Transaktionssicherheit Sicherer Signaturen

1. Einleitung

Durch die aktuellen Attacken auf Transaktionsanwendungen im Internet, wie diese beispielhaft durch Phishing, Man In The Middle Attacken und Trojanerviren durchgeführt werden, ist es angebracht die tatsächliche Sicherheit von Sicheren Digitalen Signaturen zu hinterfragen und sie mit anderen Transaktionsmodellen zu vergleichen.

Aufbauend auf die Europäische E-Commerce Richtlinie wurde 1998 die Richtlinie für Digitale Signaturen in Kraft gesetzt, die zum Ziel hatte den virtuellen Wirtschaftsstandort Europa sicherer und transparenter für KäuferInnen und BürgerInnen zu machen.

Die Initiative hatte sowohl die tatsächlichen technischen Sicherheitsbedürfnisse, wie auch die juristische Nachvollziehbarkeit und Haftungen im Blickfeld. Nur so konnte die heute nicht mehr wegzudenkende Technologie des Internets auch einen bestehen bleibenden und stabilen Wirtschaftsfaktor ausmachen.

Nationale Legislativen folgten dem Beispiel der Richtlinie und implementierten sowohl in Gesetzen, wie auch den Verordnungen zu diesem Thema, Anforderungsprofile und Haftungsregelungen zur Umsetzung von virtuellen Identitäten denen klar eine Unterschriftsleistung zugewiesen werden kann.

Alle notwendigen technischen Grundlagen und Voraussetzungen für den Einsatz solcher Unterschriften im Elektronischen Datenverkehr, insbesondere in Transaktionsanwendungen, brachte die seit mehr als 20 Jahren erprobte Technologie von Public Key Infrastrukturen mit. Nämlich eine Unterschrift mit der Gewährleistung der klaren Rückverfolgung auf die natürliche Person und die Möglichkeit der Verifikation für einen unbestimmten Empfängerkreis einer solchen Digitalen Signatur.

2. Rechtlicher Rahmen

Als Sichere Signatur kann ausschließlich verstanden werden, wenn es sich um einen als solchen angezeigten Signaturdienst eines Zertifizierungsdiensteanbieters (ZDA) bei einer Aufsichtsstelle handelt, die auf Basis eines der Richtlinie entsprechenden nationalen Signaturgesetzes aktiv ist.

Vergleiche können also, im rechtlichen Sinne, nicht durchgeführt werden, da es sich entweder um eine Sichere Signatur handelt, oder eben nicht. Wie auch in der physischen Welt eine Unterschrift vorliegt, oder eben nicht. Diese Frage ist gänzlich unabhängig von potentiellen technologischen Umsetzungen.

Durch diese Tatsache kann allerdings eine klare Gegenüberstellung, im Sinne der Haftungen, der Sicheren Signatur und den anderen Transaktionsvarianten, bei denen dem Anwender durch eine zusätzliche bilaterale Vereinbarung (Nutzungsvertrag) Transaktionsmechanismen zur Nutzung übergeben werden (z.B.: TAN Verfahren bei E-Banking, Kreditkartenzahlungen im Internet), durchgeführt werden.

Ein Signator (Anwender einer Digitalen Signatur lt. SigG) hat dafür Sorge zu tragen, dass seine technische Einsatzumgebung den Empfehlungen des ZDA entspricht, da der Empfänger einer Sicheren Signatur immer darauf vertrauen darf.

In anderen Worten ist somit der ZDA im Streitfall erste Anlaufstelle für den Empfänger einer Sicheren Signatur und dieser wiederum hat den Beweis anzutreten, dass der Signator sich nicht entsprechend den Empfehlungen bei der Signaturerstellung verhalten hat. Es ist also im ureigenen Interesse des ZDA die bestmögliche Sicherheitstechnologie dem Signator zur Verfügung zu stellen, bzw. eine solche in der Empfehlungsliste nennen zu können.

Der ZDA bedient sich dabei vorliegender Zertifizierungen anerkannter Zertifizierungsstellen, bzw. dementsprechender Gutachten von Bescheinigungs.- oder Bestätigungsstellen, wie auch eigener Technologiebeobachtung. Die Aufsichtsstelle wacht über den Prozess nicht nur als Organwalter, sondern auch in der Rolle als Schlichtungsstelle.

Es ist also aus der Sicht des Anwendungsbetreibers, wie z.B.: die Rolle der Bank im Rahmen der E-Banking Anwendung, nicht notwendig die Haftung gesondert an den Nutzer abzutreten. Der Nutzer (Signator) hat eine solche Nutzungsvereinbarung bereits durch den Signatorvertrag mit dem ZDA unterschrieben.

Im Allgemeinen ist auch keine Vereinbarung zwischen dem, die Digitale Signatur akzeptierenden, Anwendungsbetreiber und dem ZDA notwendig. Die Signatur gilt für gänzlich unbekannte Empfänger. Der ZDA hat für einen kostenlosen Zugang zu Verifikationsmöglichkeiten einer Digitalen Signatur zu sorgen.

Darin ist somit auch ein klarer Unterschied zu Kreditkartentransaktionen zu erkennen, bei denen die Empfänger solcher Transaktionen mit dem Kreditkarteninstitut ebenfalls eine bilaterale Nutzung vereinbaren müssen.

3. Technologische Sicherheit durch Prüfmethoden

Die heute für Sichere Digitale Signaturen zum Einsatz kommenden Technologien erfüllen, wie bereits einleitend erwähnt, die strengen Kriterien der Gesetzgebung und sind nachweislich durch die Zertifizierungen, Bescheinigungen und die Nennung als Empfohlene Komponente des ZDA dem Markt (Signatoren und Empfängern von Digitalen Signaturen) öffentlich zugänglich.

Konkret handelt es sich dabei um die von der EU im Rahmen von Arbeitsgruppen final beschlossenen Common Criteria Zertifizierungen und den Protection Profiles, für die technischen Hard.- und Softwarekomponenten die für eine Sichere Signatur notwendig sind. Ebenso sind klare Signaturumgebungen dafür entworfen worden, aus denen sich die Anwenderinformationen ableiten lassen, die jedem Signator mitgeteilt werden.

Eine Arbeitsplatzumgebung besteht, in der Annahme der prüfenden Stellen aus einem beliebigen System, einem beliebigen Betriebssystem und einer Internetverbindung. Um nun allgemein und jedem Anwender zumutbar eine generelle Sicherheit herzustellen, gilt es dieses System mit einem Anti-Viren-System zu betreiben und sowohl für die Virenscanner-Software, wie auch für das Betriebssystem die jeweils vom Hersteller aktuellsten Updates installiert zu haben.

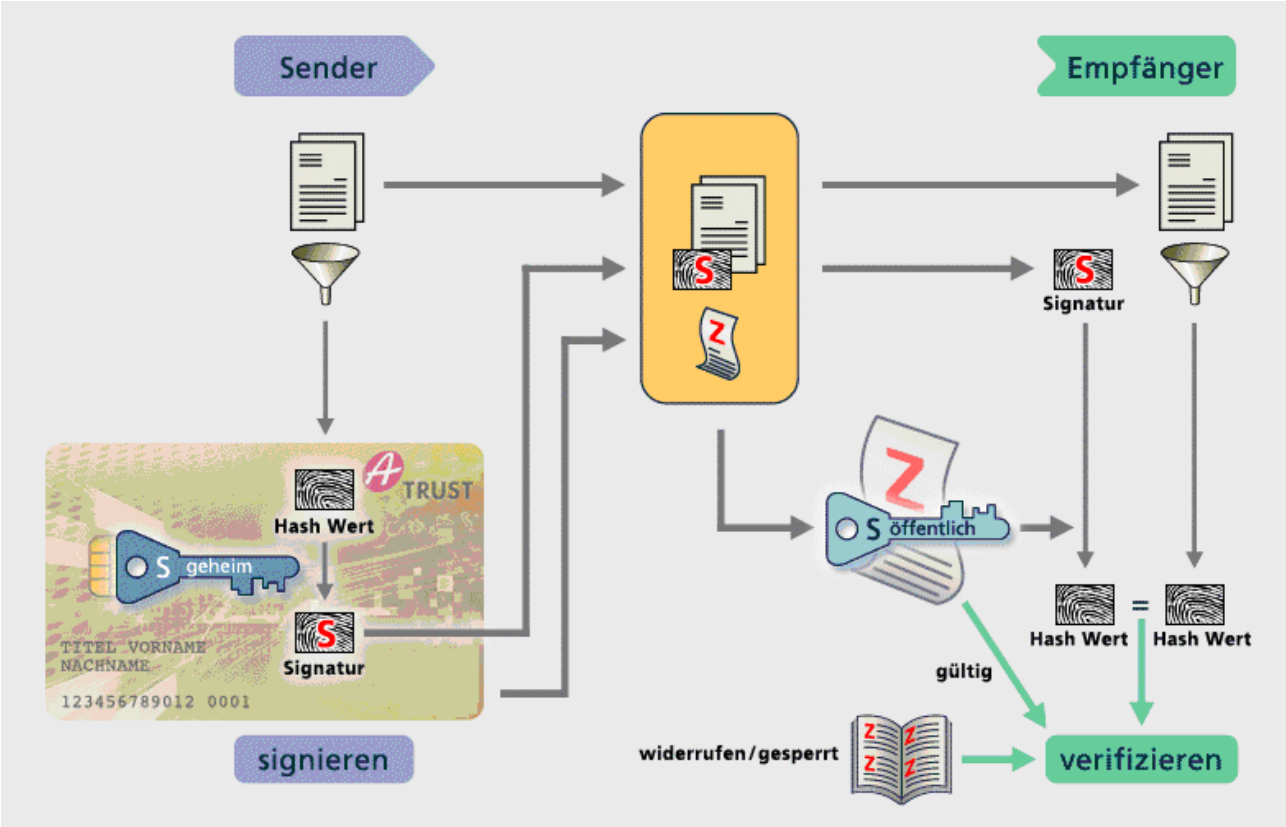
Die Sichere Signaturumgebung besteht aus den Komponenten, die für die Sichere Signaturerstellung notwendig sind:

- ✔ Prozessorchipkarte mit Krypto-Coprozessor
- ✔ Chipkartenlesegerät mit sicherem PIN-Eingabemechanismus
- ✔ Software für die Anzeige der zu signierenden Daten (Secure Viewer)
- ✔ Software für Berechnung der Hashverfahren

D.h.: Diese aufgelisteten Komponenten werden daraufhin geprüft, ob während eines Signaturvorgangs Daten manipuliert werden können, oder eine Signaturauslösung ohne des Wissens des Signators möglich ist.

Solange der Anwender von Sicheren Digitalen Signaturen sich an die Empfehlungsliste des ZDA hält, kann er somit darauf vertrauen, dass die Daten die zur Sicheren Anzeige gelangen auch die Daten sind die signiert werden.

4. Funktionsweise Digitaler Signaturen (auf PKI Basis)



Wie in der Grafik dargestellt gibt es eine eindeutige Relation zwischen der Signatur und dem signierten Dokument. Durch die Sichere Erzeugung des Hashwertes über die zu signierenden Daten und dessen ebenfalls bei der Verifikation zu Tragen kommende Neuberechnung ist eine unbemerkte Veränderlichkeit ausgeschlossen.

Durch die Sichere Digitale Signatur wird zusätzlich noch die Identität des Signators mittels des Zertifikats hinzugefügt.

Entgegen den bereits erwähnten anderen Transaktionsvarianten (TAN, iTAN, TAN-Generatoren, etc.) wird somit nicht ausschließlich eine Autorisierung parallel übermittelt.

Autorisierung der Transaktion und Gewährleistung der Unveränderlichkeit der signierten Daten sind ein und dasselbe sichere Transaktionsverfahren.

5. Sichere Signaturen und aktuelle Bedrohungsszenarien

Wie in Punkt 4 dargestellt, ist die Sicherheitsfunktion von Digitalen Signaturen als Transaktionsverfahren das derzeit bestmögliche System. Wie die Sicheren Signaturen im Lichte der aktuellen Bedrohungen bewähren können, sollen die folgenden Kurzdarstellungen zeigen.

• *Phishing*

Bei Phishing Attacken ist es üblich den Anwender mit vorgetäuschten Begründungen zur Bekanntgabe einer oder mehrerer TANs zu bewegen. Mit diesen TANs werden Autorisierungen im Namen des eigentlichen TAN-Nutzers in betrügerischer Absicht durchgeführt. Den Schaden hat durch die Nutzungsvereinbarung des Anwendungsbetreibers der TAN-Nutzer selbst. (Auch wenn dies im Kullanzfalle anders gelebt wird)

Anwender von Sicheren Signaturen sind durch mehr als eine Komponente vor einem solchen Angriff geschützt:

- ✔ Die Gewährleistung der bewussten PIN-Eingabe zur Erstellung einer Transaktionsautorisierung mittels Sicherer Signaturen
- ✔ Ohne Verfügergewalt über die Chipkarte kann keine Transaktion durchgeführt werden (der TAN ist losgelöst von jeder Hard und Software einsetzbar)

• *Man In The Middle*

Die häufigste Form dieser Art eines Angriffs betrifft jede TAN-Variante (TAN, iTAN, TAN-Generatoren, etc.), da bei diesem Bedrohungsszenario die korrekt vom Anwender durchgeführte Transaktion selbst manipuliert wird. (Es werden also z.B.: Kontodaten auf dem Weg zu Bankanwendung geändert, ohne dass dies für den TAN-Nutzer oder die Bankanwendung erkennbar wäre)

Die Sichere Signatur und die dafür einzusetzenden technischen Verfahren verhindern einen Missbrauch durch:

- ✔ Die Siegelwirkung der Signatur in Zusammenhang mit den signierten Daten. Eine sinnbringende und unbemerkte Änderung der Daten ist durch die kryptografischen Verfahren (Hashing) ausgeschlossen. Die Signatur könnte nach einer Manipulation nicht mehr als gültig dargestellt werden.

• *Trojaner(-viren)*

Unter Trojaner, in Zusammenhang mit IT-Systemen, ist zu verstehen, wenn eine Softwarekomponente auf einem PC unbemerkt vom Anwender installiert wird und diese Autorisierungs-

daten aus spähen und an ein anderes Drittsystem übertragen kann. Vom unbemerkten und unbekannten System aus können dementsprechend jegliche missbräuchlichen Nutzungen mit der Identität des eigentlichen Nutzers durchgeführt werden.

Ebenfalls können Trojaner dafür verwendet werden ein System generell dadurch angreifbar zu machen, in dem diese Manipulationen an installierter Softwarekomponenten vornehmen.

Die grundsätzlichen Parameter für die Erstellung Sicherer Signaturen minimieren in diesem Falle durch folgende Elemente das Risiko:

- ✔ Signaturerstellungsdaten (Privater Schlüssel) auf Chipkarte
- ✔ Nur die PIN-Eingabe am PIN-Pad des Chipkartenlesers erzeugt die Sichere Signatur
- ✔ Die Funktionsweise der Anzeigesoftware (Secure Viewer) zeigt sowohl vor dem Signaturvorgang als auch nach dem Signieren die unterzeichneten Daten an und macht somit transparent, wenn manipulierte Daten zur Unterschrift gelangt sind.

6. Fazit

Die Sichere Signatur stellt die einzige Form von Transaktionssicherheit im Internet dar, die grenzüberschreitend geprüft, unter Aufsichtsmaßnahmen in den Markt gelangt, und die aus technologischer Sicht eine Antwort auf die aktuellen und zukünftigen Bedrohungen bietet.

Klar festzuhalten ist, dass die besten Technologien und Handlungsanweisungen nicht vor der fahrlässigen Nutzung schützen können. Diese sind allerdings bei der Sicheren Signatur so gering und transparent wie bei keiner anderen Transaktionslösung.

Ein Achten auf Aktualität des IT-Systems (PC):

- ✔ Virenschutz (Updates wie auch Scans in regelmäßigen Abständen)
- ✔ Betriebssystem Updates lt. Hersteller

Wie auch das Festhalten an der Empfehlungsliste des ZDA (Software und Kartenleser) bieten eine Sicherheit, die in Form von Sicheren Digitalen Signaturen es Wert ist als eigenhändige Unterschrift in Europa anerkannt zu werden.

Den Anwendungsbetreibern sollte diese Form der Haftungsabgrenzung und die technologische Transaktionssicherheit den notwendigen Rückhalt bieten, die Angebote via Internet auszubauen.

Wie in allen Bereichen, in der ein Schadensfall eine empfundene Katastrophe für den Menschen darstellen kann, ist der Anspruch an die Vertrauenswürdigkeit eines Systems, bzw. eine Organisation enorm hoch.

Bei gelebter Praxis von Sicheren Digitalen Signaturen muss selbstverständlich auch mit dem Schadensfall gerechnet werden. Aufwändige und komplexe Einzelattacken auf IT Systeme und neue Technologien als Bedrohung können nicht gänzlich ausgeschlossen werden. Wie in allen anderen Lebensbereichen in denen vorbeugende Maßnahmen immer nur den bereits bekannten Bedrohungen entgegen wirken kann.

Die Sichere Signatur greift hierfür auf eine einzigartige klare Regelung in Schadensfällen zurück:

- ✔ Akkreditierte Zertifizierungsdiensteanbieter sind verpflichtet bei Bekanntwerden einer neuen Form der Bedrohung umgehend Gegenmaßnahmen im Interesse aller Anwender (Signatoren) einzuleiten. Dies kann in Form von gesicherter Übermittlung von Informationen an die Anwender sein, wie auch in der Neuausgabe von Technologiekomponenten, geschehen.
- ✔ Die Reaktionszeit eines Zertifizierungsdiensteanbieters ist bei Schadensfällen, wie auch bei Betriebsstörungen auf die kürzest lebbaren Zeitfaktoren für die einzelnen Schritte begrenzt.
- ✔ Ein tatsächlicher Schadensfall muss auch seitens des Zertifizierungsdiensteanbieters mit mindestens 1.000.000,- EUR mit einer dementsprechenden Absicherung durch eine Haftpflichtversicherung gewährleistet sein.

- ✔ Durch die gesetzliche Regelung der Schlichtungshierarchie im Streitfall ist eine sachgemäßer Umgang mit dem Sachverhalt geregelt.

Aktuell ist kein einziger Schadensfall in Zusammenhang mit der potentiellen Angreifbarkeit von Sicheren Signaturen in Europa bekannt. Für eine von Technologie abhängige Rechtsmaterie ist dies ein bemerkenswertes Faktum, wenn man den technologischen Fortschritt in einem Zeitraum von nunmehr fast 10 Jahren als Maßstab heranzieht.