Think.doc - Sondernewsletter

Digitale Signatur - Quo vadis?

Sonderausgabe | Der Weg nach der Insolvenz des einzigen in der Schweiz akkreditierten Zertifikatedienstanbieters.

Empfänger: [Anrede] [Name] ([EMAIL])
Gesendet am: [Datum]

Guten Tag [Anrede] [Name],

der einzige in der Schweiz akkreditierte Anbieter von Zertifikaten zur elektronischen Signatur musste am 14.09.2005 Insolvenz anmelden. Auch ein Projekt der PENTADOC wurde von dieser Meldung überrascht, wollte man doch dort zum Ende des Jahres Dokumente im grossen Stil digital signieren.

Ist das das Ende eines Traums, elektronische Dokumente digital signiert zu archivieren?

Wir sprachen mit:

- **Thomas J. Fuchs**,
  Geschäftsführer des Beratungsunternehmens PENTADOC GmbH Schweiz,
- **René Eberhard**,
  Geschäftsführer des Hochtechnologie-Unternehmens KEYON, Rapperswil, sowie
- **Thomas Fürling**,
  Geschäftsführer des Systemintegrationshauses e3 AG, Zürich.

Und nun viel Spaß beim neuen Denkstoff!

Ihre PENTADOC Schweiz

Selbstverständlich freuen wir uns über Ihre Anregungen, Fragen und Meinungen zum Thema. Sie finden hier die Email-Adresse für Ihr Feedback.

Wenn Sie den PENTADOC Newsletter nicht mehr erhalten möchten, dann klicken Sie bitte auf folgenden Link:

Think.doc abmelden

Inhaltsverzeichnis:

Links:

http://www.pentadoc.com/
http://www.ecm-tage.de/
http://www.dms-akademie.com/

Ansprechpartner:

PENTADOC GmbH Schweiz

Herr Thomas J. Fuchs

PENTADOC GmbH Schweiz

Stockerhof
Dreikönigstr. 31a
CH-8002 Zürich

Fon: +41 (0) 1 208 31 91
Fax: +41 (0) 1 208 35 00
mailto:info@pentadoc.ch

Service

Wir freuen uns, wenn Ihnen Think.doc gefällt.
Sie können Think.doc hier kostenlos abonnieren, weiterempfehlen oder Ihre Daten ändern.
Für Rückfragen, Anregungen und Informationen wenden Sie sich bitte an Herrn Guido Schmitz.

Impressum
Anmelden
Ummelden | Ändern

Thomas J. Fuchs

Geschäftsführer PENTADOC GmbH Schweiz

Thomas J. Fuchs berät seit 1989 Unternehmen in den Bereichen elektronischer Archivierung, Dokumenten-Management, Workflow und Geschäftsprozess-Optimierung. Von der Vorstands- und Mangementberatung über Vorstudien, Fach- und Detailkonzepte bis zur Implementierung war er in über fünfzig ECM-Projekten als führender Berater, Gesamtprojektleiter oder in den Steuerungsausschüssen tätig.

Think.Doc: Herr Fuchs, bedeutet die Insolvenz des letzten akkreditierten Zertifikatedienstanbieters (ZDA, engl. Certificate Authority, CA) das Ende der Digitalen Signatur in der Schweiz?

TJF: Nein, das Gegenteil ist der Fall. Die Zielgruppe wurde an die Verletzlichkeit durch das Modell ausländischer CAs erinnert. Man hat erkannt, wie wichtig ein rein schweizerischer CA-Anbieter ist.

Think.Doc: Wie sollen sich aber nun interessierte Unternehmen verhalten?

TJF: Wir wissen von mindestens drei schweizerischen Unternehmen, die sich bereits in der Akkreditierungsphase befinden und rechnen binnen dreier Monate mit deren Marktpräsenz. Auch ist uns ein weiteres Unternehmen bekannt, das den Markteintritt zumindest mittelfristig, also in einem Zeitraum unter einem Jahr, prüft.

Think.Doc: Was raten Sie bis anhin?

TJF: Für Unternehmen, die nicht warten können oder wollen: Als kurzfristiges Szenario sehen wir durchaus die Möglichkeit, weiterhin mit TC-Trustcenter-Zertifikaten zu signieren. Zum einen scheint TC-Trustcenter ernsthaft die Aktivitäten fortführen zu wollen. Die Zertifikate bleiben ja zunächst gültig. Sobald es den Unternehmen möglich ist, sich ElDI-V konforme Zertifikate von in der Schweiz anerkannten Zertifizierungsdiensteanbietern gemäss ZertES ausstellen zu lassen, können Zertifikate, die gestützt auf Art. 12 ElDI-V ausgegeben worden sind (also auch Trustcenter-Zertifikate), noch während einer Übergangsfrist von 12 Monaten genutzt werden. Bei Ablauf der Übergangsfrist müssen die Zertifikate, die sich auf Art. 12 ElDI-V stützen, revoziert werden. Die lange Übergangsfrist von 12 Monaten stellt jedoch eine problemlose Migration auf die Schweizer Zertifikate sicher.

Think.Doc: Wie sehen Sie den Schweizer Markt der Digitalen Signatur?

TJF: Wir glauben, dass der Mehrwert der Digitalen Signatur sowohl in der Integritätssicherung bei der Archivierung als auch über Prozessketten hinweg zuerst noch entdeckt werden muss. Aus unserer Erfahrung können wir sagen, dass sich gegenüber traditionellen, nichtveränderbaren Speichermedien enorme Kostenvorteile in Anschaffung und Unterhalt ergeben können. Somit wird sich der Marktanteil erst in den nächsten drei Jahren entwickelt. Parallel dazu steigen auch die Sicherheitsanforderungen. Auch damit müssen die Unternehmen umgehen können.
Jedoch gibt es auch Anwendungsgebiete, wo die konventionellen Medien nicht nur die technologisch bessere, sondern auch kostengünstige Variante sein werden. Auch hier gilt: Jeder Einzelfall muss geprüft werden.

top

René Eberhard

Geschäftsführer des Hochtechnologie-Unternehmens KEYON, Rapperswil

KEYON ist ein führender Lieferant von Lösungen und Dienstleistungen im Bereich der IT-Sicherheit und der rechtsgültigen Langzeitarchivierung von Daten basierend auf elektronischen Signaturen.

Think.Doc: Herr Eberhard, Ihr Unternehmen taucht immer wieder im Zusammenhang von Digitaler Signaturen auf. Warum?

RE: Unter der Leitung von Keyon wurde zusammen mit der EAN Schweiz (heute GS1) und dem deutschen Zertifizierungsdiensteanbieter TC Trustcenter eine PKI aufgebaut, die von der Eidgenössischen Steuerverwaltung ESTV anerkannt wurde. Basierend auf Zertifikaten, die vom zuvor genannten Zertifizierungsdiensteanbieter ausgegeben werden, ist es für in der Schweiz ansässige Unternehmen möglich, elektronisch signierte Rechnungen zu erstellen, welche von der ESTV anerkannt werden. Damit nahm die Schweiz im Bereich der Mehrwertsteuer europaweit eine führende Rolle bei der elektronischen Geschäftsabwicklung ein. Keyon war also seit Beginn der rechtsgültigen elektronischen Geschäftsabwicklung aktiv und hat seine Dienstleistungen und Lösungen kontinuierlich ausgebaut und weiterentwickelt. Heute basieren zahlreiche Systeme von grossen Unternehmen und Dienstleisten auf dem true-sign Framework von Keyon. Keyon unterstützt seine Kunden in organisatorischen, juristischen und technischen Fragen und bietet Lösungen aus einer Hand.

Think.Doc: Wo sehen Sie die zentralen Anwendungsmöglichkeiten für die Digitale Signatur?

RE: Im Zusammenhang mit elektronischen Geschäftsprozessen gibt es drei zentrale Anwendungsmöglichekeiten. Dies sind die elektronische Rechnungsstellung (ElDI-V), die Langzeitarchivierung basierend auf elektronischen Signaturen (GeBüV) und mittelfristig die Gleichstellung der handschriftlichen Unterschrift mit der elektronischen Unterschrift (ZertES).

Think.Doc: Rechnet sich das für Ihre Kunden?

RE: Die Kosteneinsparungen sowie die Einhaltung von Gesetzen und Revisionsrichtlinien sind der wichtigste Treiber für unsere Projekte. Im Bereich der elektronischen Rechnungsstellung liegt das Einsparpotential in der Verarbeitung, Verbuchung und der Archivierung der Rechnungen. Die Optimierung von Bestell-, Liefer- und Rechnungsprozessen wird oft parallel angegangen. Im Bereich der Langzeitarchivierung können unter Verwendung von elektronischen Signaturen preiswerte Massenspeicher (Harddisk, Tape, SAN, NAS, etc.) anstelle von teuren WORM-Speichern verwendet werden. Im weiteren ist die Bewirtschaftung der Daten und der Datenträger effizienter und kostengünstiger. Letzteres ist entscheidend für die Migration grosser Datenvolumen auf neue Speichermedien.

Think.Doc: Wie sehen Sie den Schweizer Markt der Digitalen Signatur?

RE: Im Bereich der elektronischen Geschäftsabwicklung ist die Schweiz auf anerkannte Zertifizierungsdiensteanbieter angewiesen. Wir

wissen, dass sich verschiedene Anbieter in der Akkreditierung befinden und hoffen auf einen möglichst raschen Marktauftritt. Die Konzeptionierung und Umsetzung unserer Lösungen ist jedoch vollständig unabhängig von den jeweiligen Zertifizierungsdiensteanbietern, da diese ihre Leistungen ebenfalls auf den bestehenden gesetzlichen Vorgaben abstützen müssen.

top

Thomas Fürling

Geschäftsführer des Systemintegrationshauses e3 AG, Zürich

Die e3 AG ist ein international tätiger Integrationsspezialist mit Standorten in Zürich, Frankfurt und London.

Think.Doc: Herr Fürling, die e3 AG ist ein klassisches IT-Integrationsunternehmen. Welche Rolle spielt das Thema Digitale Signaturen bei Ihnen?

TFü: Digitale Signaturen ist eine Funktionalität, die bei modernen Prozessen viel Zukunft hat und auch haben muss. Neben den schon erwähnten gesetzlichen Anforderungen sind gesteigerte Sicherheitsanforderungen und zu erwartende Kostenersparnisse gut Argumente, um die Möglichkeiten der Digitalen Signaturen zu integrieren.

Think.Doc: Sie haben schon Digitale Signatur Server in die Applikationslandschaft Ihrer Kunden integriert. Wo liegen die typischen Stolpersteine?

TFü: Die Integration in Business Prozesse, Applikationen und Infrastruktur stellt aufgrund der Sicherheit hohe Anforderungen. Bei allen Integrationen sind die Stabilität und Performance der Schnittstellen sehr wichtig. Für Digitalen Signaturen kommen neben den eigentlichen Signatur-Prozessen zusätzliche spezifische und generelle Anforderungen hinzu. Zum einen sind die betrieblichen Prozesse sehr komplex und zum anderen wird die Lösung sobald sie in den möglichen Abläufen integriert ist, sehr zentral und muss entsprechend verfügbar sein.
Der reine Signatur-Prozess ist im Gesamtablauf nur ein relativ kleines Element. Die Daten müssen vorbereitet sein, es muss die beste Lösung für die Kontrolle der Signatur auf der Gegenseite gefunden werden. Die kann von einer spezialisierten Lösung in den eigenen Archivierungsprozessen bis zu aufwändigen Massenlösungen für Endkunden reichen.

Think.Doc: Welches klassischen Integrationstechniken und welches zusätzliche Knowhow ist notwendig um Digitale Signaturen einzuführen?

TFü: Die Daten müssen schon bei der Erzeugung vorbereitet werden. Danach ist neben der technischen Integration (Messaging, Filetransfer) vor allem das Datenformat sehr wichtig. Die Signatur eines PDF ist formatbedingt anders als die Signatur eines XML-Files oder eines AFP-Dokumentes. Es ist unwahrscheinlich, dass in einem Unternehmen, das Digitale Signaturen einführen will, alle Daten im gleichen Format vorliegen oder im gleichen Format verwendet werden. Die Konvertierung ist somit ein weiteres klassisches Integrationsgebiet ohne das nur wenig geht. Natürlich ist ein gutes Verständnis um Kryptologie notwendig um die Signaturen auch richtig anzuwenden. Das benötigte Wissen nimmt zu, je umfassender die Lösung ist.

Think.Doc: Wie sehen Sie den Schweizer Markt der Digitalen Signatur?

TFü: Der Markt hat sehr viel Potential. Die Unternehmen beginnen die Möglichkeiten und Kosteneinsparungen zu erkennen. Allerdings sind die Anfangsinvestitionen noch immer im Bereich von Grossunternehmen und grösseren KMU. Kleinere KMU werden auf die Hersteller ihrer ERP-Lösungen warten müssen, was nicht mehr lange dauern wird, denn der Markt ist auch für diese Hersteller sehr interessant. Entsprechend sind Investitionen bereits getätigt worden und oder befinden sich in Planung. Die Akzeptanz von Digitalen Signaturen bei Steuerämtern, im Vertragswesen und im der Business to Business Kommunikation stehen noch bevor und bedeuten den endgültigen Durchbruch dieses potenten Verfahrens.

top

Digitale Signatur, was ist das?

Die elektronische Speicherung von Dokumenten ist bereits seit vielen Jahren etablierte Praxis in schweizerischen Unternehmen. Die Verordnung über die Führung und Aufbewahrung der Geschäftsbücher, auch kurz Geschäftsbücherverordnung - oder noch kürzer "GeBüV" genannt - regelt die Zulässigkeit dieser elektronischen Archive. So werden z.B. die zulässigen Informationsträger im Artikel 9 definiert. Neben den unveränderbaren Datenträgern wie laserbeschriebenen Disks, sog. WORMs (Write Once Read Many) sind auch explizit veränderbare Informationsträger zugelassen. Dabei müssen allerdings vier Bedingungen eingehalten werden:

1. **Technische Verfahren**
   Es müssen technische Verfahren zur Anwendung kommen, welche die Integrität der gespeicherten Informationen gewährleisten.
2. **Zeitpunkt der Speicherung**
   Der Zeitpunkt der Speicherung der Informationen muss unverfälschbar nachweisbar sein (z.B. durch «Zeitstempel»).
3. **Einhaltung weiterer Vorschriften**
   Die zum Zeitpunkt der Speicherung bestehenden weiteren Vorschriften über den Einsatz der betreffenden technischen Verfahren müssen eingehalten werden.

4. **Verfahrensdokumentation**
   Die Abläufe und Verfahren zum Einsatz der technischen Verfahren müssen festgelegt und dokumentiert sein sowie die entsprechenden Hilfsinformationen (wie Protokolle und Log files) müssen ebenfalls aufbewahrt werden.

Die GeBüV nennt explizit die Digitale Signatur als ein solches technisches Verfahren.

top

Das Prinzip der digitalen Signatur

Die digitale Signatur ist ein asymmetrisches Verfahren. Asymmetrisch deshalb, weil zum Erzeugen der Signatur ein anderer Schlüssel verwendet wird, als zum Prüfen. Ausschließlich mit dem privaten Schlüssel kann eine Signatur erzeugt werden. Die Prüfung der Signatur erfolgt allein mit dem öffentlichen Schlüssel. Beide Schlüssel zusammen bilden ein Schlüsselpaar, dessen Erzeugung und Verarbeitung auf kryptografischen Algorithmen, z. B. RSA basiert.

Jeder Anwender der digitalen Signatur erhält ein persönliches Schlüsselpaar. Der private Schlüssel ist absolut geheim zu halten und i.d. R. vor Missbrauch durch eine zusätzliche PIN oder biometrische Merkmale geschützt. Der öffentliche Schlüssel wird wie der Name sagt, öffentlich bekannt gegeben. Dem asymmetrischen Verfahren der digitalen Signatur sind daher folgende Eigenschaften inhärent:

- Der Absender ist eindeutig identifizierbar - **Authentifizierung**
- Die Daten sind vor Manipulation geschützt – **Integrität**

Das asymmetrische Verfahren erfüllt somit die Anforderungen an eine sog. fortgeschrittene elektronische Signatur. Eines ist jedoch nicht gewährleistet: der Nachweis der **Urheberschaft**. Denn es besteht die Möglichkeit, dass eine Person einen öffentlichen Schlüssel unter falschem Namen veröffentlicht.

Um schließlich auch die Urheberschaft der Daten und damit der mitgelieferten Signatur nachzuweisen, muss eine Sicherungsinfrastruktur mit einem „vertrauenswürdigen Dritten“ vorhanden sein, welcher die Zuordnung des öffentlichen Schlüssels zu einer natürlichen Person in Form eines Zertifikats bestätigt. Durch ein solches Schlüsselzertifikat wird die Signatur authentisch und somit implizit die Urheberschaft der signierten Daten nachgewiesen. Der vertrauenswürdige Dritte, ein sog. Zertifizierungsdiensteanbieter (englisch: certification authority, umgangssprachlich auch Trustcenter genannt) stellt sozusagen eine digitale Identität aus - eine Art elektronischer Personalausweis.

Abbildung 1 veranschaulicht das Erzeugen einer digitalen Signatur. Signiert wird hierbei nicht das elektronische Dokument selbst, sondern ein vorher, ebenfalls durch einen kryptografischen Algorithmus erzeugter, digitaler Fingerabdruck (Hashwert) der Datei.

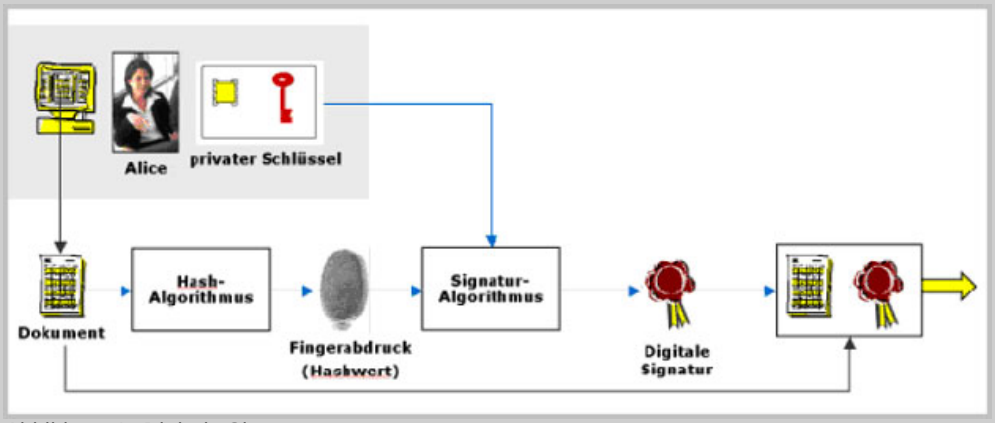

Abbildung 1: Digitale Signatur erzeugen

Abbildung 2 stellt den Prüfvorgang dar. Um für jedermann jederzeit eine Prüfung von digitalen Signaturen zu ermöglichen, stellt der Zertifizierungsdiensteanbieter ein öffentliches Verzeichnis mit gültigen und gesperrten Zertifikaten online zur Verfügung. Mit Hilfe der vertrauenswürdigen dritten Instanz wird die fortgeschrittene zur **qualifizierten elektronischen** Signatur. **Nur diese** ist gesetzlich der Schriftform gleichgestellt.

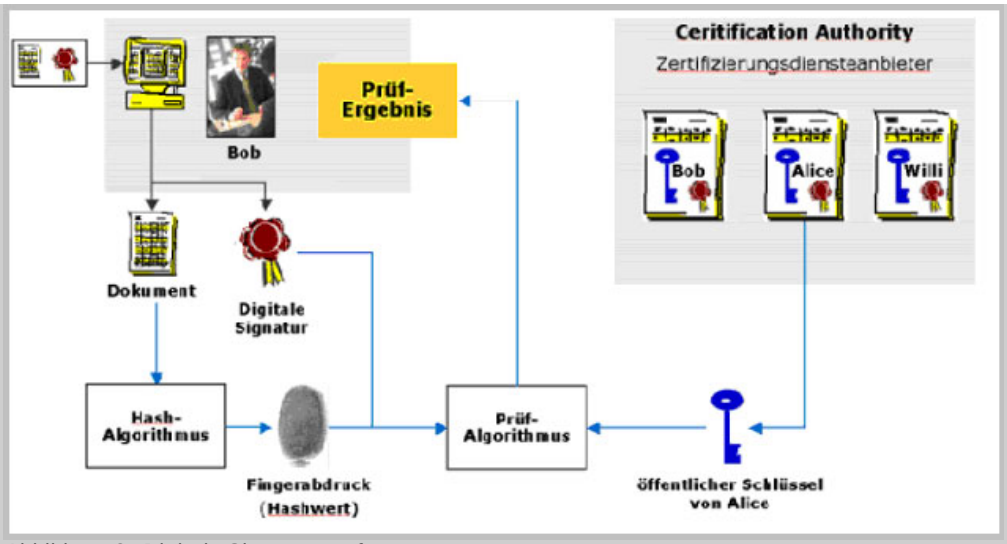

Abbildung 2: Digitale Signatur prüfen

top

Funktionszertifikate

Funktionszertifikate werden nicht auf eine Person, sondern auf ein Unternehmen und/oder eine Abteilung wie z.B. Rechnungswesen/ Buchhaltung innerhalb des Unternehmens ausgestellt. Im Gegensatz zum personenbezogenen Zertifikat ist das Funktionszertifikat nicht auf eine natürliche Person ausgestellt, kann also nicht für eine Willenserklärung herangezogen werden (e.g. wie das elektronische Unterschreiben eines Kaufvertrages).

Unter Verwendung von elektronischen Signaturen (Funktionszertifikate) können nicht nur elektronische Rechnungen und somit der Vorsteuerabzug gegenüber der Eidgenössischen Steuerverwaltung (ESTV) auf der Basis von elektronisch signierten Daten geltend gemacht, sondern auch rechtlich relevante Daten auf veränderbaren Speichermedien signiert werden.

Damit die Zulassung der digitalen Signatur gestützt auf diese Zertifikate erfolgen kann, müssen zudem auch die übrigen in der Verordnung des Eidgenössischen Finanzdepartments (EFD) über elektronisch übermittelte Daten und Informationen (EIDI-V) festgehaltenen Auflagen erfüllt werden. Dies entspricht einer sog. weiteren Vorschriften gem. GeBüV Artikel 9 1 b 3.

top

Rechtliche Grundlagen

Während in benachbarten Ausland die digitale Signatur schon eine signifikante Rolle bei der Integritätssicherung von elektronischen Archiven spielt, konnte der Durchbruch in der Schweiz noch nicht erreicht werden. Dies mag auch daran liegen, dass sich kein schweizerischer Zertifikatedienstanbieter am Markt etablieren konnte (Henne-Ei-Problematik). Mangels Alternativen wurden ausländische Anbieter explizit zugelassen (Artikel 12 ElDI-V). De facto war in der Schweiz bislang nur ein Anbieter akkreditiert, die nun insolvente TrustCenter aus Hamburg.

- **GeBüV** - Die Verordnung über die Führung und Aufbewahrung der Geschäftsbücher, auch kurz Geschäftsbücherverordnung - oder noch kürzer "GeBüV" genannt – beschreibt die Anforderungen an elektronische Archive.
- **EIDI-V** - Die Verordnung des Eidgenössischen Finanzdepartments (EFD) über elektronisch übermittelte Daten und Informationen (EIDI-V) regelt die Anforderungen an die Beweiskraft und die Kontrolle von elektronischen Dokumenten, im besonderen im Rahmen der Digitalen Signatur.
- **MWSTG** - Das Bundesgesetz über die Mehrwertsteuer (Mehrwertsteuergesetz) regelt zusammen mit der...
- **MWSTGV** - Verordnung zum Bundesgesetz über die Mehrwertsteuer, die vorsteuerabzugsrechtliche Anerkennung elektronischer Rechnungen.
- **OblRecht** - Bundesgesetz betreffend die Ergänzung des Schweizerischen Zivilgesetzbuches (Fünfter Teil: Obligationenrecht), v. a. Art. 957, "erlaubt" die elektronische Archivierung im Geschäftsleben.
- **ZertES** - Bundesgesetz über Zertifizierungsdienste im Bereich der elektronischen Signatur (Bundesgesetz über die elektronische Signatur).
- **ZertDV** - Verordnung über Dienste der elektronischen Zertifizierung (Zertifizierungsdiensteverordnung).
- Schweizerisches Strafgesetzbuch

top

Die Säulen der digitalen Signatur

Die Gesamtheit der Verfahren, sowie der organisatorischen und technischen Einrichtungen, welche für die digitale Signatur vorgehalten werden müssen, bezeichnet man als Public Key Infrastructure (PKI). Wichtigstes Bindeglied in dieser Infrastruktur sind sicherlich die Zertifizierungsdienstanbieter (engl. Certification Authority, CA). Auf Antrag und nach Prüfung der Identität eines neuen Anwenders, generiert das CA das persönliche Schlüsselpaar und integriert den privaten Schlüssel in eine Sicherheitsmedium, e.g. eine Smartcard. Das CA stellt dem Anwender ein digitales Zertifikat aus, welches den öffentlichen Schlüssel enthält und über einen Verzeichnisdienst für die Signaturprüfung bereit gestellt wird.

Ein oberstes Kontrollorgan wie in Deutschland (dort ist es die Regulierungsbehörde für Telekommunikation und Post, RegTP), welches über die Einhaltung von Signatur-Gesetz und -Verordnung wacht, gibt ist in der Schweiz nicht. Allerdings kann das Bundesamt für Metrologie und Akkreditierung gegen Nachweis von Qualifikation, ausreichender technischer Infrastruktur und Sicherheitsvorkehrungen Anbieter akkreditieren. Dies tut sie formal, indem sie dem ZDA wiederum ein digitales Zertifikat ausstellt. Akkreditierte ZDAs müssen Zertifikate mindestens 30 Jahre in einem öffentlichen Verzeichnis zur Verfügung stellen.

Die Überprüfung einer digitalen Signatur erfolgt demnach mehrstufig über eine Zertifikatkette: vom Zertifikat des Anwenders über dasjenige des ZDA bis zum Zertifikat der zuständigen Behörde (sog. Root CA), die ihr Zertifikat selbst ausstellt. Die Sicherheit der digitalen Signatur beruht im Wesentlichen auf der Stärke der zugrundeliegenden Verschlüsselungsalgorithmen. Diese kryptografischen Algorithmen basieren auf praktisch unlösbaren mathematischen Problemen. Unlösbar jedoch nur solange, bis steigende Rechenkapazitäten eine empirische Lösung des Problems erlauben. Daher unterliegen für die digitale Signatur zugelassene Algorithmen einem Verfallsdatum, aktuell bis 2008. Danach ist eine Erhöhung der Schlüssellängen notwendig, bei Bedarf jedoch schon früher.

top

Pro und Contra Digitale Signatur

Die folgende Tabelle nennt – ohne Anspruch auf Vollständigkeit – eine Reihe von Eigenschaften der digitalen Signatur in Form einer PRO und CONTRA-Liste:

Pro

- Kostengünstige Möglichkeit zur GeBüv-konformen elektronischen Speicherung von Dokumenten
- Rechtliche Gleichstellung der signierten Dokumente mit dem Papieroriginal
- Gewährleistung von Integrität, Authentizität und Nachweis der Urheberschaft
- Höhere Sicherheit als manuelle Unterschrift
- Erweitertes Anwendungsfeld: Signatur beliebiger elektronischer Dokumente möglich
- Sekundenschnelle Überprüfbarkeit (online)
- Einsparpotenziale in Verwaltung und Wirtschaft aufgrund durchgängiger elektronischer Bearbeitung (kein Medienbruch)
- Mögliche Förderung des eCommerce durch bessere abgesicherte Transaktionen
- Basis für viele eGovernment-Dienste

Contra

- Missbrauch möglich
- Missbrauch schwierig nachzuweisen (digitale Unterschrift kann im Gegensatz zur manuellen"aus der Hand“ gegeben werden)
- Signaturalgorithmen könnten früher als geplant unbrauchbar ("geknackt“) werden
- Teure und komplexe technische und organisatorische Infrastruktur (PKI)
- Hohe Kosten, sowohl für Unternehmen als auch private Endanwender
- Erneuerung wg. Gültigkeitszeitraum (ähnlich Kreditkarten):
  - Dokumente mit langen Aufbewahrungsfristen
  - besitzen danach juristisch keine Unterschrift mehr, falls kein Zeitstempel verwendet wurde
- Vertrauen in die Zuverlässigkeit der ZDAs ist eingeschränkt
- z. T. International unterschiedliche Standards und Akzeptanz

top

Fazit

In den nächsten Monaten, spätestens zur Mitte des nächsten Jahres, wird sich zeigen, ob die Digitale Signatur in der Schweiz aus der Nische tritt und als neue Technologie wahrgenommen und eingesetzt wird. An der Frage der gesetzlichen Akzeptanz kann es nun aber nicht mehr liegen. Ebenso ist die Technologie als solche stabil verfügbar. Fraglich bleibt, ob die Nutzenpotentiale von den Unternehmen erkannt und die Technologie beherrscht wird. Darin dürfte auch eine Chance für die Unternehmen liegen, sich als Marketmover zu profilieren.

top

Service

Wir freuen uns, wenn Ihnen Think.doc gefällt.
Sie können Think.doc hier kostenlos abonnieren, weiterempfehlen oder Ihre Daten ändern.
Für Rückfragen, Anregungen und Informationen wenden Sie sich bitte an Herrn Guido Schmitz.

Impressum
Anmelden
Ummelden | Ändern

Newsletter abmelden

Wenn Sie den PENTADOC Newsletter nicht mehr erhalten möchten, dann klicken Sie bitte auf folgenden Link:

Think.doc abmelden