Ein Service zur Haftungsverteilung für kompromittierte digitale Signaturen

Birgit Baum-Waidner

Entrust Technologies Europe, Glatt Tower, CH-8301 Glattzentrum/Zurich, birgit.baum@entrust.com

Zusammenfassung

Wenn eine digitale Signatur vom Schlüsselinhaber für kompromittiert erklärt wird, ist es nicht notwendigerweise möglich zu entscheiden, ob sie tatsächlich kompromittiert wurde. Dies kann zu Fehlurteilen führen, was Risiken sowohl für den Schlüsselinhaber als auch für denjenigen birgt, der sich auf die Signatur verläßt. In dieser Arbeit wird der sogenannte „Commitment Service“ vorgestellt, der es ermöglicht, eine digitale Signatur so zu nutzen, daß für alle an der Transaktion Beteiligten das Risiko zu begrenzt ist.

1 Einleitung

Die Sicherheit einer digitalen Signatur basiert auf

- der kryptographischen Sicherheit (Nicht-Brechbarkeit) des Signieralgorithmus
- der Sorgfalt des Benutzers
- der Verläßlichkeit und Vertrauenswürdigkeit der Zertifizierungsinstanz, die durch Zertifikate bestätigt, mit wessen Schlüssel signiert wurde
- der Annahme, daß die Signierkomponenten des Benutzers keine Attacken erlauben, die ohne Wissen und Veranlassung des Benutzers das Signieren beliebiger Information erlauben.

In den meisten Publikationen über „Public Key Infrastructures“ (PKIs) sowie in den meisten Regelungen zur digitalen Signatur findet man nur die ersten drei Punkte berücksichtigt, der vierte wird weitgehend ignoriert. Jedoch wird gerade dieser Punkt um so relevanter, je eher die betrachteten Szenarios das Internet und dessen Benutzer miteinschließen. Bereits heute werden Privatpersonen und Organisationen Opfer von Angriffen sogenannter „Trojanischer Pferde“, die typischerweise (aber nicht ausschließlich) durch das „Herunterladen“ und Installieren von Programmen auf den Rechner des Benutzers gelangen. Solche Angriffe, die eine Signatur des Benutzers erschleichen, sind nicht notwendigerweise nachweisbar, da sie die Beseitigung der Spuren nach vollbrachter Tat miteinschließen können. Angriffe dieser Art können sich nur vermeiden bzw. erkennen lassen, wenn die Signaturfunktion und die Darstellung des unterschriebenen Inhalts ein sicheres Betriebssystem benutzen oder zumindest mit sicherer Hardware (inklusive Display) durchgeführt wird, so daß die Funktionalität abgeschirmt von äußeren Einflüssen ist. Jedoch ist weder das eine noch das andere derzeit mit der Sicherheit verfügbar, wie sie zu diesem Zweck notwendig wäre. Andererseits eröffnet gerade diese Tatsache unehrlichen Parteien die Möglichkeit, Angriffe vorzutäuschen, was die Rechtsunsicherheit weiter vergrößert.

In dieser Arbeit wird die resultierende Haftungssituation für kompromittierte Signaturen analysiert und gezeigt, daß die derzeitige Situation nicht für den Signierer und gleichzeitig für den Signaturempfänger akzeptabel sein kann. Zur Lösung wird ein sogenannter „Commitment Service“ vorgeschlagen, der eine faire Verteilung der Haftung erreicht, so daß das Risiko sowohl für den Signierer als auch für den Signaturempfänger einschätzbar und tragbar ist. Dieser Dienst kann sowohl als Online-Service wie auch durch Smartcards realisiert werden. Da mit limitiertem Risiko auch die Flexibilität des Schlüsselinhabers beschränkt wird, kann diese Lösung zumindest als praktikabler Kompromiß verstanden werden, solange bis jeder Schlüsselinhaber entweder ein sicheres Betriebssystem benutzt oder aber sichere Hardware zur Erzeugung der digitalen Signatur zur Verfügung hat. Zudem ist es die einzige bisher vorgeschlagene Lösung, die für alle involvierten Parteien für den derzeitigen Stand der Technik akzeptabel sein kann.

Produkthaftung wird hier ausgeklammert, da sie zusätzlich und separat geregelt werden sollte. Jedoch kann erwartet werden, daß die hier betrachteten Attacken eher darauf zurückzuführen sind, daß verwendete Betriebssysteme Attacken nicht verhindern, als beispielsweise auf ein fehlerhaftes Produkt zur Signaturerzeugung.

1.1 Rechtsverbindlichkeit der digitalen Signatur

Eine digitale Signatur [DiHe_76, MeOV_97, BKWG_98] wird derzeit nicht als rechtsverbindlich anerkannt in der Weise wie eine 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 Monate in Anspruch nehmen. Zudem ist die Haftungsfrage bisher nicht geregelt für den Fall, daß der angebliche Signierer bestreitet, die Signatur tatsächlich selbst erzeugt zu haben. Dies würde im Einzelfall nach Ermessen des Richters entschieden werden. Generell ist eine Beweislastumkehr angestrebt, was bedeutet, daß der angebliche Signierer beweisen muß, daß er nicht signiert hat. Dies würde ihm jedoch bei bestimmten Attacken gar nicht möglich sein, so daß er den Beweis für seine Aussage schuldig bliebe. Daher strebt man an, 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. Dies führt dazu, 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 Europäischen Richtlinie zur ‘elektronischen Signatur’ [CEC_98] gearbeitet, um hier eine Harmonisierung zu erreichen. Eine Weiterentwicklung dieses Entwurfes liegt dem Europäischen Parlament vor. Er beinhaltet Regelungen für eine Signatur, die der handschriftlichen äquivalent sein soll und sichere Geräte vorschreibt sowie Regelungen für eine weniger harte Signatur, deren Rechtsverbindlichkeit und Haftung sich durch den Markt selbst regulieren soll. Bei letzterem ist beabsichtigt, daß es Urteile zulasten des Schlüsselbesitzers geben wird, wenn man der Zertifizierungsinstanz keinen Fehler nachweisen kann, sie beispielsweise den Schlüssel-

besitzer auf die Möglichkeit von Attacken aufmerksam gemacht hat. Dies erscheint jedoch bedenklich für eine breite Anwendung im Electronic Commerce, solange sich der Schlüsselbesitzer technisch gar nicht vor solchen Attacken schützen kann. 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 Attacken 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. 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 ohne weiteres auf deren Gültigkeit verlassen kann, d.h. nicht sicher vor nachträglichen Überraschungen ist.

Dieses Dilemma soll durch Anwendung des hier vorgeschlagenen Commitment Service bis zu einem gewissen Grad gelöst werden. Gleichzeitig schützt der Commitment Service sogar vor Schaden im Falle von Erpressung und Attacken, die unabhängig von der technischen Sicherheit der digitalen Signatur sind. Für eine allgemeine Diskussion möglicher Attacken durch eigene Unachtsamkeit bis hin zu Trojanischen Pferden sei auf [PPSW_97, Webe_97, Baum_99] verwiesen.

1.2 Risiken durch die digitale Signatur

Selbst mit großer Sorgfalt lassen sich Attacken durch Trojanische Pferde nicht ausschließen. Mit der Bereitschaft, sich einen Schlüssel zur digitalen Signatur zu besorgen und zertifizieren zu lassen, sowie mit der Entscheidung, sich auf digitale Signaturen zu verlassen, sind daher gewisse Risiken verknüpft.

Entsteht ein Disput zwischen angeblichem Sender und Transaktionsempfänger, weil der Sender bestreitet, die vorliegende Transaktion (z.B. eine Bestellung, ein Auftrag) veranlaßt zu haben, so könnte dieser Disput in bestimmten Fällen vor Gericht gelangen. Leider ist es zum heutigen Zeitpunkt nicht möglich, richterliche Entscheidungen annähernd zuverlässig vorherzusagen, da Urteile dieser Art bisher nicht genügend vorliegen. Es ist außerdem zu erwarten, daß durch die neue mit dem Internet und dessen Risiken verbundene Sachlage mancher Richter überfordert ist: das Somm-Urteil [Somm_98] ist ein Beispiel für eine unsachgemäße Entscheidung eines Richters, obwohl in diesem Fall sachgemäße Gutachten vorlagen. Jedoch mag es in der hier betrachteten Situation technisch gar nicht möglich sein, zu beurteilen, ob die Signatur tatsächlich kompromittiert wurde oder nicht. Es gibt daher die folgenden Möglichkeiten:

	Signatur tatsächlich von Schlüsselinhaber	Signatur kompromittiert
Richter entscheidet: „Signatur echt“	ok	Problem für Schlüsselinhaber
Richter entscheidet: „Signatur gefälscht“	Problem für Transaktionsempfänger	ok

1.2.1 Mögliche Regelungen und resultierende Risiken

Nun betrachten wir die Situation von einer anderen Seite: Wir nehmen an, die richterliche Entscheidung sei durch eine klare Regelung vorhersehbar. Zur Vereinfachung unterscheiden wir die folgenden Lösungen für Regelungen, um die Risiken der einzelnen Parteien genauer betrachten zu können:

a) Der angebliche Signierer ist immer haftbar für seine digitale Signatur, auch im Falle einer Attacke. Dies bedeutet, es nützt ihm nichts, seine Signatur zu leugnen.
b) Der angebliche Signierer kann seine Signatur immer leugnen, ohne haftbar gemacht zu werden. Dies bedeutet, er kann sie auch leugnen, obwohl er sie tatsächlich geleistet hat.
c) Der angebliche Signierer ist haftbar für seine digitale Signatur, auch im Falle einer (auch angeblichen) Attacke, jedoch in diesem Fall nur bis zu einem bestimmten Limit (beispielsweise im Bereich von EURO 500, EURO 5.000 für Privatleute, EURO 50000, EURO 500.000, EURO 5.000.000 für Unternehmen). Selbstverständlich muß nach einer (angeblichen) Attacke der Schlüssel zurückgerufen werden.

Die Risiken dieser Regelungen a, b, c sind für die jeweiligen Parteien in folgender Tabelle skizziert. Man beachte die Felder unten rechts, die zeigen, daß die Einführung eines Haftungslimits nicht genügt.

	a) Schlüsselinhaber immer haftbar	b) Schlüsselinhaber niemals haftbar	c) Schlüsselinhaber bei (angeblicher) Attacke bis zu bestimmtem Limit haftbar
Risiken für Schlüssel-inhaber	• Haftbar ohne Limit auch als Opfer einer Attacke (z.B. bestehend aus Hunderten von Transaktionen)	• Kein Haftungsrisiko	• Haftungsrisiko im Falle einer Attacke bis zum Limit
Risiken für Empfänger	• Kein Risiko	• Volles Risiko für alle entgegengenommen en Transaktionen	• Fast volles Risiko, da das Limit des Senders bereits überschritten sein könnte.
Fazit	Unakzeptabel für Schlüsselinhaber, jedoch gut für den Empfänger	Gut für den Schlüsselinhaber, jedoch schlecht für den Empfänger	Akzeptabel für den Schlüsselinhaber, jedoch immer noch schlecht für den Empfänger

Wir werden sehen, daß der Commitment Service bessere Regelungen ermöglicht, die beide Seiten tatsächlich zufriedenstellen können – im Gegensatz zu a), b), c), wie in der Tabelle illustriert.

1.3 Commitment Service als Lösung zur fairen Verteilung der Haftung zwischen Sender und Empfänger

Die betrachteten Risiken haben ergeben, daß keine der Lösungen a), b), oder c) für sowohl Sender als auch Empfänger akzeptabel sind. Dies bedeutet nach den Regeln von Angebot und Nachfrage, daß potentielle Dienste, die unter idealen Bedingungen über das Internet möglich wären, erst gar nicht in Angriff genommen oder aber nach den ersten Fehlschlägen eingestellt oder nicht mehr in Anspruch genommen werden. Dies könnten Dienste sein, in denen es um sehr hohe Werte geht, wie z.B. Geldtransfer, Aktiengeschäfte, Dienstleistungen im Beratungsbereich, Handel mit großen Mengen an Frischware oder kundenspezifische Bestellungen und Sonderanfertigungen von Kraftfahrzeugen oder Computern. Jedoch können Attacken, die Tausende von kleinen Transaktionen durch eine Signatur veranlassen, auch Transaktionen, die in kleinerem Rahmen beabsichtigt sind, gefährden. So bleibt der elektronische Handel auf dem Internet nur in einem Rahmen, der dem Empfänger keine zu hohen Risiken impliziert, d.h. Anbieter werden sich nicht einem zu hohen Risiko widerrufener Aufträge, und Nutzer sich nicht einer potentiellen Haftung ohne akzeptables Limit für den Fall von kompromittierten digitalen Signaturen, aussetzen.

Die Lösung, die hier vorgeschlagen wird, soll diesen „Deadlock“ aufbrechen und beide Parteien ermuntern, ein Risiko bis zu einem gewissen Grad zu übernehmen, um etwas flexibleren elektronischen Handel innerhalb dieser Grenzen führen zu können, so daß das Risiko auch jeweils für den Geschäftspartner akzeptabel ist. Hierzu ist eine faire Risiko-Verteilung nötig:

- Der Signaturempfänger sollte in Kauf nehmen, daß Signaturen widerrufbar sind, jedoch als Ausgleich „Commitments“ (Zusicherungen) anfordern, die rechtsverbindlich und nicht widerrufbar sind. Für widerrufene Transaktionen ohne ausreichende „Commitments“ muß der Signaturempfänger selbst haften.
- Der Signierer sollte ein Risiko für „Commitments“ übernehmen, das in etwa seine geplanten monatlichen Verbindlichkeiten umfaßt. Im schlimmsten Fall wäre sein Verlust gleich dem Umfang der „Commitments“, die er im Monat ausgeben würde.

Die vorgeschlagene Lösung ist auch trotz unsicherer Rechnerausstattung des typischen Internet Benutzers anwendbar. Sie verhindert zwar nicht mögliche Angriffe, 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 begrenzt das Risiko nicht nur für Attacken, sondern auch für alle Angriffe durch mangelnde Sorgfalt bis hin zur Erpressung. Vor letzterem kann auch ein sicheres Gerät nicht schützen, jedoch kann der Commitment Service (sofern die Signatur unter den Regeln des Commitment Service Gültigkeit hat) den Schaden begrenzen.

Durch den Vertrag, den der Benutzer bei der Initiierung des Commitment Services unterschreibt, ist das Risiko für den Benutzer begrenzt sogar für den Fall, daß der Commitment Service selbst betrügerisch ist. Der schlimmste Fall ist derselbe wie im Falle einer Attacke, denn der Benutzer kann nachweisen, welches sein oberstes Haftungslimit ist.

Als weiterer Vorteil braucht der Commitment Service nicht auf eine Harmonisierung der Regulierungen zu warten, sondern er kann kurzfristig aufgebaut und angewandt 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. Im folgenden wird der Commitment Service vorgestellt, der um einiges flexibler ist als der anschließend vorgestellte Haftungszertifikat-Service, einem Sonderfall des Commitment Services, der genau zur Verteilung der Haftung bei digitalen Signaturenbenötigt wird.

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 Commitments des Benutzers, so daß sie einen bestimmten Betrag oder eine bestimmte Menge (je nach Art des Commitments) 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.
- Der Benutzer bestimmt selbst die Höhe seines (monatlichen) Limits.
- Der Benutzer bestimmt selbst den Inhalt des ausgegebenen Commitments. Bei Kreditkartenzahlungen dagegen können ohne Wissen des Kunden andere, auch höhere Beträge autorisiert werden (z.B. beim Leihen von Mietwagen oder Reservieren eines Hotelzimmers).

2.1 Definition des „Commitments"

Unter „Commitment" wird hier eine rechtsverbindliche Zusicherung verstanden, die vom Benutzer erfüllt werden muß. Die Zusicherung kann z.B. darin bestehen, jemandem einen bestimmten Geldbetrag zukommen zu lassen.

Ist eine Bedingung mit dieser Zusicherung verknüpft, so ist die Zusicherung nur gültig, falls diese Bedingung erfüllt ist. Diese Bedingung könnte lauten „falls der Schlüsselinhaber die Signatur zu dieser Transaktion Schlüsselinhaber für kompromittiert erklärt". Komplexere Bedingungen sind ebenfalls denkbar. Der Benutzer kann bereits bei der Initialisierung Bedingungen spezifizieren, und/oder bei der konkreten Anforderung eines Commitments.

Der Benutzer verpflichtet sich bei seiner Registrierung zu Commitments (z.B. insgesamt EURO 2000 pro Monat) durch einen Vertrag mit der Commitment CA, 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 Commitments, die der Benutzer später veranlaßt. Dies gilt aber auch für ausgegebene Commitments, die der Benutzer nicht veranlaßt hat, z.B. wenn er Opfer einer Attacke wurde. Allerdings muß der Benutzer keine Commitments 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.

Stellt die Commitment CA mit Hilfe ihrer digitalen Signatur ein Commitment im Auftrag des Benutzers aus und kommt dieses beim spezifizierten Begünstigten an, und ist die Bedingung zur Gültigkeit erfüllt (sofern eine solche spezifiziert wurde), so muß der Benutzer aufgrund des Vertrages das Commitment erfüllen. Dies geht für den Empfänger aus dem von der Commitment CA (in Form eines Zertifikats) bestätigten Commitment hervor. Um den

potentiellen Schaden für den Benutzer zu begrenzen, ist es jedoch sinnvoll, zu fordern, daß das Commitment seine Gültigkeit verlieren kann, wenn es nicht innerhalb von wenigen Wochen eingelöst wird oder der Benutzer der Gültigkeit zustimmt. Dies schränkt natürlich die möglichen Bedingungen ein, z.B. “gültig am 24. Dezember” wird im September eventuell keine sinnvolle Bedingung für ein ausgegebenes Commitment sein.

Man kann Commitments sehen als Blanko-Gutscheine mit benutzerspezifizierten Gültigkeitsbedingungen, die die Commitment CA auf Anforderung und insgesamt nur bis zu einem gewissen Limit ausfüllt, signiert und ausgibt. Selbst im Falle einer Attacke ist der Benutzer zumindest davor geschützt, daß sein Limit überschritten wird. Der Empfänger bekommt zwar kein Geld, jedoch ein rechtsverbindliches Commitment, das auch per Gericht eingeklagt werden kann, aufgrund des vom Benutzer unterschriebenen Vertrags.

2.2 Initialisierung des Benutzers

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 später Commitmentzertifikate ausgestellt werden, die den Schlüsselinhaber binden.

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

Beispiele für Commitments sind Geldbeträge oder ein maximal auszugebender Geldbetrag, aber es können auch Dinge sein (eine bestimmte Anzahl an spezifizierten (Ersatz-) Rechnern oder anderen Produkten) oder Dienstleistung (z.B. Stunden an Beratungstätigkeit, Service, Support). Die mögliche Stückelung muß von Anfang an klar sein (2 Stunden Dienstleistung am Stück sind etwas anderes als 120 mal 1 Minute Dienstleistung).

Die Commitments können aus den erlaubten Teilmengen der festgelegten Menge der Einzelcommitments bestehen. Bei Commitments über Zahlungen dürfen die Zahlungen insgesamt die festgelegte Geldmenge (bzw. das Geldlimit) nicht übersteigen.

Gleichzeitig kann der Benutzer für die jeweils möglichen Commitments Bedingungen festlegen, unter denen ausgegebene Commitments Gültigkeit haben sollen. Alternativ können die Bedingungen auch später im aktuellen Fall festgelegt werden. Eine solche Bedingung kann beispielsweise lauten:

- „gültig nur wenn die Signatur vom Benutzer für kompromittiert erklärt wird“ – dies ist im Spezialfall des Haftungszertifikats-Service der typische Fall,
- „gültig nur wenn der Benutzer (z.B. aus finanziellen Gründen) die Transaktion rückgängig machen möchte und dies (z.B. aus Kulanz) akzeptiert wird“,
- „gültig nur wenn der Signaturempfänger die mit dem Schlüssel *S* digital signierte Information *I* vorlegen kann“.

Die Gültigkeit selbst in Abhängigkeit von der Erfüllung einer Bedingung betrifft nicht das System selbst, sondern nur Signierer und Signaturempfänger. Die Bedingung kann damit grundsätzlich „blind“ durch die Commitment CA mitaufgenommen werden, ohne daß sie interpretiert werden muß.

Ein Vertrag mit dem Benutzer legt fest, daß sich der Benutzer zur Erfüllung aller vom Commitment Service ausgegebenen Commitments, unter den jeweils von der CA bestätigten und im Commitment spezifizierten Bedingung, verpflichtet. Genau für die Zusicherung dieser Verpflichtung agiert die Commitment CA als Zeugin – durch Ausstellung, Signierung und Ausgabe des angeforderten Commitmentzertifikats. Diese Verpflichtung gilt insbesondere auch für Commitmentzertifikate, 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 ein gültiges Commitment erhält. Die Notwendigkeit wird verlagert auf die Überprüfung der Commitment CA selbst.

Im Vertrag wird zudem vereinbart, auf welche Weise der Benutzer die Commitment CA veranlassen soll, ein Commitmentzertifikat auszugeben, und auf welche Weise der Commitment Service die Anfrage autorisieren soll, z.B. nur durch Prüfen der digitalen Signatur des Benutzers einschließlich Prüfen der Schüsselrückrufliste, oder auch durch weitergehende Maßnahmen, 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 des auszugebenden Commitments, ist ebenfalls denkbar.

2.3 Schlüsselzertifikat

Das von der Commitment CA ausgegebe Schlüsselzertifikat unterscheidet sich nicht grundsätzlich von Schlüsselzertifikaten anderer CAs. Entscheidend hier ist jedoch die „Policy“, d.h. daß sich der Empfänger einer Signatur darüber informieren kann, 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,
- dagegen jedoch ein Commitment nicht widerrufbar ist.

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 kein Commitment mehr ausgegeben, nachdem der Schlüssel zurückgerufen wurde. Es muß wieder eine neue Initialisierung mit neuem Schlüssel vorgenommen werden.

2.5 Anforderung und Ausgabe eines Commitments

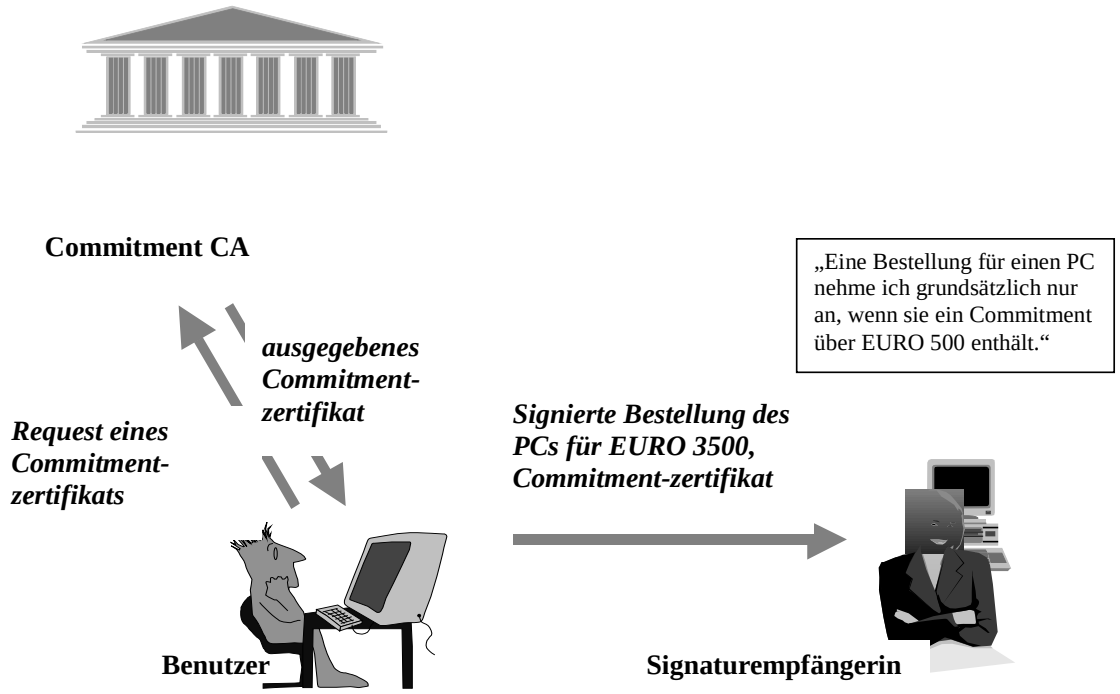

Abb.2: Vereinfacht dargestellte Transaktion

Möchte der Benutzer einem Geschäftspartner ein verläßliches nichtabstreitbares Commitment 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, z.B ein Pseudonym und eine Kundennummer)
- hash **(**
  - Eindeutige Kontext ID spezifiziert durch den Benutzer für die beabsichtigte Transaktion,
  - Eine eindeutige ID des Signaturempfängers (z.B. ein Pseudonym) **)** – 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.
- Commitments, die ausgegeben werden sollen, zusammen mit den jeweiligen (neuen oder bereits bei der Initialisierung festgelegten) Bedingungen, unter denen sie gelten sollen. (Z.B. Betrag, über den ein Commitment ausgestellt werden soll (z.B. EURO 500), wobei die Bedingung sein könnte, daß die Signatur als kompromittiert erklärt wurde.)

- Ggf. weitere Transaktionsinformation, die im Klartext oder verschlüsselt im Zusammenhang mit dem Commitment 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 ein Commitment ausgegeben wurde, ob die angeforderten Commitments insgesamt das vereinbarte Limit bzw. die vereinbarte Menge aller Commitments nicht bereits übersteigen, unter Einrechnung dessen, was bereits ausgegeben worden ist.

Waren alle Überprüfungen erfolgreich, so stellt der Commitment Service ein digital signiertes Commitmentzertifikat aus (das hier nur „Commitment“ genannt wird, wenn der Zusammenhang klar ist), das an den Benutzer zurückgeschickt wird. Zudem streicht der Commitment Service die ausgegebenen Commitments aus der Menge der Commitments, die noch ausgegeben werden können.

Das Commitmentzertifikat kann folgende Information enthalten:

- Seriennummer des ausgegebenen Commitmentzertifikats
- Benutzer ID (in der Form, wie sie der Benutzer dem Signaturempfänger zeigen möchte und von diesem verstanden wird)
- Dazugehöriger öffentlicher Schlüssel des Benutzers
- hash **(**
  - Eindeutige Kontext ID spezifiziert durch den Benutzer für die beabsichtigte Transaktion,
  - Eine eindeutige ID des Signaturempfängers (z.B. ein Pseudonym) **)**, siehe Request
- Commitments, die ausgegeben werden sollen, zusammen mit den jeweiligen Bedingungen, siehe Request
- Weitere Transaktionsinformation, die im Klartext oder verschlüsselt im Zusammenhang mit dem Commitment einen Zeitstempel von der Commitment CA bekommen soll, siehe Request.
- Datum und Zeit, Gültigkeit des Commitmentzertifikats
- Bestätigung daß der obige Schlüssel des Benutzers nicht zurückgerufen wurde
- Referenz zur Policy zu Anwendung und Gültigkeit der digitalen Signatur des Benutzers
- Signatur der Commitment CA, und Information zur Überprüfung ihres Zertifikats

Das ausgestellte Commitmentzertifikat wird dem Benutzer übermittelt. Dieser kann es überprüfen und weiß im Erfolgsfall, daß sich der darauf verlassen kann. Er braucht nicht die Schlüsselrückrufliste zu befragen, da das Commitmentzertifikat dessen Gültigkeit (zum Zeitpunkt der Ausgabe) bestätigt - auch nach einem Rückruf des Schlüssels ist der Benutzer an das Commitmentzertifikat gebunden, sofern es vor dem Zeitpunkt des Rückrufs ausgestellt wurde.

Ein Commitmentzertifikat kann auch im Kontext einer eigens dafür spezifizierten Transaktionen als nichtabstreitbarer Gutschein dienen. Eine Bedingung muß in diesem Fall gar nicht vorhanden sein.

Wenn man Probleme bei der Nachweisbarkeit des zustandegekommenen Vertrags befürchtet (z.B. wenn er mündlich zustandegekommen ist), kann der Händler ein Commitment über den zu bezahlenden Preis anfordern. Die Bedingung des Signierers könnte hier lauten „sobald die Leistung durch die Gegenseite erbracht wurde“, oder „falls die Leistung durch die Gegenseite bis zu einem bestimmten Termin erbracht wurde“. Der Händler könnte damit die Bezahlung gerichtlich erzwingen – denn es handelt sich um ein Commitment – müßte allerdings nachweisen, daß die Bedingung erfüllt war.

2.6 Betrugsmöglichkeiten durch die Commitment CA

Die Commitment CA hat den Zweck, Commitments des Benutzers zu verwalten und auf Anforderung des Benutzers auszugeben, und zwar nur innerhalb des vorher vereinbarten Rahmen pro Monat. Diesen Rahmen kann der Benutzer z.B. durch einen schriftlichen Vertrag nachweisen, den er unterschrieben hat und der ihm zu Beginn ausgehändigt wurde.
Damit verbleiben die folgenden Angriffsmöglichkeiten:

- Die Commitment CA könnte Commitments auch ohne Anforderung des Benutzers ausstellen und anderen betrügerischen Parteien zukommen lassen, auch unbemerkt vom Benutzer. Dieser würde es erst dann merken, wenn die Erfüllung des Commitments von ihm verlangt würde. Der schlimmste Fall wäre, daß sein monatliches Limit ausgeschöpft würde, eventuell für mehrere Monate, bis das erste der unberechtigten Commitments eingelöst wird. Um zu verhindern, daß sich die Limits über mehrere Monate summieren, ist die oben genannte Regelungen sinnvoll, die besagt, daß ein ausgestelltes Commitment innerhalb einer bestimmten Zahl von Wochen eingelöst werden muß und danach seine Gültigkeit verliert.
- Die Commitment CA könnte den Vertrag fälschen, den der Benutzer unterschrieben hat. Damit stünde Aussage gegen Aussage, da der Benutzer ebenfalls eine Version des Vertrages hat. Jedoch wäre es fatal, wenn betrügerische CAs handschriftliche Commitment-Verträge mit irgendwelchen Personen fälschen würden, von denen diese Personen gar nichts wüßten und auch keine anderslautenden Verträge zeigen könnten. Hieraus folgt zumindest, daß die Commitment CAs nicht beliebige Institutionen sein, sondern einer bestimmten Kontrolle unterliegen sollten.

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 eines Commitmentzertifikats, des Haftungszertifikats, ausgedrückt.

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

Beim allgemeinen Commitment Service könnte ein Commitment folgendermaßen lauten: „EURO 500 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 Empfänger als Entschädigung zumindest ein Commitment über EURO 500, die er auf jeden Fall bekommt, unabhängig vom tatsächlichen Schaden. Beim Haftungszertifikat-Service würde das Commitment dagegen wie folgt lauten: „je nach Schaden beim Empfänger *E* ***Haftung bis zu*** EURO 500 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 EURO 500. Beträgt der Schaden nur EURO 240 (z.B. Versandkosten plus Aufwand), so beinhaltet das Commitment nur eine Verpflichtung, EURO 240 zu erstatten. Die tatsächliche Verpflichtung kann durch Einigung (z.B. mit Hilfe von Nachweisen) oder vor Gericht festgelegt werden, jedoch kann sie EURO 500 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 des Commitments, die durch das Haftungszertifikat bestätigt werden soll, zuvor ausgehandelt werden. Beim Haftungszertifikat-Service würde das Commitment entsprechend wie folgt lauten: „je nach Schaden bei Empfänger E ***bis zu*** EURO 500 für Transaktionskontext *k*, gültig nur, wenn die Transaktion aus Gründen, die beim Schlüsselinhaber liegen, nicht zustande kommt.“

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

Zusätzliche benutzerspezifizierte Bedingungen zur Gültigkeit des Commitments gibt es beim Haftungszertifikatservice – im Gegensatz zum Commitment Service – jedoch nicht.

4 Offline Commitment Service mit Hilfe einer Smartcard

Den Commitment Service bei jeder Transaktion einzuschalten erscheint aufwendig. Er kann auch mit Hilfe einer Smartcard ausgeführt werden, die in gewissen Bereichen den Online Commitment Service ersetzen kann. Es gibt hierbei verschiedene Varianten.

4.1 Nutzung der Smartcard für die Kontrolle und Ausgabe der Commitmentzertifikate

Die Initialisierung läuft in diesem Fall wie gehabt, außer daß der Benutzer eine Smartcard bekommt, auf der das monatliche Limit nichtmanipulierbar eingestellt ist, das der Benutzer ausgeben kann. Optimalerweise sollte diese Karte auch gleich den Signierschlüssel des

Benutzers enthalten. Ein Verlust der Karte ist sofort zu melden, zum Rückruf des Schlüssels und um weiteren Schaden zu vermeiden.

Den Request (Abschnitt 2.5) richtet der Benutzer an die Karte. Die Karte führt dieselben Prüfungen durch wie die Commitment CA im Abschnitt 2.5, außer der Prüfung, ob der Schlüssel zurückgerufen wurde. Das Commitmentzertifikat – hier ohne die Bestätigung, daß der Schlüssel nicht zurückgerufen wurde – wird ebenfalls durch die Karte ausgestellt und mit einem karteninternen und kartenspeziellen Schlüssel der Commitment CA signiert. Ein solches Commitmentzertifikat ist ebenso rechtsverbindlich wie on-line von der Commitment CA ausgestellt. Jedoch muß der Empfänger zusätzlich überprüfen, ob der Schlüssel zurückgerufen wurde, bevor er sich auf das Commitment wirklich verlassen kann. Insbesondere für den Haftungszertifikat-Service ist die Verwendung einer Smartcard praktikabel.

Die Transaktionen, die generell mit einer Karte durchgeführt werden können, sollten in ihrem Wert möglichst nicht so hoch liegen wie der Aufwand, der benötigt würde, um eine Karte zu brechen oder zu manipulieren. Daher sollten die insgesamt ausgegebenen Commitments nicht nur monatlich, sondern auch total pro Karte limitiert sein. Für jede Karte sollte daher ein eigener Vertrag ausgegeben werden, um den Kartenbesitzer vor Ansprüchen jenseits des Limits zu schützen.

4.2 Nutzung der Smartcard zur Änderung der Limits

Sollen die Limits geändert werden, so muß der Benutzer dies normalerweise direkt bei der Commitment CA veranlassen, um Attacken zu vermeiden, die das den Benutzer schützende Limit umgehen können. Mit Hilfe einer Karte jedoch kann der Benutzer eine Änderung bis zu einem gewissen Ausmaß (das bei der Initialisierung des Commitment Services vereinbart wird) selbst vornehmen. Beispielsweise kann vereinbart sein, daß der Benutzer sein monatliches Limit dreimal pro Monat um denselben Betrag wieder aufstocken kann. Dies jedoch sollte mindestens die Eingabe eines exklusiv hierfür benötigten Passwords erfordern sowie eine Benutzerführung beinhalten, so daß der Benutzer weiß, was er tut. Mit einer digitalen Signatur auf der Karte wird die gewünschte Erhöhung unterschreiben, so daß dieser Schritt nachvollziehbar ist. Auch hier sollte die Anzahl der Aktionen zur Erhöhung pro Karte begrenzt sein. Selbstverständlich kann dieser Vorgang ohne sichere Geräte auch attackiert und eine höhere Limite erreicht werden. Darum ist es wichtig, daß das Ausmaß dieser Aktion begrenzt ist (siehe oben), um höheren Schaden zu vermeiden.

Auf diese Weise ist es möglich, das Risiko für den kompromittierten Fall flexibler zu staffeln, ebenso das Risiko des Verlusts der Karte. Mehrere Stufen können hier definiert sein, wobei die Sicherheit der Authentifizierung wachsen kann. Beispielsweise kann ein Anruf bei der Commitment CA erforderlich sein, die nach der Prüfung aller Daten und einiger vorher vereinbarter Kontrollfragen (z.B. Mädchenname der Mutter des Vaters, etc.) eine Kennung mitteilt, die man der Karte eingeben muß. Alternativ kann die Karte auch online von der Commitment CA geladen werden, nachdem der Wille des Benutzers, das Limit zu erhöhen, verifiziert wurde. Eine Karte kann zur Änderung des Limits insbesondere auch benutzt werden, wenn der eigentliche Commitment Service online, d.h. nicht auf der Karte selbst, ausgeführt wird.

5 Mögliche Varianten zum Online Service

Aus Platzgründen sollen mögliche Varianten des Online Service nur erwähnt werden.

- Der Request kann auch durch den Signaturempfänger erfolgen, jedoch muß dies durch den Schlüsselinhaber selbst spezifiziert und autorisiert werden. Der Nachteil ist, daß der Benutzer weniger Kontrolle hat, welche Commitments 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 das Commitmentzertifikat kann der Benutzer vor unberechtigt von der Commitment CA ausgegebenen Commitments geschützt werden.
- Weiterhin können sowohl Request als auch die Commitment auf anderen Wegen als dem Internet erfolgen, ebenso die Übermittlung des Commitments zum Signaturempfänger. Beispielsweise könnte der Request telefonisch erfolgen, das Commitment könnte gefaxt werden, und der Benutzer – der zu diesem Zweck nicht einmal einen Signierschlüssel bräuchte – könnte das Commitment weiterfaxen innerhalb einer Bestellung per Fax, die vom Empfänger eingescannt werden kann. Dies bedeutet: Die handschriftliche Unterschrift auf einem Fax, deren Rechtsverbindlichkeit fragwürdig ist, kann entscheidend “aufgewertet” werden durch ein aufgedrucktes nichtabstreitbares rechtsverbindliches Commitmentzertifikat. Oder der Benutzer kann ein Commitmentzertifikat telefonisch bestellen, das vom Commitment Service elektronisch direkt 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 Sinn macht.
- Im Falle einer kompromittierten Signatur kann eine alternative Regelung vom Benutzer grundsätzlich die Übernahme einer bestimmten Haftung verlangen, die auf jeden Fall übernommen werden muß. Dies kann überlappend mit zu erfüllenden Commitmentzertifikaten sein, d.h. dabei können Commitmentzertifikate bereits diese Haftung darstellen. Vor allem macht dies Sinn, wenn der Benutzer nicht oder nur wenig zur Abgabe von Commitments bereit ist.
- 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. Dieser Service könnte auch mit Hilfe einer von der Bank ausgegebenen Smartcard anstatt online ausgeführt werden.

6 Wer hat Interesse am Commitment Service

In Abschnitt 1.2.1 wurde gezeigt, daß andere suggestive Regelungen nicht für Signierer und Signaturempfänger beide akzeptabel sein können. Der Nutzen des Commitment Services liegt darin, das eigene Risiko zu minimieren, aber gleichzeitig dem potentiellen Geschäftspartner gerade soviel zu bieten, daß sein Risiko so akzeptabel wird, daß er zum effektiven Geschäftspartner werden kann.

Es liegt daher auf der Hand, daß es vor allem die Händler auf dem Internet sind, die von diesem Dienst profitieren, denn sie können nicht nur den Besteller identifizieren, sondern sich auch vor dessen Abstreiten der Bestellung schützen, indem sie ein rechtsverbindliches Commitmentzertifikat über einen Betrag verlangen, der ihrem Schaden entsprechen würde. Dies wird dem Händler bereits eine ähnliche Sicherheit bieten wie Signaturgesetze, die hochsichere Signierkomponenten vorschrieben. Ein weiterer Vorteil ist, daß ein Commitment (sofern sie nicht von einer Smartcard des Benutzers ausgegeben wurde) die Abfrage erspart, ob der Schlüssel des Bestellers bereits zurückgerufen wurde – die Notwendigkeit dieser 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 – die Unterschrift könnte irgend ein unbedeutendes Krakel sein), 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 erfolgen. Dies kann durch den Preis oder durch günstige Konditionen beim Händler wieder ausgeglichen werden.

Etwas weniger reizvoll scheint dieser Service auf ersten Blick für den Benutzer selbst, da ein gewisses Risiko eingegangen werden muß, geradezustehen für Commitments, die durch Attacken zustandegekommen sind. Jedoch muß man dies mit der Alternative vergleichen, nämlich einer rechtverbindlichen digitalen 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 abstreitbar ist. Es ist abzusehen, daß viele Händler rechtsverbindliche digitale Signaturen vom Kunden verlangen werden, sobald der gesetzliche Rahmen hierfür geschaffen sein wird. Commitmentzertifikate plus widerrufbare Signaturen (im Falle einer Attacke) können diese rechtsverbindlichen Signaturen ersetzen und gleichzeitig das Risiko für den Schlüsselinhaber begrenzen.

Der Commitment Service bietet also eine Risikoverteilung auf Gegenseitigkeit. Sowohl Signierer als auch Signaturempfänger tragen bei diesem Service dazu bei, daß das Risiko des anderen erträglich da vorhersehbar begrenzt bleibt.

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

7 Literatur

Baum_99 Birgit Baum-Waidner: Haftungsbeschränkung der digitalen Signatur durch einen Commitment Service; Arbeitskonferenz "Sicherheitsinfrastrukturen, Hamburg, 9.-10.März 1999.

Baum_99a 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.

Somm_98 Decision of 28 May 1998 - 8340 Ds 465 Js 173158/95 - "CompuServe"

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.