Rechtsgeschäfte, für deren Abschluss das Obligationenrecht die Form der Schriftlichkeit mit handschriftlicher Unterschrift erfordert (plus eventuell eine notarielle Beurkundung). Diese Geschäfte, darunter Grundstückkauf, Ehevertrag, Testament usw., sind aber für den E-Commerce von untergeordneter Bedeutung. Ausserdem bestehen zwei parlamentarische Motionen zur vollständigen rechtlichen Gleichstellung von handschriftlichen Unterschriften und digitalen Signaturen. Sie verlangen, dass die im Obligationenrecht vorgeschriebene Schriftlichkeit so ergänzt wird, dass die digitale Signatur der handschriftlichen Unterschrift gleichgestellt wird – natürlich unter gewissen Qualitätsbedingungen. Ähnliche Anstrengungen werden in der EU und in anderen Ländern wie USA, Kanada usw. unternommen.

Bezüglich Verbindlichkeit bzw. Zustandekommen eines elektronischen Vertrags gelten aber noch weitere Bedingungen als nur die technischen. Ein Vertrag ist eine von beiden Parteien bewusst gefällte übereinstimmende Willenserklärung. Damit dies der Fall ist, müssen alle signierenden Parteien Kenntnis vom gesamten Inhalt des signierten Dokuments genommen haben können. Dies ist in der elektronischen Welt eine hohe Anforderung, die unter Umständen nicht einfach zu erfüllen ist. So sind beispielsweise Signaturen, die ein System von sich aus im Versteckten tätigte, ohne dass der Vertragspartner darüber informiert wurde, wahrscheinlich nicht verbindlich. Es muss auch ausgeschlossen werden können, dass ein Virus oder ein Trojanisches Pferd auf dem Computer des Signierenden installiert war und diesem einen anderen Inhalt anzeigte als der effektiv signierte. Ausserdem können bestimmte Dokumentenformate versteckte Informationen beinhalten, wie beispielsweise Metainformationen in Webseiten, versteckte Texte in Word-Dokumenten, sehr stark verkleinerte Bild- oder Textelemente, die in einem grösseren hochauflösenden Bild versteckt sind und nur mittels starker Vergrösserung sichtbar werden usw. Damit stellt sich die Frage, ob solche versteckten Informationen als Bestandteil eines Vertrags gelten oder nicht. Der Beweiswert aller Elemente eines elektronischen Vertrags wird also erhöht, wenn einfache Formate für Text, Bild, Ton und Video verwendet werden, die keine versteckten Informationen enthalten können. Ausserdem muss glaubhaft gemacht werden können, dass die zum Zeitpunkt der Signatur verwendete Hard- und Software den gesamten Inhalt des Vertrags korrekt angezeigt hat. Somit kann ein elektronischer Vertrag dann als gültig betrachtet werden, wenn sowohl die erwähnten technischen Kriterien als auch die nichttechnischen erfüllt sind.

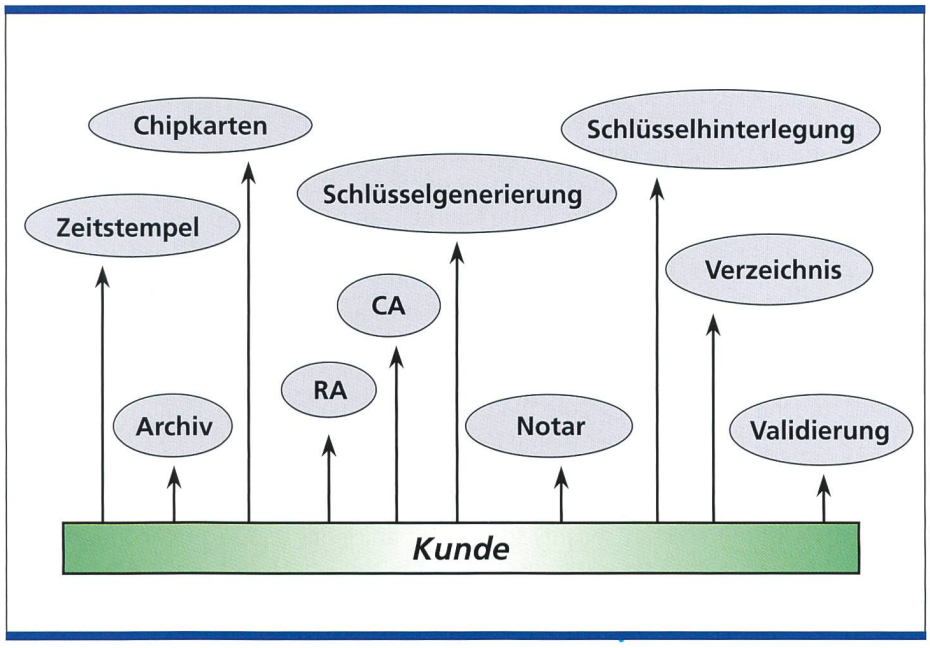

Bild 8. Trusted-Third-Party-(TTP)-Dienste.

Staatliche Unterstützung des Vertrauensaufbaus in Zertifikate und Zertifizierstellen

Der Bundesrat wird demnächst eine «Verordnung über eine PKI in der Schweiz (PKIV)» sowie die zugehörigen Ausführungsbestimmungen erlassen. Darin wird interessierten Zertifizierstellen («Zertifizierdienstanbieterinnen») angeboten, sich vom Staat freiwillig eine Art Qualitätsbestätigung ausstellen zu lassen. Dabei sollen die bestehenden und etablierten Mechanismen der «Zertifizierung durch akkreditierte Prüfstellen» angewendet werden. Diese kommen beispielsweise bei der Homologisierung von elektrischen Apparaten zum Zuge. Der Hauptzweck der Verordnung, die nota bene direkt nichts mit digitalen Signaturen zu tun hat, ist die Erhöhung des Vertrauens in diese Technologie, indem der Staat quasi seinen Qualitätsstempel auf diejenigen Zertifizierstellen setzt, die freiwillig seine Qualitäts- und Sicherheitskriterien erfüllen.

Schlussfolgerungen

Einige oft vorgelegte Einwände von Händlern, Dienstleistungsanbietern oder Privatpersonen gegen E-Commerce sind Misstrauen bezüglich der Sicherheit des Internets, Schwierigkeiten der Nachweisbarkeit bzw. Beweisführung von elektro-

nischen Abläufen vor Gericht (Beweislage), Mangel an Erfahrung und fehlende Jurisprudenz. Alles Faktoren, die die Gewissheit bestärken würden, dass die im Internet vorhandenen Risiken abschätzbar und in den Griff zu bekommen sind. Qualitativ hochwertige Sicherheitsfunktionen fürs Internet sind aber vorhanden, wie beispielsweise Verschlüsselung, digitale Signaturen, Zertifikate und Zeitstempel, obwohl sie zum Teil bezüglich Standardisierung, Verbreitung und Benutzerfreundlichkeit noch reifen müssen. Unter Verwendung dieser Sicherheitsfunktionen ist das Internet sicherer als die klassische Papierwelt. Hochwertige digitale Signaturen sind fälschungssicherer als handschriftliche Unterschriften. Ausserdem können mit digitalen Signaturen im Vergleich zu handschriftlichen Unterschriften zusätzliche Sachverhalte nachgewiesen werden, wie beispielsweise die Integrität der signierten Informationen. Die Möglichkeiten der Nachweisbarkeit oder Beweisführung vor Gericht sind also durchaus nicht schlecht.

Ausblick

Es geht nun also darum, die neuen Sicherheitsfunktionen kennen zu lernen und Erfahrungen im Umgang mit ihnen zu sammeln. Dabei müssen die in der traditionellen Welt existierenden Sicherheitsfunktionen in die elektronische Welt abgebildet und neue Funktionen eingeführt werden, welche die im neuen elektronischen Medium auftretenden Probleme lösen. Dies genügt aber nicht, denn die in der traditionellen Welt durch jahrhundertelange Erfahrung erhärteten Gewissheiten wie Verlässlichkeit der Geschäftsbeziehungen, Verbindlichkeit der Transaktionen und Vertrauen in das System müssen sich in der elektronischen Welt erst noch festigen. Die heute noch fehlende Gerichtspraxis im Umgang mit digitalen Signaturen kann dabei relativ einfach durch das auch in anderen Bereichen übliche Herbeiführen eines Präzedenzfalls erzwungen werden.

Die Chancen, von E-Commerce zu profitieren, sind für ein Unternehmen, eine Behörde und für die ganze Bevölkerung umso höher, je mehr sie sich mit der Materie befassen, sich Kenntnisse im Umgang mit Sicherheitsfunktionen des neuen elektronischen Mediums aneignen und Erfahrungen sammeln. Je früher dieser Prozess gewagt wird und je intensiver er durchgeführt wird, desto besser stehen die Chancen, dass sich die Schweiz mit ihrem hohen Bildungsgrad der Bevölkerung und der hohen Durchsetzung von Informatik und Internet im nationalen und internationalen E-Commerce bestens behaupten kann. [4, 7]

Bausteine des sicheren und verbindlichen E-Commerce

- Sichere Kommunikation bezüglich Authentifikation, Integrität und Vertraulichkeit
- Beweisbarer und verbindlicher Meldungsaustausch mit Sende- und Empfangsbestätigungen von hohem Beweiswert
- Sichere, geschützte EDV-Infrastrukturen bei allen beteiligten Stellen
- Verbindliche und unfälschbare elektronische Verträge mit hohem Beweiswert
- Unfälschbare elektronische Zeitstempel für die Beweisbarkeit des Zeitpunktes von elektronischen Aktionen oder Transaktionen oder der Existenz von Informationen
- Sichere Archivierung von elektronischen Dokumenten, Meldungen und Transaktionen über Jahre oder Jahrzehnte hinweg
- Erhalt des Beweiswerts, das heisst der Überprüfungs- und Beweisfähigkeit einer Aktion oder Transaktion über Jahre oder Jahrzehnte hinweg

Bild 9. Anforderungen für Sicherheit und hohe rechtliche Beweislage im E-Commerce.

Peter Keller *studierte an der ETH Lausanne Elektrotechnik und arbeitet seit 1994 bei Swisscom Corporate Technology. Er ist als Experte für Informationssicherheit in diversen Explorations-, Dienstentwicklungs- und Infrastrukturschutzprojekten involviert. Sein Hauptgebiet ist die Sicherheit im Internet, wobei sein besonderes Interesse Public-Key-Verfahren, Schlüsselzertifikaten und Certification Authorities gilt.*

Summary

Some of the mostly used arguments of merchants, service providers or consumers against the use of E-commerce are doubts concerning the security of the Internet, the insufficient ability to conduct proofs for electronic actions and transactions, the lack of experience and the missing jurisdiction – issues which all would support the assurance that the risks in the Internet can be estimated and handled. However, at least in Switzerland, the actual situation with respect to electronic proofs is not bad at all, and the necessary security mechanisms like digital signatures, public key certificates and timestamps are known and can be used, although they sometimes lack maturity with respect to standardisation, widespread use and user friendliness. When using these high quality security mechanisms, the Internet is more secure than the classical paper world. High quality digital signatures are stronger than hand-written signatures, and they even proof additional features like for example the integrity of the signed information.
The article describes the building blocks to achieving a high level of security, presents a list of necessary security services for efficiently and securely conducting e-commerce, and analyses some special security and legal issues which are new in the electronic media like the Internet.