

(Neue) Ansätze für Geschäftsmodelle zum Einsatz digitaler Signaturen

Michael Welschenbach

SRC Security Research & Consulting GmbH

12.06.2003

Inhalt

1	Digitale Signaturen in der Sackgasse ?	3
2	Ein neuer Ansatz zur Zertifikatprüfung	4
3	(K)eine neue Rolle - Aufgaben der Acquirer	5
4	Vorteile des Modells	7

1 Digitale Signaturen in der Sackgasse ?

Die Vorstellung, die mit dem Einsatz digitaler Signaturen allgemein verbunden ist, geht davon aus, dass digitale Signaturen von den Besitzern der Signaturmedien und gültigen Zertifikaten erstellt und weitergegeben werden, und dass die Gültigkeit der Signaturen von jedem Empfänger ohne Beschränkung geprüft werden kann. Die vollständige Prüfung umfasst zwei Schritte: Zum einen ist die Signatur in Verbindung mit dem signierten Inhalt auf ihre Gültigkeit hin zu überprüfen, zum anderen die Gültigkeit des zugehörigen Zertifikats bzw. der Zertifikatskette bis zum Root-Zertifikat der ausgebenden Stelle. Zur Bestätigung der Gültigkeit des Zertifikats wendet sich der Empfänger in aller Regel an das ausgebende Trust Center, das die für diesen Zweck benötigten Auskunftsdienste (Verzeichnisdienste, Sperrlisten, OCSP) unterhält.

Dieser Ablauf basiert auf einem Drei-Parteien-Verhältnis, in dem zwar Zertifikatseigentümer und Aussteller einer digitalen Signatur (Cardholder, CH) in einem Vertragsverhältnis zur Zertifizierungsinstanz (Issuer, I) steht, nicht aber der Akzeptant (ACC) der Signatur:

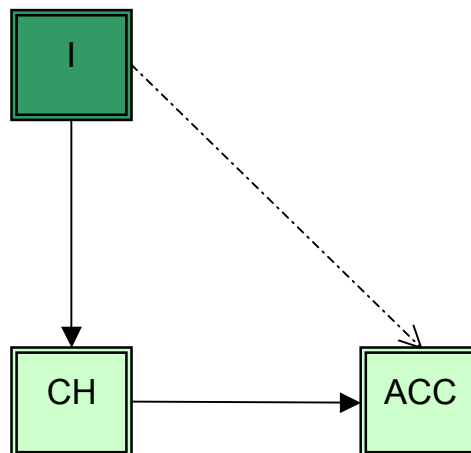


Abb. 1: Konventionelles Beziehungsschema zur Erzeugung und Prüfung digitaler Signaturen

Dieses Modell stellt dem Akzeptanten frei, eine Gültigkeitsauskunft vom Issuer einzuholen oder eben auch nicht. Der Akzeptant kann abwägen, ob er sich auf die lokale Prüfung der Signatur beschränkt, **ohne** eine Auskunft über die Gültigkeit des Zertifikats einzuholen, bzw. er kann sich auf eine bereits früher eingeholte Auskunft verlassen. Das Signaturgesetz (SigG) unterstützt eine solche Vorgehensweise, indem festgelegt wird, dass keine Prüfungspflicht besteht und eine Signatur unabhängig von einer Gültigkeitsprüfung durch den Akzeptanten dem Aussteller zugerechnet wird.

Im Allgemeinen gibt es keine Vertragsbeziehung zwischen Akzeptant und Issuer und damit keinen Rahmen, innerhalb dessen der Issuer seine Leistung der Auskunftserteilung über die Gültigkeit der Zertifikate dem Akzeptanten gegenüber fakturieren könnte. Die bisher in die-

sem Zusammenhang diskutierten Geschäftsmodelle gehen vielmehr davon aus, dass die Kosten für die Herausgabe einer Signaturkarte, für das Zertifikat und den Auskunftsdienst im Rahmen des Issuer/Cardholder-Verhältnisses abgedeckt werden, etwa durch einen finanziellen Beitrag des Cardholder oder durch Rationalisierungseffekte beim Issuer, was jedoch nur dann eintreten kann, wenn dieser gleichzeitig in der Rolle des Akzeptanten agiert.

Grob gesprochen fallen auf der Issuerseite die Kosten und auf der Akzeptantenseite der Nutzen an. Diese aus Sicht des Issuer ungünstige Situation kann nur dadurch aufgelöst werden, dass der Akzeptant an den Kosten für die Infrastruktur angemessen beteiligt wird.

Im Folgenden wird eine Möglichkeit erläutert, um eine solche Beteiligung auf dem Wege einer Strukturänderung zu forcieren und dabei gleichzeitig zusätzliche Services für die Akzeptanten einzurichten.

2 Ein neuer Ansatz zur Signatur- und Zertifikatprüfung

Der wesentliche Schritt zur Erreichung eines finanziellen Ausgleichs zwischen Issuer und Akzeptant liegt darin, die Einholung einer kostenpflichtigen Auskunft in Verbindung mit der Prüfung einer Signatur für den Akzeptanten **unverzichtbar** zu machen. Eine vierte Instanz könnte die Funktion einer Auskunftszentrale gegenüber dem Akzeptanten übernehmen. Die so entstehende Struktur ist vergleichbar mit der klassischen Vier-Parteien-Struktur der kreditwirtschaftlichen Zahlungssysteme: die Auskunftszentrale würde dort dem Acquirer (ACQ) entsprechen. Ein Acquirer innerhalb eines kreditwirtschaftlichen Zahlungssystems hat ein Vertragsverhältnis mit einem Händler und ermöglicht diesem so z.B. Kreditkartenzahlungen von seinen Kunden zu akzeptieren und führt alle hierfür notwendigen Prüfungen (z.B. Autorisierungen) durch.

Übertragen auf ein Vier-Parteien-System zur Signatur- und Zertifikatprüfung bedeutet dies, dass Auskunftszentrale (Acquirer) und Akzeptant ein Vertragsverhältnis eingehen. Im Auftrag des Akzeptanten vermittelt der Acquirer die Prüfung von Signatur **und** Zertifikat und teilt ihm das Prüfergebnis auf vertrauenswürdige Weise mit. Der Akzeptant wird durch eine solche Vorgehensweise von der aufwändigen Suche nach dem richtigen Ansprechpartner zur Verifizierung von Signaturen freigehalten, da dies vom Acquirer übernommen wird, der sich dazu seinerseits an den jeweiligen Issuer wendet.

Der Akzeptant zahlt ein Entgelt für die Gültigkeitsprüfung an den Acquirer. Für den Erhalt der Verifizierungsinformation zahlt der Acquirer im Rahmen der vertraglichen Vereinbarungen eine Interchange-Gebühr an den Issuer. Es ergibt sich die in Abbildung 2 dargestellte Struktur.

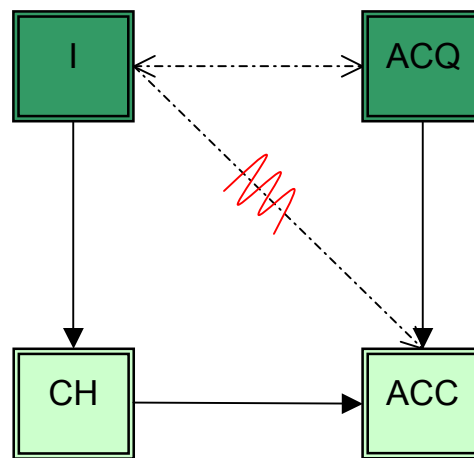


Abb. 2: Beziehungsschema zur Erzeugung und Prüfung digitaler Signaturen unter Einbeziehung von Acquireern

Als technischer Mechanismus, um die Prüfung von Signaturen für den Akzeptanten unverzichtbar zu machen, wird vorgeschlagen, die Signatur vor der Ausgabe durch die Chipkarte **zusätzlich mit einem symmetrischen Kryptoalgorithmus zu verschlüsseln**. Der hierzu verwendete Schlüssel ist nur dem Issuer bekannt, die Signatur kann ohne Kenntnis dieses Schlüssels nicht verifiziert werden.

Die Prüfung einer solchermaßen verschlüsselten digitalen Signatur geschieht nach folgendem Ablauf:

Der Akzeptant übergibt an „seinen“ Acquirer den Hashwert, die verschlüsselte Signatur und das Zertifikat des Cardholders. Der Akzeptant reicht diese Information an den entsprechenden Issuer zur Prüfung weiter. Dieser entschlüsselt die Signatur mit dem passenden symmetrischen Schlüssel und prüft die Signatur danach auf herkömmliche Weise. Die Zuordnung des passenden symmetrischen Schlüssels zum Cardholder erfolgt anhand dessen Zertifikat. Die Prüfung der Gültigkeit dieses Zertifikats rundet den Prüfungsvorgang ab. Die Antwort des Issuer wird integritätsgesichert an den Acquirer gesendet, der sie versehen mit seiner (unverschlüsselten) Signatur an den Akzeptanten sendet.

3 (K)eine neue Rolle - Aufgaben der Acquirer

Das wesentliche Merkmal in der Rolle der Acquirer liegt darin, dass die bisher unregelte Beziehung der Akzeptanten zu den Herausgebern von Signaturkarten und Zertifikaten durch vertragliche Regelungen ersetzt werden und somit alle handelnden Parteien in einen geregelten Kontext analog zu den kreditwirtschaftlichen Zahlungssystemen eingebunden sind.

Die Acquirer übernehmen die Aufgaben

- Gewinnung und vertragliche Bindung von Akzeptanten,
- Einrichtung und Unterhaltung einheitlicher Schnittstellen,
- Vermittlung von Gültigkeitsanfragen „seiner“ Akzeptanten an den jeweiligen Issuer,
- Fakturierung und Abrechnung der Gebühren gegenüber Akzeptanten und Isser.

Die bisherige Konzeption, wonach die Akzeptanten zum einen die Validierung von Signaturen selbst zu organisieren haben, zum anderen aber davon ausgehen können, dass sie die hierzu benötigten Auskünfte kostenlos beziehen können, wird durch ein für alle beteiligten Parteien vorteilhaftes, serviceorientiertes Vorgehensmodell ergänzt.

Aus der Rolle der Acquirer erwachsen die folgenden Vorteile:

- Die Akzeptanten werden im Umfang der Nutzung an den Kosten für die Infrastruktur beteiligt.
- Die Akzeptanten werden von der technischen Komplexität der Signaturprüfung freigehalten: Die Klärung, welcher Root-Schlüssel in die Prüfung einzubeziehen oder welches Gültigkeitsmodell zu Grunde zu legen ist, erfolgt durch den Acquirer. Der Akzeptant erhält maßgeschneiderte Information, die auch Auskunft über die Güte der Signatur (fortgeschritten, qualifiziert, qualifiziert mit Akkreditierung) geben kann. **Anders als in derzeitigen Denkmodellen wird die technische Kompetenz, die zur Klärung dieser Fragen erforderlich ist, nicht dem Akzeptanten abverlangt, sondern den hierauf spezialisierten Dienstleistern.**
- In Verbindung mit den Vermittlungsleistungen der Acquirer zur Signaturprüfung könnten weitere Dienstleistungen angeboten werden, wie etwa bestimmte Auskunftsdienste oder auch Garantieleistungen.

Aus der Sicht eines Akzeptanten ergibt sich das folgende Bild:

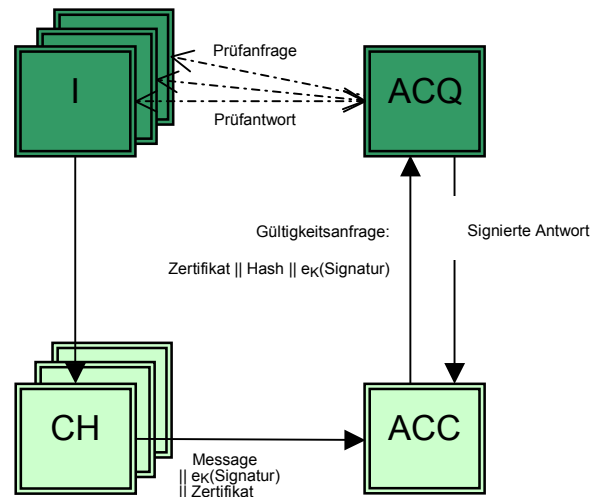


Abb. 3: Beziehungsschema mit mehreren Signaturkarteninhabern aus der Sicht eines Akzeptanten

4 Vorteile des Modells

Nach heutigem Stand ist festzustellen, dass die Akzeptanten mit den hiermit verbundenen technischen und organisatorischen Problemen der Signaturprüfung alleine gelassen werden. Hohe Investitionssummen für den Aufbau von PKI sind gerade für diejenigen Funktionen zu veranschlagen, die benötigt werden, um die komplizierten internationalen Gültigkeitsbeziehungen von Zertifikathierarchien verifizieren können. Dabei ist absehbar, dass Kosten für immer gleichartige Entwicklungsschritte in den Unternehmen immer wieder neu entstehen. Diese Perspektive mag mit dazu beitragen, dass sich die Nutzung digitaler Signaturen für den privaten Anwender (z. B. im eGovernment) bisher nur schleppend entwickelt.

Der Vorteil des vorgestellten Modells liegt gerade darin, dass die Last der technischen und organisatorischen Vorkehrungen, die zur Verifizierung von Signaturen und Zertifikaten erforderlich sind, dem Akzeptanten abgenommen und zu spezialisierten Dienstleistern verlagert wird. Die vereinfachte Prüfung von Signaturen würde sich gerade dann als vorteilhaft erweisen, wenn die Akzeptanten es bei dem für die Zukunft erhofften hohen Signaturaufkommen mit Signaturen und Zertifikaten aus einer Vielzahl unterschiedlicher Quellen zu haben werden.

Das Modell verfügt andererseits über genügend Flexibilität, die es erlaubt, auch unverschlüsselte Signaturen in die Abläufe einzubeziehen. Die zusätzliche Verschlüsselung ist lediglich als ein Briefumschlag anzusehen, in den eine Signatur verpackt wird und der, einmal zugeklebt, nur von einer autorisierten Stelle geöffnet werden kann.

Die Prüfung von Signaturen kann im gleichen Rahmen erfolgen, wenn auf diesen zusätzlichen Umschlag verzichtet wird.

Insgesamt ist festzuhalten, dass das Modell alle Vorteile der digitalen Signatur bewahrt und dabei zusätzlich ihre technische Handhabung in einem wirtschaftlich geregelten Rahmen erleichtert.