Haftungsbeschränkung der digitalen Signatur durch einen Commitment Service

Birgit Baum-Waidner
Entrust Technologies Europe
E-mail: birgit.baum@entrust.com

Zusammenfassung

Der Commitment Service ist ein Notariatsdienst auf einem offenen Netz, z.B. dem Internet. Er enthält eine Registrierungsinstanz für Benutzer und deren öffentliche Schlüssel, und basiert auf einem speziellen Vertrag mit dem Benutzer. Der Commitment Service erlaubt es einem registrierten Benutzer, dem Geschäftspartner eine garantierte Zusicherung zu übermitteln. Eine solche Zusicherung soll auch dann gelten, wenn der Benutzer behauptet, daß seine digitale Signatur gefälscht und die Zusicherung erschlichen wurde. Auf diese Weise kann eine Zusicherung z. B. die Übernahme einer bestimmten Haftung für Schaden beim Empfänger bedeuten für den Fall, daß die digitale Signatur z.B. nach einer Kompromittierung widerrufen wird. Der Commitment Service nimmt hier die Rolle als Zeuge für die Zusicherung (nicht für die digitale Signatur!) wahr und kontrolliert, daß nicht mehr bezeugte Zusicherungen ausgegeben werden als über ein Volumen, das mit dem Benutzer zu Beginn vereinbart wurde. So begrenzt er den schlimmsten Fall für den Benutzer, falls dessen digitale Signatur z.B. durch ein Trojanisches Pferd gefälscht wird. Gleichzeitig ermöglicht er dem Empfänger, sich auf die Zusicherung zu verlassen. Es wird gezeigt, wie dieser Service als Zwischenlösung zum Schutz des Benutzers sowie dessen Geschäftspartner eingesetzt werden kann, solange es noch keine geregelte rechtsverbindliche digitale Signatur gibt, die nicht nur kryptographisch, sondern auch in ihrem Umfeld sicher ist gegen Angriffe. Falls letzteres Problem nicht genügend in Signaturgesetzen und deren Anforderungen berücksichtigt werden sollte, dann könnte sich die vorgeschlagene Lösung auch als Alternative zu einer gesetzlich geregelten digitalen Signatur durchsetzen, indem sie eine vertraglich festgelegte Rechtsverbindlichkeit bietet und gewährleistet, daß ein vom Benutzer definiertes Haftungslimit nicht überschritten wird. Weiterhin kann der vorgestellte Dienst auch allgemeiner genutzt werden, z.B. um nichtabstreitbare Gutscheine zu übermitteln.

1 Einleitung

1.1 Rechtsverbindlichkeit der digitalen Signatur

Eine digitale Signatur [DiHe_76, MeOV_97, BKWG_98] wird derzeit nicht in derselben Weise als rechtsverbindlich anerkannt wie die handschriftliche Unterschrift. Mit wenigen Ausnahmen (z.B. Utah) gibt es noch keine durchsetzbare Regelung ihrer Rechtsverbindlichkeit. Das deutsche Signaturgesetz einschließlich der Verordnungen [DigSigG_97, DigSigV_97] bedeutet zwar einen großen Schritt in diese Richtung, jedoch wird deren Umsetzung noch einige Jahre in Anspruch nehmen. Zudem ist die Haftungsfrage nicht geregelt für den Fall, daß der angebliche Signierer bestreitet, die Signatur erzeugt zu haben. Dies würde im Einzelfall nach Ermessen des Richters entschieden werden. Generell ist die Beweislastumkehr angestrebt, was bedeutet, daß der angebliche Signierer beweisen muß, daß er nicht signiert hat. Dies ist jedoch bei bestimmten Attacken nicht möglich. Daher wird angestrebt, nur solche Komponenten zum Zwecke der Signaturerstellung zu verwenden, mit denen Attacken entdeckt oder sogar mit hoher Wahrscheinlichkeit ausgeschlossen werden können. Weitere kritische Aspekte der Umsetzung werden in [RBHK_94] beschrieben.

Auch in anderen Ländern innerhalb und außerhalb Europas werden derzeit Signaturgesetze erarbeitet. Jedoch besteht das Risiko, daß die resultierenden Gesetze unverträglich miteinander sein und damit für grenzüberschreitende Transaktionen Probleme bereiten könnten. Ein wesentlicher Punkt ist hier die gegenseitige Anerkennung von Zertifizierungsinstanzen über Landesgrenzen hinweg.

Auf Europäischer Ebene wird daher am Entwurf einer Europäische Richtlinie zur 'elektronischen Signatur' [CEC_98] gearbeitet, um hier eine Harmonisierung zu erreichen. Eine Einigung scheitert momentan jedoch vor allem an der Frage der Anforderungen an Signierkomponenten. Es bleibt ungewiß, wann eine Einigung erzielt werden kann.

Abgesehen von Ansätzen aus Deutschland berücksichtigen die bisherigen Initiativen weltweit nur ungenügend [BaZi_99], daß es technische Möglichkeiten gibt, eine digitale Signatur, z.B. mit Hilfe eines Trojanischen Pferdes, zu erschleichen. Ein solcher Angriff mag nicht einmal nachweisbar sein, falls das Trojanischen Pferd sich nach dem Angriff selbst zerstört. Sobald bestimmte Electronic Commerce Anwendungen in breitem Einsatz sein werden und gleichzeitig die digitale Signatur, auf welcher Basis auch immer, rechtsverbindlich sein wird, könnte die Entwicklung solcher Trojanischen Pferde attraktiv für gewisse kriminelle Gruppen werden. Dies könnte je nach Rechtslage dazu führen, daß das Risiko für den Benutzer, den Schaden tragen zu müssen für Aufträge, die er angeblich gegeben hat, jedes vorhersehbare (geschweige denn, akzeptable) Limit überschreitet. Genau diese Gefahr besteht beispielsweise für jeden, der sich derzeit in Utah zertifizieren läßt. Berücksichtigt umgekehrt die Rechtslage die Möglichkeit solche Angriffe, kann dies wiederum bedeuten, daß sich der Empfänger einer Signatur nicht mehr auf deren Gültigkeit ohne weiteres verlassen kann, d.h. nicht sicher vor nachträglichen Überraschungen ist.

Genau dieses Dilemma kann durch Anwendung des hier vorgeschlagenen Commitment Service bis zu einem gewissen Grad gelöst werden. Jedoch soll zunächst auf die möglichen Attacken eingegangen werden.

1.2 Mögliche Attacken auf die digitale Signatur

Zum besseren Verständnis der Problematik soll hier genauer auf mögliche Attacken eingegangen werden. Für eine allgemeine Diskussion wird auf [Webe_97] verwiesen.

Lediglich erwähnt werden sollen die folgenden Attacken:

- Benutzen des Passwords des Benutzers, das auf einem Zettel an seinem Bildschirm oder in der näheren Umgebung hängt.
- Fortsetzen einer Sitzung des Benutzers, der für kurze Zeit seinen Rechner verläßt, jedoch das Password so eingegeben und konfiguriert hat, daß während dieser Zeit keine erneute Eingabe erforderlich ist.
- Erstellen einer Signatur ohne Auftrag des Benutzers, nachdem der Angreifer (oder ein anderer, der ihm die nötige Information direkt oder indirekt weitergegeben hat) schon einmal zuvor erfolgreich – und im Auftrag des Benutzers – eine Signatur an dessen Stelle geleistet hat.

Diese Attacken lassen sich durch den Benutzer selbst durch etwas Disziplin vermeiden.

Weitere Attacken sind:

- Erpressung, d.h. Erzwingen der Signatur des Benutzers, unter Androhung oder Anwendung von Gewalt. Solche Attacken sind ähnlich schwierig vermeidbar sind wie bei der handschriftlichen Unterschrift.
- Brechen der kryptographischen Signierfunktion des Signierers, d.h., die kryptographische Möglichkeit, eine digitale Signatur gegen Wissen und Absicht des Signierers zu erzeugen. Solche Attacken können nur durch die Wahl geeigneter Kryptosysteme mit großer Wahrscheinlichkeit vermieden werden.
- Schlechte Implementierung der Signierfunktion (mit oder ohne Absicht), so daß es einem Angreifer erleichtert wird, eine Signatur zu erzeugen, ohne im Besitz des Schlüssels zu sein. Eine bösartige Variante beispielsweise wäre, wenn ein bestimmtes vom Implementierer definiertes Password für alle Schlüssel funktioniert. In einem solchen Fall stellt sich natürlich die Frage der Produkthaftung, die hier jedoch ausgeklammert wird.
- Zertifizierenlassen eines Schlüssels unter einem falschen Benutzernamen, und Benutzen dieses Schlüssels zum Signieren anstelle des angeblichen Schlüsselbesitzers.
  Solche Attacken können durch vertrauenwürdige Zertifizierungsinstanzen vermieden werden, die sowohl organisatorisch als auch technisch absolut verläßlich sind und insbesondere die Identität eines Schlüsselbesitzers genau prüfen.

Im folgenden soll jedoch auf eine heiklere Klasse von Attacken eingegangen werden, die etwas weniger bekannt ist, und wogegen es schwieriger ist, sich zu schützen. Es geht um die sogenannten “Trojanischen Pferde”, die nicht notwendigerweise in den attackierten Programmen selbst enthalten sind, sondern eher in irgendeinem anderen Programm auf dem Rechner [PPSW_97].

Im folgenden sollen zwei Beispiele genannt werden.

- Wir nehmen an, die digitale Signatur wird auf dem Rechner selbst erzeugt. Der Signierschlüssel ist (verschlüsselt oder unverschlüsselt) auf dem PC gespeichert und liegt zu einem Zeitpunkt unverschlüsselt im Hauptspeicher vor. Die üblichen derzeit verfügbaren PC-Betriebssysteme lassen es im Prinzip zu, daß eine Anwendung eine andere laufende Anwendung beobachten und oft sogar beeinflussen kann. Hier kann ein sogenanntes "Trojanisches Pferd" in eine andere Anwendung eingebaut sein und zum Ziel haben, die Ein- und Ausgaben zwischen dem Benutzer und dem Signierprogramm bzw. dem das Signierprogramm aufrufende Electronic Commerce Programm zu beobachten, obwohl die genannten Programme absolut korrekt sein könnten. So kann in einem ersten Schritt das Password abgefangen werden und in einem nächsten Schritt mit Hilfe dieses Passwords eine Signatur unter einem beliebigen Auftrag erzeugt werden. Diese Attacke benötigt also nicht unbedingt den Signierschlüssel im Klartext. Ist dieser einfach zu bekommen, so lassen sich andere Attacken erzeugen.

- Selbst wenn der Signierschlüssel sowie die Signierfunktion auf der Smartcard gespeichert sind, lassen sich noch Attacken finden. Zum einen kann ein "Trojanisches Pferd" immer noch das Password abfangen, das benötigt wird, um den Signierschlüssel zu aktivieren. Selbst wenn dieses Problem durch ausgeklügelte Mechanismen gelöst wird, z.B. durch Eingabe von PINs und TANs (die man z.B. in Bankanwendungen aber eigentlich gerade mit Hilfe der digitalen Signatur überflüssig machen möchte), bleibt doch eine weitere wirksame Attacke übrig. Sie soll hier die "Fensterattacke" genannt werden: Das Trojanisches Pferd ist hier in eine andere Anwendung eingebaut, die parallel läuft, und beobachtet Eingaben und Ausgaben des Electronic Commerce Programms. Sobald der Benutzer sieht und überprüfen will, was er nun digital zu signieren beabsichtigt, überdeckt das Trojanische Pferd das erwartete Fenster rechtzeitig mit einem gefälschten Fenster, das identisch mit dem zu sein scheint, das der Benutzer erwartet, und auch genau die Angaben zeigt, die der Benutzer digital signieren will. Dies könnte z.B. eine Bestellung bei einem bestimmten Händler über eine bestimmte Ware sein, in bestimmter Stückzahl zu einem bestimmten Preis. Jedoch wird diese Information durch diese Attacke daran gehindert, signiert zu werden. Stattdessen wird eine andere Information „injiziert", so daß der Benutzer ohne sein Wissen etwas anderes digital signiert als er möchte, z.B. eine andere Bestellung zu einer ihm unbekannten Lieferadresse, oder sogar einen Zahlungsauftrag anstatt einer Bestellung.

1.3 Mögliche Abhilfe gegen Attacken durch Trojanische Pferde

Leider erlaubt die typische Rechnerausstattung eines typischen „Internet-Surfers" prinzipiell solche Trojanischen Pferde. Wirksame Maßnahmen wären

- sichere PC-Betriebssysteme, die dafür sorgen, daß Applikationen sich nicht gegenseitig beeinflussen können;
- sichere Geräte, die anstelle von Smartcards verwendet werden und nicht nur den Signierschlüssel speichern, die Signaturfunktion ausführen, sondern darüber hinaus auch anzeigen, was tatsächlich signiert werden wird - unbeeinflußt von der CPU des benutzten Rechners. Dies bedeutet, sichere Geräte benötigen ein sicheres Display. Optimalerweise benötigen sie auch eine Tastatur, so daß eine einfache Eingabe des Passwords möglich ist. Absolut notwendig ist das aber nicht, denn das Display könnte ein Zufallspassword zeigen, das (z.B. durch Auf- und Abscrollen) vom Benutzer auf der Rechnertastatur in das tatsächliche Password überführt werden kann, ohne daß ein Trojanisches Pferd auf dem Rechner dadurch Schlüsse auf das Password ziehen kann.

- Eine weitere Möglichkeit wäre natürlich die Abschottung des benutzten Rechners gegen unbekannte Programme durch Disziplin, so wie es innerhalb mancher Firmen üblich oder zumindest gefordert ist. Es ist jedoch unrealistisch, von privaten Benutzern eine solche Einschränkung generell zu erwarten.

Es liegt auf der Hand, daß die mögliche Existenz der genannten Attacken den eigentlichen Zweck der digitalen Signatur untergraben kann, nämlich ein Nachweis zu sein für eine Willenserklärung des Benutzers. Aus diesem Grund versuchte man in Deutschland den Maßnahmenkatalog für das deutsche Signaturgesetz so hoch zu schrauben, daß die Signaturfunktion mindestens durch eine Smartcard, aber je nach Situation eventuell auch durch ein sicheres Geräte geleistet werden muß.

Auch zum Entwurf der EU Richtlinie versucht Deutschland, den sogenannten „Annex III“ durchzusetzen, der letztlich in seiner Konsequenz sichere Geräte vorschreiben könnte, zumindest da, wo eine Formvorschrift „Schriftlichkeit“ besteht[1] und die digitale Signatur als äquivalent zur handschriftlichen Unterschrift gesehen werden soll. Da sich der Ministerrat bei seiner letzten Tagung am 27. November 1998 nicht auf den vorgelegten Entwurf für die EU Richtlinie geeinigt hat, ist die Fortsetzung der Diskussion zum derzeitigen Zeitpunkt noch unklar. Es hat sich gezeigt, daß Deutschland, Frankreich und Italien eine solche Regelung mit hohen Sicherheitsanforderungen an Signierkomponenten befürworteten, während Großbritannien, die Niederlande, Finnland und Schweden diese Regelung zu hart fanden und die „Wahl der Komponenten dem Markt überlassen“ wollen. Beide Seiten argumentieren, daß die jeweils andere Initiative den Electronic Commerce behindere, einmal durch zu harte Regelungen, die so schnell nicht realisiert werden könnten, beziehungsweise durch fehlende Regelungen, die keine verläßlichen Transaktionen erlaubten. Vor April 1999 wird der Ministerrat die Diskussion nicht fortsetzen. Deutschland hatte bereits im Vorfeld signalisiert, daß es “ohne Annex III keine Direktive” geben werde. Es ist daher durchaus denkbar, daß die EU Richtlinie sich bezüglich der technischen Komponenten weiter in Richtung des deutschen Signaturgesetzes (inkl. Verordnung und Maßnahmenkatalogen) entwickeln wird. Sicher ist zumindest, daß es noch einige Zeit dauern wird, bis eine harmonisierte Gesetzgebung erreicht sein wird.

1.4 Commitment Service als alternative Lösung

Die Lösung, die hier vorgeschlagen wird, ist auch trotz unsicherer Rechnerausstattung des typischen Internet Benutzers anwendbar. Sie verhindert zwar nicht die Angriffe wie oben beschrieben, bietet jedoch Sicherheit für den Benutzer, indem sie sein Risiko vorhersehbar macht und Möglichkeit zur Begrenzung gibt, die der Benutzer selbst bestimmen kann.

Der Commitment Service [Baum_99] begrenzt das Risiko sogar für alle Angriffe, die oben beschrieben wurden: Erpressung ist auch mit einem sicheren Gerät möglich, und sogar in solchen Fällen kann der Commitment Service (sofern die Signatur unter den Regeln des Commitment Service Gültigkeit hat) den Schaden begrenzen – im Gegensatz zur ausschließlichen Verwendung von sicheren Geräten.

---

[1] Im Deutschen wird die schweizerische „Schriftlichkeit“ in diesem Zusammenhang „Schriftform“ genannt

Selbst wenn der Signierschlüssel der Zertifizierungsinstanz (Certification Authority, CA) kompromittiert werden sollte, könnte der Benutzer nachweisen, daß sein Schaden nicht oberhalb einer gewissen Schranke sein kann, sofern er eine Kopie der schriftliche Bestätigung seiner Zertifizierung mit seinem gewählten Limit vorlegen kann und die CA keinen schriftlichen Vertrag mit höherem Limit zeigt.

Als weiterer Vorteil braucht der Commitment Service nicht auf eine Harmonisierung zu warten, sondern er kann praktisch sofort aufgebaut und angewandt werden.

Die hier vorgeschlagene Lösung bietet vor allem Sicherheit für den Signaturempfänger, da ihm Zusicherungen gegeben werden können, auf deren Rechtsverbindlichkeit er sich verlassen kann. Hierfür allerdings ist erforderlich, daß der Signierschlüssel des Commitment Service nicht kompromittiert wird, oder daß der Commitment Service in einem solchen Fall die Haftung übernimmt. Denkbar ist, dass auch er eine gewisse begrenzte Haftung übernimmt und der Rest eben doch zulasten der Signaturempfänger geht. Je mehr Haftung der Commitment Service für die Korrektheit seiner Aktivität übernimmt, desto glaubwürdiger kann der Service gesehen und benutzt werden.

Der Kern des Commitment Service ist eine Registrierungs- und Zertifizierungsinstanz, im folgenden ***Commitment CA*** genannt, von der angenommen wird, daß die Beteiligten ihr trauen.

Ein weiterer Aspekt dieser Lösung ist die Verwendung einer digitalen Signatur des Benutzers, deren Bedeutung und Gültigkeit innerhalb des Vertrag mit dem Commitment Service festgelegt ist und aus dem ausgegebenen Schlüsselzertifikat hervorgeht. Diese Signatur ist vom Schlüsselinhaber widerrufbar, allerdings nur im Falle einer (auch nicht nachweisbaren) Attacke. Man sollte hier also möglichst keine andere digitale Signatur auf demselben Rechner verwenden, die rechtsverbindlich ist und möglicherweise kein begrenztes Haftungslimit hat. Denn sonst könnte ja gerade diese andere Signatur attackiert werden und – unabhängig vom Commitment Service – genau den Schaden beim Benutzer verursachen, den man durch den Commitment Service vermeiden will.

2 Beschreibung des Commitment Service

Der Commitment Service hat Ähnlichkeit mit dem Prinzip der Banken bei Kreditkartenzahlungen (z.B. bei SET [SET_97]) oder Cheques, wenn sie den Händlern die "Authorization Response" erteilen, was bedeutet, daß der Kunde zahlungsfähig ist.

In ähnlicher Weise kontrolliert die Commitment CA die ausgegebenen Zusicherungen des Benutzers, so daß sie einen bestimmten Betrag oder eine bestimmte Menge (je nach Art der Zusicherung) pro Monat nicht überschreiten können. Dies gewährleistet die Schadensbegrenzung bei Attacken für den Benutzer. Wesentliche Unterschiede sind jedoch:

- Es handelt sich nicht um ein Zahlungssystem. Beim Commitment Service kann eine verbindliche Zusicherung unabhängig vom später benutzten Zahlungssystem gemacht werden, auch unabhängig von der Zahlung selbst. Sie wird eindeutig an einen Transaktionskontext und an einen Begünstigten gebunden (zur Vermeidung von 'Double-Spending');
- Beim Commitment Service bestimmt der Benutzer selbst die Höhe seines (monatlichen) Haftungslimits. Das Kreditlimit wird dagegen von der Bank bestimmt und ist vom Kontostand und der Vorgeschichte des Kunden abhängig.

- Beim Commitment Service bestimmt der Kunde selbst die Höhe der ausgegebenen Zusicherungen. Bei Kreditkartenzahlungen dagegen können ohne Wissen des Kunden andere, auch höhere Beträge autorisiert werden, z.B. beim Leihen von Mietwagen oder Reservieren eines Hotelzimmers.
- Beim Commitment Service kann die Signatur widerrufen werden im Falle einer Attacke. Die ausgegebene nichtabstreitbare Zusicherung zeigt dabei jedoch dem Signaturempfänger die Verpflichtung des anderen zu bezahlen, zumindest den in der Zusicherung angegebenen Betrag. Wird dagegen nur eine Zahlungsfähigkeit bestätigt, bedeutet dies nicht notwendigerweise eine Verpflichtung zu bezahlen, schon gar nicht im Falle einer (nachgewiesenen) Attacke.

2.1 Definition der "Zusicherung"

Unter "Zusicherung" wird hier eine rechtsverbindliche Zusicherung verstanden, die vom Benutzer erfüllt werden muß. Ist eine Bedingung mit dieser Zusicherung verknüpft, so muß die Zusicherung erfüllt werden, falls diese Bedingung erfüllt ist. Hierbei kann diese Bedingung aus einem logischen Ausdruck aus mehreren Bedingungen bestehen.

Der Trick besteht darin, daß der Benutzer sich bei seiner Registrierung zu Zusicherungen (z.B. insgesamt 2000 DM pro Monat) durch einen Vertrag mit der Commitment CA verpflichtet, bevor er weiß, wann, an wen, in welcher Stückelung und ob überhaupt manche oder alle Zusicherungen jemals zu irgendeinem Empfänger gelangen und dort erfüllt werden müssen.

Durch diesen Vertrag ist der Benutzer verpflichtet zur Einhaltung aller von der Commitment CA ausgegebenen Zusicherungen, die der Benutzer später veranlaßt. Dies gilt aber auch für ausgegebene Zusicherungen, die der Benutzer nicht veranlaßt hat, z.B. wenn er Opfer einer Attacke wurde. Genau dies macht die Zusicherung verläßlich und wertvoll für den Empfänger. Allerdings muß der Benutzer keine Zusicherungen erfüllen, die von der Commitment CA ausgegeben werden, nachdem sein (monatliches) Limit bereits überschritten wurde oder nachdem er seinen Schlüssel, der für den Request benutzt wurde, bereits zurückgerufen hat.

Gibt die Commitment CA eine Zusicherung aus und gelangt diese in die Hände des spezifizierten Begünstigten, und ist die Bedingung zur Gültigkeit erfüllt (sofern eine spezifiziert wurde), so muß der Benutzer aufgrund des Vertrages die Zusicherung erfüllen. Dies geht für den Empfänger aus der Zusicherung hervor, die de facto aus einem Zertifikat der Commitment CA besteht.

Man kann dies vergleichen mit Blanko-Gutscheinen oder Blanko-Schecks, die die Commitment CA bis zu einem gewissen Limit ausfüllen und ausgeben kann und soll – wenn alles gut geht, im Auftrag des Benutzers. Selbst im Falle einer Attacke beim Benutzer ist dieser zumindest insoweit geschützt als daß sein vordefiniertes Limit (z.B. 2000 DM pro Monat) nicht überschritten wird. Es wird zwar kein Geld ausgegeben, jedoch eine rechtsverbindliche Zusicherung, die auch per Gericht eingeklagt werden kann, aufgrund des vom Benutzer unterschriebenen Vertrags.

2.2 Initialisierung beim Benutzer

Abb.1: Vereinfacht dargestellte Initialisierung

Zu Beginn werden Benutzer und sein Schlüssel beim Commitment Service registriert. Die Commitment CA ist dafür verantwortlich und haftbar, daß die richtige Person registriert wird. Dies ist bei diesem Dienst besonders wichtig, da anschließend Zusicherungen ausgestellt werden, die den Schlüsselinhaber binden.

Der Benutzer legt eine Menge von Zusicherungen fest, die der Commitment Service für eine bestimmte Zeiteinheit (z.B. einem bestimmten Monat) oder insgesamt verwalten soll. Auch kann die Menge der Zusicherung sich auf jeden Monat beziehen, oder es können verschiedene Mengen für verschiedene Monate festgelegt werden.

Beispiele für Zusicherungen sind Geldbeträge, aber es können auch Dinge sein (eine bestimmte Anzahl an Flaschen Wein) oder Dienstleistung (z.B. Stunden an Beratungstätigkeit, Gartenarbeit, Klavierstimmen).

Die Zusicherungen können aus beliebigen Teilmengen der festgelegten Menge der Zusicherungen bestehen. Bei Zusicherungen über Zahlungen dürfen die Zahlungen insgesamt die festgelegte Geldmenge nicht übersteigen.

Gleichzeitig legt der Benutzer für die jeweils möglichen Zusicherungen Bedingungen fest, unter denen ausgegebene Zusicherungen Gültigkeit haben sollen. Eine solche Bedingung kann beispielsweise lauten:

- „gültig nur wenn die Signatur vom Benutzer für kompromittiert erklärt wird", oder
- „gültig nur wenn der Benutzer (z.B. aus finanziellen Gründen) die Transaktion rückgängig machen möchte und dies (z.B. aus Kulanz) akzeptiert wird", oder

- „gültig nur wenn der Signaturempfänger die mit dem Schlüssel *S* digital signierte Information *I* vorlegen kann".
- gültig unter der vom Benutzer beim Request der Zusicherung definierten Bedingung. Hier ist gemeint, daß die Bedingung später vom Benutzer definiert werden kann, sobald es um eine konkrete Zusicherung geht.

Die Gültigkeit einer Zusicherung betrifft nicht das System selbst, sondern nur Signierer und Signaturempfänger. Sie kann theoretisch „blind" durch die Commitment CA bestätigt werden, ohne interpretiert zu werden.

Ein Vertrag mit dem Benutzer legt fest, daß sich der Benutzer zur Erfüllung aller vom Commitment Service ausgegebenen Zusicherungen, unter den jeweils von der CA bestätigten und in der Zusicherung spezifizierten Bedingung, verpflichtet. Dies gilt insbesondere auch für Zusicherungen, die durch Kompromittierung des Signierschlüssels des Benutzers erschlichen wurden, bevor der Schlüssel zurückgerufen wurde. Dies wiederum bedeutet, der Empfänger kann sich die Überprüfung der Gültigkeit des Schlüsselzertifikats ersparen, wenn er eine gültige Zusicherung erhält. Die Notwendigkeit wird verlagert auf die Überprüfung der Commitment CA selbst.

Im Vertrag wird zudem vereinbart, auf welche Weise der Benutzer den Commitment Service veranlassen soll, eine Zusicherung auszugeben, und auf welche Weise der Commitment Service die Anfrage authentisieren soll, z.B. nur das Prüfen der digitalen Signatur des Benutzers einschließlich Prüfen der Schüsselrückrufliste, oder weitergehende Massnahmen zur sicheren Authentifikation, für die im Extremfall der Commitment Service sogar selbst die Verantwortung und Haftung hat. Je nach vereinbartem Verfahren kann der Dienst niedrige oder hohe Kosten verursachen. Ein kombinierter Dienst, z.B. mit verschiedenen Schlüsseln für den Request, oder verschiedene Authentifizierungsmöglichkeiten je nach Höhe der auszugebenden Zusicherung ist ebenfalls denkbar.

2.3 Schlüsselzertifikat

Ein Schlüsselzertifikat wird von der Commitment CA ausgegeben, das den Empfänger einer Signatur darüber informiert, daß der entsprechende Signierschlüssel nur im Rahmen der Vereinbarungen mit dem Commitment Service benutzt wird und gültig ist, insbesondere daß eine Signatur vom Schlüsselinhaber geleugnet werden kann, und daß dagegen eine Zusicherung nicht widerrufen werden kann. Zum Schutz der Signaturempfänger verweist das Zertifikat ebenfalls auf eine Schwarze Liste, die Namen oder Pseudonyme und Schlüssel von Schlüsselinhabern enthält, die innerhalb eines bestimmten Zeitraumes eine Signatur als kompromittiert erklärt haben. Dies bedeutet keine Diskriminierung des Schlüsselinhabers, der eventuell tatsächlich Opfer einer Attacke geworden ist, sondern soll lediglich den Signaturempfänger zur Vorsicht ermahnen vor Geschäftspartnern, bei denen offensichtlich solche Attacken auftreten oder die Attacken vortäuschen könnten. Als Konsequenz könnte der Signaturempfänger im Rahmen seines eigenen Risikomanagements eine höhere Zusicherung aushandeln für den Fall einer (angeblichen) Attacke, die z.B. zusammen mit einer Bestellung geschickt wird. Das Schlüsselzertifikat enthält keine Information über die insgesamt ausgegebenen Zusicherungen.

Schlüsselzertifikate können auf Pseudonyme anstatt auf Namen ausgestellt werden, die jedoch im Disputfall aufgedeckt werden können.

2.4 Schlüsselrückrufliste

Eine Schlüsselrückrufliste wird von der Commitment CA geführt und sofort erneuert, wenn ein Schlüssel zurückgerufen wird (z.B. als kompromittiert gemeldet). Dies ist nicht anders als bei üblichen Zertifizierungsinstanzen. Lediglich wird hier keine Zusicherung mehr ausgegeben, nachdem der Schlüssel zurückgerufen wurde. Es muß wieder eine neue Initialisierung mit neuem Schlüssel vorgenommen werden.

2.5 Anforderung und Ausgabe einer Zusicherung

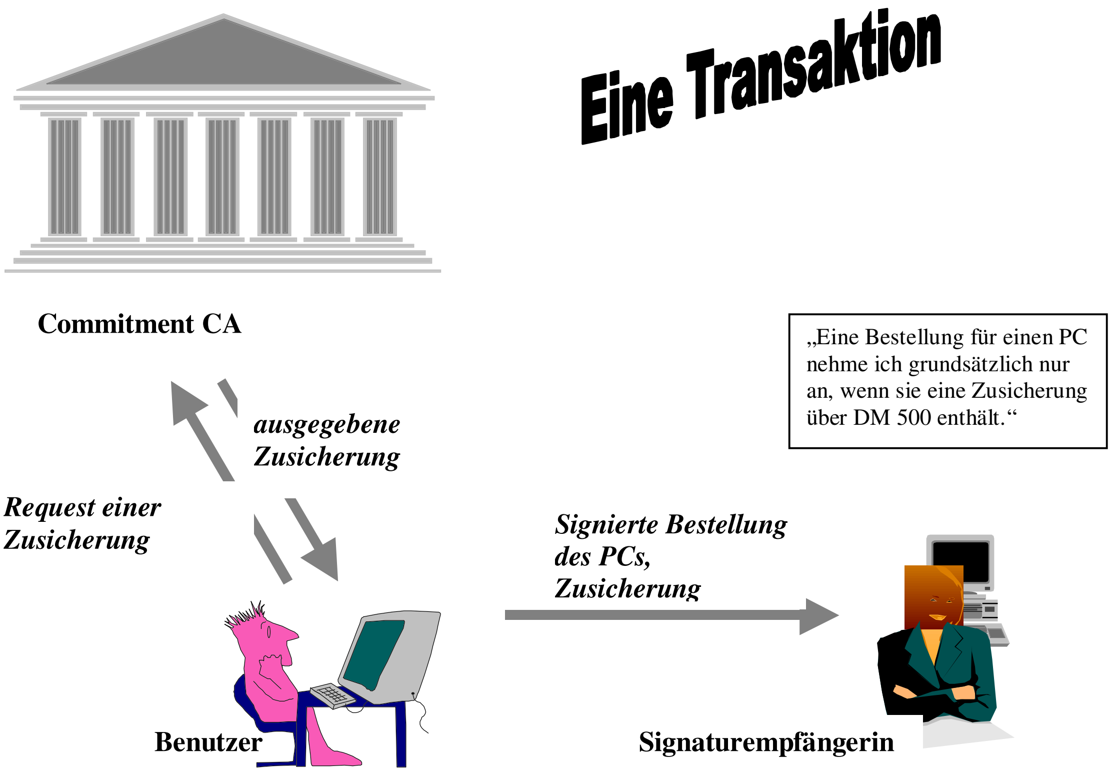

Abb.2: Vereinfacht dargestellte Transaktion

Möchte der Benutzer einem Geschäftspartner eine verläßliche nichtabstreitbare Zusicherung zukommen lassen, so sendet er einen Request an den Commitment Service (siehe Abb.2).

Der Benutzer sichert den Request auf die mit dem Commitment Service vereinbarte Weise, d.h. signiert sie im Normalfall mit dem registrierten Schlüssel, und sendet sie an den Commitment Service.

Der Request könnte folgende Information enthalten:

- Service ID des Benutzers
- Benutzer ID (in der Form, wie sie der Benutzer dem Signaturempfänger zeigen möchte und von diesem verstanden wird)
- hash (
  - Eindeutige Kontext ID spezifiziert durch den Benutzer für die beabsichtigte Transaktion,

    - Eine ID des Signaturempfängers (z.B. der Fingerprint seines öffentlichen Schlüssels)) – die hier gewählte Hashfunktion soll so gewählt werden, daß sie den Inhalt vor der Commitment CA verbirgt. Sie kann auch weggelassen werden, so daß der Inhalt ganz oder teilweise im Klartext vorliegt.
- Betrag, über den eine Zusicherung ausgestellt werden soll (z.B. DM 500)
- Ggf. Bedingung, unter der die Zusicherung gültig sein soll
- Ggf. weitere Transaktionsinformation, die im Klartext oder verschlüsselt im Zusammenhang mit der Zusicherung einen Zeitstempel von der Commitment CA bekommen soll
- Die digitale Signatur des Benutzers über die gesamte Information

Der Commitment Service führt die vereinbarte Authentifizierung aus, prüft insbesondere, ob der verwendete Schlüssel zurückgerufen wurde, prüft weiterhin, ob zu diesem Kontext an diesen Begünstigten, bzw. für den entstandenen Hashwert, nicht bereits eine Zusicherung ausgegeben wurde, ob die angeforderten Zusicherungen insgesamt das vereinbarte Limit bzw. die vereinbarte Menge aller Zusicherungen nicht übersteigen, unter Einrechnung dessen, was bereits ausgegeben worden ist.

Waren alle Überprüfungen erfolgreich, so stellt der Commitment Service ein digital signiertes Zusicherungs-Zertifikat aus (das hier nur „Zusicherung“ genannt wird). Zudem streicht der Commitment Service die ausgegebenen Zusicherungen aus der Menge der Zusicherungen, die noch ausgegeben werden können.

Die Zusicherung kann folgende Information enthalten:

- Seriennummer der ausgegebenen Zusicherung
- Öffentlicher Schlüssel des Benutzers
- Benutzer ID (in der Form, wie sie der Benutzer dem Signaturempfänger zeigen möchte und von diesem verstanden wird)
- hash (
    - Eindeutige Kontext ID spezifiziert durch den Benutzer für die beabsichtigte Transaktion,
    - Eine ID des Signaturempfängers (z.B. der Fingerprint seines öffentlichen Schlüssels))
- Betrag, über den eine Zusicherung ausgestellt wird bzw. werden soll
- Ggf. Bedingung, unter der die Zusicherung gültig sein soll (diese Bedingung kann aus dem Request stammen, oder bereits aus der Initialisierung)
- Ggf. weitere Transaktionsinformation, die im Klartext oder verschlüsselt im Zusammenhang mit der Zusicherung einen Zeitstempel von der Commitment CA bekommen soll
- Datum und Zeit
- Bestätigung daß der obige Schlüssel des Benutzers nicht zurückgerufen wurde
- Signatur der Commitment CA, und Information zur Überprüfung ihres Zertifikats

Das ausgestellte Zusicherungs-Zertifikat wird nun dem Benutzer übermittelt. Dieser kann das Zertifikat überprüfen und weiß im Erfolgsfall, daß sich der Signaturempfänger auf die enthaltene Zusicherung verlassen kann. Letzterer braucht nicht die Schlüsselrückrufliste zu befragen, da das Zusicherungs-Zertifikat dessen Gültigkeit (zum Zeitpunkt der Ausgabe) bestätigt - auch nach einem Rückruf des Schlüssels ist der Benutzer an seine Zusicherung gebunden, wenn sie vor dem Rückruf ausgestellt wurde.

Ein Zusicherungs-Zertifikat kann im Kontext einer eigens dafür spezifizierten Transaktionen als nichtabstreitbarer Gutschein dienen. Eine Bedingung könnte hier lauten „sobald Du Geburtstag hast“.

Wenn man Probleme bei der Nachweisbarkeit des zustandegekommenen Vertrags befürchtet (z.B. wenn er mündlich zustandegekommen ist), kann der Händler Zusicherungen über den zu bezahlenden Preis anfordern. Die Bedingung des Signierers könnte hier lauten „sobald die Leistung durch die Gegenseite erbracht wurde“. Der Händler könnte damit die Bezahlung gerichtlich erzwingen.

3 Haftungszertifikat-Service

3.1 Haftungszertifikat-Service als Sonderfall des Commitment Service

Der Haftungszertifikat-Service ist ein Sonderfall des Commitment Service. Er ist speziell dazu gedacht, eine Haftung für eine digitale Signatur zu spezifizieren für den Fall, daß der Schlüssel (angeblich oder tatsächlich) kompromittiert wurde. Diese Haftung wird mit Hilfe einer Zusicherung, des Haftungszertifikats, ausgedrückt.

Der wesentliche Charakter des Haftungszertifikat-Service liegt in der speziellen Bedeutung der Zusicherungen, also in der Semantik des Services. Nehmen wir als Beispiel die Bestellung einer Sonderanfertigung eines PCs, Kosten 3.500 DM.

Beim allgemeinen Commitment Service könnte eine Zusicherung folgendermaßen lauten: „500 DM für Transaktionskontext *k* an Empfänger *E*, gültig nur, wenn die Signatur vom Signierer als kompromittiert gemeldet wird und die Transaktion dadurch nicht zustande kommt.“ Da die Signatur durch den Vertrag mit dem Commitment Service sowieso als kompromittiert erklärt werden kann und in diesem Fall nicht gültig ist, hat der andere als Entschädigung zumindest eine Zusicherung über 500 DM, die er auf jeden Fall bekommt, unabhängig vom tatsächlichen Schaden.

Beim Haftungszertifikat-Service würde die Zusicherung dagegen wie folgt lauten: „je nach Schaden beim Empfänger *E* ***Haftung bis zu*** 500 DM für Transaktionskontext, gültig nur, wenn die Signatur vom Signierer als kompromittiert gemeldet wird und die Transaktion dadurch nicht zustande kommt.“

Der Unterschied ist, in letzterem Fall handelt es sich um eine Haftung des Schlüsselinhabers für die Transaktion, die mit seinem Schüssel signiert wurde, und zwar für den Schaden, der im Falle der Kompromittierung der Signatur durch deren Widerruf beim Empfänger entstanden ist – und zwar nur bis zu einer Höhe von 500 DM. Beträgt der Schaden nur 240 DM (Versandkosten plus Aufwand), so beinhaltet die Zusicherung nur eine Verpflichtung, 240 DM zu erstatten. Die tatsächliche Verpflichtung kann durch Einigung (z.B. mit Hilfe von Nachweisen) oder vor Gericht festgelegt werden, jedoch kann sie 500 DM nicht überschreiten.

Ebensogut kann die Verwendung von Haftungszertifikaten auch unter anderen Bedingungen vereinbart werden, z.B. wenn man erlaubt, die Transaktion (nicht die Signatur) zu widerrufen. Dies ist unüblich in normalen Geschäftsvorgängen, jedoch könnte der Haftungszertifikat-Service die Zustimmung des Geschäftspartners zum

Widerruf einer Bestellung erleichtern. All diese Konditionen sollten zur Vereinfachung bereits vor Abschluß des Vertrages geklärt werden, z.B. kann die Art der Zusicherung, die durch das Haftungszertifikat bestätigt werden soll, zuvor ausgehandelt werden. Beim Haftungszertifikat-Service würde die Zusicherung entsprechend wie folgt lauten: „je nach Schaden beim Empfänger E ***bis zu*** 500 DM für Transaktionskontext *k*, gültig nur, wenn die Transaktion aus Gründen, die beim Schlüsselinhaber liegen, nicht zustande kommt.“

Die Menge der zu Beginn vereinbarten Zusicherungen besteht hier in einem Maximalbetrag der insgesamt auszugebenden Haftungszertifikate, absolut oder z.B. pro Monat. So mag ein Benutzer sein monatliches Haftungslimit auf DM 1500 festlegen, während er ein anderes Limit für andere Varianten des Commitment Services festlegen kann. Services und Limits können natürlich auch miteinander kombiniert werden.

Eine benutzerspezifizierte Bedingung zur Gültigkeit der Haftungszusicherung gibt es beim Haftungszertifikat-Service, im Gegensatz zum Commitment Service, jedoch nicht.

3.2 Nutzung des Haftungszertifikat-Service zur Sicherung der digitalen Signatur

Eine Sicherung der digitalen Signatur kann im Prinzip auch mit dem allgemeinen Commitment Service erreicht werden, jedoch ist es naheliegend, es mit Hilfe des Haftungszertifikat-Service zu erläutern.

Wie zuvor nehmen wir an, daß der öffentliche Schlüssel des Schlüsselpaares zum Signieren bei keiner anderen Zertifizierungsinstanz registriert und zertifiziert wird als bei dem hier vorgestellten Haftungszertifikat-Service - es sei denn, die dort geltenden Regeln und Policies stehen nicht mit diesen in Konflikt.

Aus dem Schlüssel-Zertifikat muß hervorgehen, daß der entsprechende Signierschlüssel nur im Rahmen der Vereinbarungen mit dem Haftungszertifikat-Service (bzw. auch dem Commitment Service) benutzt wird und Gültigkeit haben soll. Dies soll dazu beitragen, daß ein Gericht im Streitfall nicht anderweitig entscheidet.

Der Vertrag mit dem Haftungszertifikat-Service enthält die folgenden Vereinbarungen:

- Der Benutzer erklärt explizit, daß er an alles gebunden ist, was er mit diesem Schlüssel digital signiert, ebenso wie er sich an seine handschriftliche Unterschrift gebunden fühlt.
- Der Benutzer erklärt, daß er bis zum vereinbarten Limit an alle Haftungszertifikate gebunden ist, die vom Haftungszertifikat-Service auf seinen Namen ausgestellt werden, auch wenn er deren Ausstellung nicht veranlaßt hat (d.h. wenn sein Schlüssel kompromittiert wurde).
- Der Benutzer ist nur begrenzt gebunden an digitale Signaturen, die zwar mit seinem Signierschlüssel erzeugt wurden, von denen er aber bestreitet, sie gemacht zu haben - unabhängig davon, ob man ihm dies nachweisen kann oder nicht. In solchen Fällen haftet der Benutzer dem Geschäftspartner gegenüber bis zu dem Betrag, der im beigefügten Haftungszertifikat für diesen Transaktionskontext steht.
- Je nach Policy erklärt sich der Benutzer einverstanden, daß sein öffentlicher Schlüssel auf eine Schwarze Liste gesetzt wird, wenn sein Schlüssel

kompromittiert wurde und dadurch ein anderer über die Deckung des Haftungszertifikats hinaus geschädigt wurde.

Die Sicherung der digitalen Signatur für den Empfänger besteht ausschließlich im beigefügten Haftungszertifikat. Die digitale Signatur selbst ist widerrufbar. Jedoch bietet beides zusammen eine Sicherung der digitalen Signatur gegenüber dem Empfänger, erst recht wenn die Haftungshöhe auch dem Transaktionsvolumen entspricht.

Die Haftung, die der Benutzer pro Monat bereit ist einzugehen, entspricht genau seinem Spielraum, Haftungszertifikate den Empfängern zukommen zu lassen. Insofern hat der Benutzer einen Trade-off zwischen erhöhtem Risiko und guten Möglichkeiten den Geschäftspartner zufriedenzustellen, und einem niedrigeren Risiko mit weniger Möglichkeiten.

Streitigkeiten außerhalb dieser Vereinbarung sind außerhalb dieses Kontexts zu behandeln, z.B. Strafverfolgung des Attackers und Entschädigung durch ihn, oder Strafverfolgung des Signierers wegen Betrugs, z.B. wenn man durch Zeugen oder andere Beweise nachweisen kann, daß er tatsächlich signiert hat.

Selbst für Aktiengeschäfte kann dieser Service verwendet werden. Hierbei wird der Broker generell ein Haftungszertifikat verlangen, das weit über dem erwarteten Verlust liegt, falls er die Transaktion im Falle einer Attacke rückgängig machen sollte. Umgekehrt kann ein Broker bei einem teuren kostenpflichtigen Service seine ausgegebene Information mit Haftungszertifikaten an bestimmte Benutzer unterlegen, die er im Falle von Irrtümern, oder auch im Falle einer Attacke auf seiner Seite, einlösen muß. Dies könnte den Service des Brokers verteuern, da sein Haftungsvolumen mit wachsender Zahl von Abfragen zunimmt.

4 Mögliche Varianten

Aus Platzgründen sollen einige denkbare Varianten nur erwähnt werden.

Natürlich kann der Request auch durch den Signaturempfänger erfolgen, jedoch muß diese durch den Schlüsselinhaber selbst spezifiziert und autorisiert werden. Der Nachteil ist, daß der Benutzer weniger Kontrolle hat, wieviele Zusicherungen bereits ausgegeben wurden, und daß eine Anonymität der Transaktion inklusive des Geschäftspartners gegenüber der Commitment CA schwieriger zu bewerkstellen ist, was dagegen in der vorgestellten Variante durch Anwenden einer Hashfunktion leicht erreicht werden kann.

Durch Einschließen des Requests des Benutzers in die Zusicherung kann der Benutzer vor unberechtigt von der Commitment CA ausgegebenen Zusicherungen geschützt werden.

Weiterhin können sowohl der Request als auch die Zusicherung auf anderen Wegen als dem Internet erfolgen, ebenso die Übermittlung der Zusicherung zum Signaturempfänger. Beispielsweise könnte der Request telefonisch erfolgen, die Zusicherung könnte gefaxt werden, und der Benutzer – der zu diesem Zweck nicht einmal einen Signierschlüssel bräuchte – könnte die Zusicherung weiterfaxen innerhalb einer Bestellung per Fax, die vom Empfänger eingescannt werden kann. Dies bedeutet: Die handschriftliche Unterschrift auf einem Fax, deren Rechtsverbindlichkeit sowieso fragwürdig ist, kann “aufgewertet” werden durch eine aufgedruckte, von der Commitment CA digital signierte, nichtabstreitbare Zusicherung. Oder man kann eine Zusicherung telefonisch bestellen, die vom

Commitment Service elektronisch zum Empfänger gesandt wird. Auf diese Weise können telefonische Bestellungen für den Empfänger höchst wirksam gesichert werden. Dies zeigt, daß der Commitment Service auch völlig losgelöst von registrierten Schlüsseln existieren kann und auch ohne Signaturen auskommt.

Der Commitment Service kann unter veränderter Semantik auch, z.B. von einer Bank, als "Solvency" Service, oder als "Commitment- and Solvency" Service betrieben werden. Der Solvency Service würde Zahlungsfähigkeit bescheinigen, jedoch nicht die Verpflichtung zu bezahlen. Beim Commitment Service ist dies genau umgekehrt.

5 Wer hat Interesse am Commitment Service

Wer würde Interesse daran haben sollte, einen solchen Commitment Service zu betreiben, und wer würde ihn nutzen?

Es liegt auf der Hand, daß es vor allem die Händler auf dem Internet sind, die davon profitieren, denn sie können nicht nur den Besteller identifizieren, sondern sich sogar vor dessen Abstreiten der Bestellung schützen, indem sie eine rechtsverbindliche Zusicherung über einen Betrag verlangen, der ihrem Schaden entsprechen würde. Dies wird dem Händler bereits dieselbe Sicherheit bieten wie wenn Signaturgesetze mit hochsicheren Komponenten in Anwendung wären. Ein weiterer Vorteil ist, daß eine Zusicherung die Abfrage erspart, ob der Schlüssel des Bestellers bereits widerrufen wurde – die Notwendigkeit diese Abfrage wird verlagert auf das Prüfen, ob die Commitment CA selbst mittlerweise Opfer einer Attacke geworden ist, was hoffentlich sehr unwahrscheinlich ist. Der generelle Bedarf der Händler an einer rechtsverbindlichen digitalen Signatur ihrer Kunden liegt auf der Hand. Widerruft der Besteller seine Bestellung (was er ohne digitale Signatur oder handschriftliche Unterschrift ohne weiteres kann, indem er behauptet, er habe das nicht bestellt), so hat heute der Händler das Nachsehen.

Daher liegt es nahe, daß eine Interessensgemeinschaft der Händler einen Commitment Service betreibt, z.B. die Industrie- und Handelskammern, und zwar möglichst im Zusammenhang mit bereits existierenden CAs, die diesen Dienst als Zusatzdienst anbieten könnten. Die Ausstellung der Zertifikate kann kostenpflichtig für den Benutzer sein, dies sollte jedoch durch den Preis oder durch günstige Konditionen beim Händler wieder ausgeglichen werden.

Etwas weniger reizvoll scheint dieser Service für den Benutzer selbst, da ein gewisses Risiko eingegangen werden muß, nämlich geradezustehen für Zusicherungen, die durch Attacken zustandegekommen sind. Jedoch muß man die Alternative betrachten, nämlich eine rechtverbindliche digitale Signatur womöglich ohne generelles Haftungslimit, so daß der Schaden im Falle einer Attacke – die möglicherweise gar nicht nachgewiesen werden kann – wesentlich größer sein kann als der begrenzte Schaden, der beim Commitment Service eintreten kann, da dort die digitale Signatur in diesem Fall einfach widerrufbar ist. Für den Preis eines selbstgewählten Risikos bietet der Commitment Service dem Benutzer eine hohe Sicherheit und gleichzeitig die Möglichkeit, auch dem Händler eine gewisse Sicherheit zu bieten. Es ist abzusehen, daß viele Händler rechtsverbindliche digitale Signaturen vom Kunden verlangen werden, sobald der gesetzliche Rahmen hierfür geschaffen sein wird. Zusicherungen plus widerrufbare Signaturen (im Falle einer Attacke) können diese rechtsverbindlichen Signaturen ersetzen.

Diese Arbeit entstand im Rahmen des ACTS Projekts SEMPER (http://www.semper.org) und wurde gefördert durch die Europäische Kommission und dem Schweizerischen Bundesamt für Bildung und Wissenschaft.

6 Literatur

Baum_99 Birgit Baum-Waidner: Limiting Liability in E-commerce, Chapter 13 in SEMP_99.

BaZi_99 Birgit Baum-Waidner, Rita Zihlmann: Legal Aspects, Chapter 14 in SEMP_99.

BKWG_98 Wendelin Biser, Heinrich Kersten, Bruno Wildhaber, Matthias Gut: Chipkarte statt Füllfederhalter. Hüthig GmbH, Heidelberg. ISBN 3-7785-2634-0.

CEC_98 Entwurf für EG-Richtlinie über gemeinsame Rahmenbedingungen für elektronische Signaturen, Vorschlag für eine Richtlinie des Europäischen Parlaments und des Rates KOM(1998)297/2, 98/0191 (COD), deutsche Fassung, vorgelegt am 22. Juni 1998

DigSigG_97 Gesetz zur Regelung der Rahmenbedingungen für Informations- und Kommunikationsdienste (Informations- und Kommunikationsdienste-Gesetz - IuKDG), Artikel 3: Gesetz zur digitalen Signatur (Signaturgesetz - SigG) vom 22. Juli 1997 (BGBl. I S.1870)

DigSigV_97 Verordnung zur digitalen Signatur (Signaturverordnung - SigV) in der Fassung des Beschlusses der Bundesregierung vom 8. Oktober 1997

DiHe_76 Whitfield Diffie, Martin E. Hellman: New Directions in Cryptography. IEEE Transactions on Information Theory 22/6 (1976) 644-654

MeOV_97 Alfred J. Menezes, Paul C. van Oorschot, Scott A. Vanstone: Handbook of Applied Cryptography; CRC Press, Boca Raton 1997.

PPSW_97 Andreas Pfitzmann, Birgit Pfitzmann, Matthias Schunter, Michael Waidner: Trusting Mobile User Devices and Security Modules; in Computer 30/2 (1997) 61-68.

RBHK_94 Alexander Rossnagel, Johann Bizer, Volker Hammer, Christel Kumbruck, Ulrich Pordesch, Heinz Sarbinowski, Michael J. Schneider: Die Simulationsstudie Rechtspflege - Eine neue Methode zur Technikgestaltung für Telekooperation, Projektgruppe Verfassungsverträgliche Technikgestaltung e. V. (Provet), Gesellschaft für Mathematik und Datenverarbeitung mbH (GMD), Edition Sigma, Berlin, 1994, ISBN 3-89404-373-3

SEMP_99 Gerard Lacoste, Michael Steiner, Michael Waidner (Hrsg): Secure Electronic Marketplace for Europe – Final Report of Project SEMPER; LNCS, Springer-Verlag, to appear.

SET_97 Mastercard Inc., Visa Inc.: Secure Electronic Transactions (SET) Version 1.0; May 31, 1997.

Webe_97 Arnd Weber: Zur Notwendigkeit sicherer Implementation digitaler Signaturen in offenen Systemen; in: Müller, Günter; Pfitzmann, Andreas (Hrsg.): Mehrseitige Sicherheit in der Kommunikationstechnik. , Addison-Wesley-Longman 1997, 465-478.