

## Funktion

Ein Trust Center soll die Zurechenbarkeit einer elektronischen Signatur zu einer natürlichen Person sichern. (Authentifizierung, Identitätsversorger, ID-Provider).

Der Akzeptant einer Nachricht vertraut auf die Authentizität des Absenders im Rahmen der vom Trust Center bei der Zertifikatsausgabe betriebenen Prüfleistungen.

Natürlicherweise hat der Einzelne das höchste Vertrauen nach persönlichem Augenschein. Insofern kann es die auf wikipedia angesprochene *nichtauthorisierte Person* auf höchster Vertrauensebene gar nicht geben. Diese vom SigG *fortgeschritten* genannten Signaturen unterliegen daher der freien Beweiswürdigung.

Für den administrativen Verkehr (im Geschäftsverkehr die letzte Stufe im Rahmen der Vollstreckung) ist die persönliche, "fortgeschrittene" Signatur natürlich ungeeignet. Das Amt akzeptiert nur Signaturen die von Zertifikaten anerkannter (qualifizierter) Trust Center signiert wurden. Im Geschäftsverkehr ist es vorteilhaft nur durch das SigG anerkannte Signaturen zu akzeptieren, weil dies die Vollstreckung erleichtert. Notwendig ist dies jedoch keineswegs.

## Praxis und SigG

Insbesondere Zertifizierungs- und Zeitstempeldienste müssen, wie alle mit Rechtsfolgen behafteten Vorgänge durch leicht und öffentlich nachprüf- und analysierbare offene Standards realisiert werden. -- Nur wo stehen die entsprechenden Bestimmungen im Signaturgesetz?

( ursprüngliche Fassung 2001 )

"Einfache" elektronische Signaturen nach SigG können als nicht relevant abgetan werden. Ihnen kann im Rahmen der freien Beweiswürdigung keinerlei Wert eingeräumt werden.

"Fortgeschrittene" Signaturen entstehen typischerweise durch cryptographische Verfahren. Auch die Anmeldung an an einem Askemos-Netzwerk, selbst wenn diese mit Nutzernamen/Passwort erfolgt, erfüllt die Anforderungen nach SigG §2 Punkt 2. BALLfIXml implementiert die notwendigen cryptographischen Algorithmen.

Signaturen von den Servern eines Askemos-Netzwerkes können als "qualifiziert" eingestuft werden, wenn

1. Auf qualifiziertem Zertifikat beruhen (§7) und von Zertifizierungsdiensteanbieter gemäß §§ 4-14 oder §23 erfüllen:
  - ◆ Zuverlässigkeit und Fachkunde
  - ◆ Deckungsvorsorge lt. §12 250000 €, versicherbar?
  - ◆ § 24 1,3,4
2. der Server entsprechend § 2 Punkt 3 als "sichere Signaturerstellungseinheit" gilt. Das sind Soft- oder Hardware-Einheiten, welche die folgende Anforderungen lt. §17 oder §23 erfüllen:

---

Offensichtlich wurde der Aufwand, symmetrische Verfahren vorzuschreiben als zu hoch eingeschätzt. Dadurch sind Vorgaben entstanden, welche Lücken offen lassen. Diese können jedoch leicht geschlossen werden.

Das wesentliche Problem ist der Fakt, daß bereits eine einzelne Signatur eines einzigen Identitätsversorgers

## TrustCenter

zur sicheren Identifikation akzeptiert wird. Dies reicht jedoch nur aus, wenn Trust Center und Rechtsträger identisch sind. Um handelseinig werden zu können braucht es in diesem Fall die byzantinische Einigung mindestens zweier, sich gegenseitig zertifizierender Paare aus Rechtsträger und Trust Center.

Das Problem kann leicht gelöst werden, wenn mehrere Signaturen unterschiedlicher und administrativ unabhängiger Trust Center gleichzeitig angebracht werden. Dann wird der Rechtsträger vom einzelnen Trust Center unabhängig. Der Rechtsträger erhält durch diese Freiheit eine qualitativ höhere Rechtssicherheit und gleichzeitig können die Anforderungen an die einzelnen Trust Center gesenkt werden. Während nämlich die kurzzeitige Verletzung der Vertrauenswürdigkeit des Trust Centers (Schlüsselverrat) in der gegenwärtigen Regelung sämtliche Signaturen invalidiert, kann der byzantinische Verbund den Totalausfall des einzelnen Trust Center störungsfrei verkraften und einen konsistenten Zustand auf einem Ersatz Trust Center wieder herstellen.

## Aufgaben des Trust Centers

TODO: Vergleiche mit SigG, ob die genau so vorgeschrieben sind, oder ob ie angemerkt Probleme im Rahmen der bestehenden Verordnung geklärt werden können.

1. Erzeugung von Schlüsselpaaren.
2. Identifikation der Schlüsselinhaber.
3. Zertifizierung des öffentlichen Schlüssels.
4. Einbringen des privaten Schlüssels in einen sicheren Träger (Chipkarte).
5. Unterrichtung der Schlüsselinhaber.
6. Entgegennahme von Sperrungen von Schlüsselpaaren.
7. Bereitstellung von Sperrlisten (elektronisch, 24 Stunden, 7 Tage pro Woche).
8. Möglichkeit der Einzelabfrage (elektronisch, 24 Stunden, 7 Tage pro Woche).
9. Bereitstellung eines Zeitstempeldienstes (freiwillig).

### Das Vertrauen

## Die Enttäuschung vom Vertrauen

DoD definition of trust: "a trusted system is one, which can break the security policy"

1. Wer erstellt den öffentlichen und den privaten Schlüssel ?

*Das zum Elektronischen Signieren verwendete Schlüsselpaar wird von einem Trustcenter erstellt. Jedes Schlüsselpaar darf es nur einmal geben. Niemand, auch nicht das Trustcenter selbst, darf Kenntnis von dem privaten Schlüssel erlangen. Deshalb wird dort der private Schlüssel nach dem Einlesen in die Signaturkarte gelöscht.*

**Damit ist der Begriff "Zentrum des Vertrauens" leider gerechtfertigt.**

Ein vollwertiges System muß sicherstellen, daß das Schlüsselpaar vom Schlüsseleigentümer erzeugt und nur der öffentliche Schlüssel einem dem Kommunikationspartner genehmen Zertifizierer zur Unterzeichnung vorgelegt wird.

Der Prozeß ist natürlich zu kompliziert. Alternativ kann ein Massenzertifizierer anonyme Zertifikate ausgeben, welche erst nach ihrem Erwerb personalisiert werden.

2. Welche Aufgaben erfüllt der Verzeichnisdienst?

## TrustCenter

*Der Verzeichnisdienst erteilt vertrauenswürdig Auskunft, ob das Signaturschlüsselzertifikat existiert, gültig und nicht gesperrt ist.*

**Vertrauenswürdig:** Auch hier gilt, es darf - jedenfalls in einer Demokratie - keine einzelne Instanz geben, welcher der Rechteinhaber total vertrauen muß. Im Streit zu unterwerfen ist der einzelne Bürger nur dem durch Recht und Gesetz gefaßten Volkswillen.

Ein vollwertiges System muß derartige Verzeichnisdienste im Askemos anbieten. D.h. in irgendeiner Weise durch byzantinische Abstimmung des Verzeichnisses in administrativ unabhängigen Kopien. (Eigenwerbung: besonders einfach ist das natürlich, wenn alle Kopien von BALL-Servern bereitgestellt werden.)

Wiederum ist es zu aufwändig, jedem Bürger den Betrieb eines eigenen Servers zuzumuten. Massenversorger können den Betrieb jedoch wiederum anonym anbieten. Der einzelne Bürger wählt sich sodann ein Quorum passend zur Aufgabe. Das Restrisiko, daß bei der Mehrheit der Massenversorger eine Fälschung zugunsten einzelner erfolgt, ist absehbar gering, ergo versicherbar und somit ist es ökonomisch vernünftig akzeptierbar.

### 3. Was ist ein Zeitstempeldienst?

*Für viele elektronische Daten ist es wichtig, den Zeitpunkt Ihrer Entstehung rechtsverbindlich feststellen zu können. Für solche Fälle stellt das Trustcenter einen Zeitstempeldienst bereit. Die Kurzform (Hash-Wert) der Daten wird mit einer verbindlichen, amtlichen Zeitangabe nach Zeitgesetz versehen und von dem Trustcenter mit einem speziellen Zeitstempelschlüssel elektronisch signiert.*

**Für alle vorgänge mit Rechtsfolge ist der entsprechende Zeitstempel notwendig. Deswegen führen wir im Askemos den Zeitstempel mit jeder Nachricht mit.**

Für den Anwender ist dies eine erhebliche Erleichterung. Spezielle Zeitstempeldienste gehören der Vergangenheit an. Der Zeitstempel ist Teil des Interpreters und damit der Programmiersprache. (Vgl. WhatIsTime)

4. Warum erhält man die PINs von vielen Zertifizierungsdiensteanbietern in zwei Teilen? Die PIN kommt aus Sicherheitsgründen in zwei Teilen. Nur aus beiden Teilen der PIN kann man die endgültige PIN ermitteln, d.h. geht ein Teil verloren, kann mit diesem Teil kein Missbrauch erfolgen.
5. Was sind die gesetzlichen Grundlagen der Elektronischen Signatur ?

Die gesetzliche Grundlage für Elektronische Signaturen bildet in Deutschland das Gesetz zur Elektronischen Signatur (SigG). Dieses Gesetz ist am 22.05.2001 in Kraft getreten und regelt für Deutschland die Erstellung, die Verteilung und Administration von elektronischen Signaturen. Die dafür notwendige Infrastruktur wird PKI (Public Key Infrastructure) genannt. Auf der Grundlage des SigG wurde weiterhin die Signaturverordnung erlassen und Maßnahmenkataloge geschaffen, die insbesondere die technischen Anforderungen weiter spezifizieren. Gleichsetzung der Elektronischen Signatur und der eigenhändigen Unterschrift: Zivilrecht Änderung des § 126 BGB in § 126 a BGB (01.08.2001). Das deutsche Signaturgesetz entspricht der Europäischen Signaturverordnung.

6. Wo erhält man weitere Informationen zu technischen oder rechtlichen Fragen ? Zu rechtlichen und technischen Hintergründen finden sich Informationen auf der www-Seite des Bundesamtes für Sicherheit in der Informationstechnik (BSI unter <http://www.bsi.de>, beim Bundesministerium für Wirtschaft und Technologie unter <http://www.iukdg.de>. Die Regulierungsbehörde für Telekommunikation und Post (RegTP) erstellt die Schlüsselpaare und Zertifikate für alle Trustcenter und stellt ebenfalls Informationen unter <http://www.regtp.de> bereit. Was unterscheidet ein akkreditiertes von einem nicht akkreditiertem Trustcenter ?

## TrustCenter

Das SigG2001 sieht 2 Typen von Zertifizierungsdiensteanbietern zur Vergabe von qualifizierten Zertifikaten vor: 1. Angemeldete Zertifizierungsdiensteanbieter. Die Qualität beruht weitgehend auf Erklärungen der Unternehmen. Die Unternehmen bieten Gewähr für die Einhaltung der Rechtsvorschriften. 2. Freiwillig akkreditierte Zertifizierungsdiensteanbieter. Bei diesen Zertifizierungsdiensteanbietern erfolgt eine Prüfung der Einhaltung der im Signaturgesetz festgelegten Regeln und Vorschriften vor Aufnahme des Betriebes durch zugelassene Prüf- und Zertifizierungsstellen. Die einzelnen sicherheitstechnischen, personellen und organisatorischen Maßnahmen sind in einem von der Reg TP gemäß § 12 der Signaturverordnung herausgegebenen Maßnahmenkatalog konkretisiert.

7. Welche Arten von Signaturen werden unterschieden ?

1. Einfache elektronische Signaturen 2. Fortgeschrittene elektronische Signaturen 3. Qualifizierte elektronische Signaturen 4. Qualifizierte elektronische Signaturen eines akkreditierten Zertifizierungsdiensteanbieters (kurz akkreditierte elektronische Signatur genannt) Gesetzlich festgelegte Rechtsfolgen haben nur qualifizierte elektronische Signaturen und akkreditierte elektronische Signaturen. Alle Signaturen sind verbindlich. Nur die qualifizierten elektronischen Signaturen und akkreditierten elektronischen Signaturen erfüllen alle Formvorschriften und sind bei Gericht ohne Einschränkung als Beweismittel zugelassen. Die beiden anderen Formen der elektronischen Signatur unterliegen der freien Beweiswürdigung des Richters.

---

Last modifikation: Wed, 01 Jul 2009 14:15:13 +0200

Author(s): jfw,

Document number A849640f672ed0df0958abc0712110f3c page TrustCenter delivered to public at Tue, 07 Sep 2010 17:43:27 +0200