Bezahlsystem für einen Mixkaskaden-basierten Anonymisierungsdienst

Stefan Köpsell, Andreas Müller
sk13@inf.tu-dresden.de, am12@inf.tu-dresden.de

Abstract: Vorgestellt wird ein Bezahlsystem für einen Mixkaskaden-basierten Anonymisierungsdienst. Es ermöglicht eine Datenvolumen-abhängige Bezahlung. Das Bezahlsystem wurde unter dem Gesichtspunkt der praktikablen Anwendbarkeit entworfen, d. h. es werden existierende Zahlungsmethoden genutzt und die Qualität des Anonymisierungsdienstes wird nicht beeinträchtigt. Ein eventueller Betrug einer Partei wird erkannt und kann mit Hilfe von Nachweisen geahndet werden.

1 Einführung

„JAP“ ist ein Mixkaskaden-basierter Dienst zur Anonymisierung von HTTP-Verbindungen für den anonymen Zugriff auf das World Wide Web [BeFK01]. Jeder Nutzer muss sich dazu ein gleichnamiges Programm als lokalen Proxy für seinen Browser installieren. JAP dient als Schnittstelle zu sogenannten Mixkaskaden, über die die Kommunikation zu den Zielservern im Internet (um-)geleitet wird.

Ein Mix ist im wesentlichen ein Server, der mehrfach verschlüsselte Datenpakete empfängt, zwischenpuffert, umkodiert (durch Entschlüsselung eine „Verschlüsselungsschale“ entfernt) und umsortiert wieder ausgibt [Chau81]. Werden mehrere Mixe in Form einer statischen Kette hintereinandergeschaltet, so spricht man von einer Kaskade.

Die Anonymität ist gewährleistet, solange wenigstens ein Mix der Kaskade vertrauenswürdig ist. Dies gilt selbst unter der Annahme, dass ein Angreifer alle anderen Mixe kontrolliert und sämtliche Netzwerkverbindungen überwachen bzw. aktiv manipulieren kann (d. h. Pakete löscht, verändert, hinzufügt etc.)

Betrachtet man eine Kaskade als „Black Box“, so ist das Ziel, die Zuordnung von eingehenden zu ausgehenden Nachrichten zu verbergen. Es bleibt jedoch beobachtbar, wer den Dienst verwendet und an welche Empfänger Nachrichten gesendet werden. Beispielsweise „sieht“ ein Angreifer, wer welches „Bitmuster“ an den ersten Mix gesendet hat.

Jedem Mixbetreiber entstehen Kosten, die hauptsächlich durch das Datenvolumen der zu bearbeitenden Mixpakete verursacht werden [BFRW02]. Eine faire Möglichkeit zur Deckung der anfallenden Kosten besteht darin, diese auf die Nutzer umzulegen.

Bisherige Ansätze [FrJe98, FrJW98, BaNe99] nutzen zur Bezahlung der Mixpakete anonyme digitale Münzen. Diese werden vom Nutzer bei einer Bank erworben und den Mixpaketen mitgegeben. Da momentan keine Bank digitale Münzen anbietet, sind diese

Verfahren nicht praktikabel. Zudem hat eine Bezahlung mit digitalen Münzen generell den Nachteil, dass die Verhinderung von Betrug durch mehrfaches Ausgeben (engl. Doublespending) der selben Münze zum Teil erheblichen zusätzlichen Kommunikationsaufwand verursacht.

Daher wird ein kontobasiertes Bezahlsystem vorgeschlagen, welches auf vorhandene Zahlungsmethoden aufbaut und die Kommunikationsqualität der zu anonymisierenden Verbindung nicht verschlechtert. Es berücksichtigt die mehrseitigen Sicherheitsanforderungen aller involvierten Parteien (Nutzer, Mixbetreiber, Banken). Dies wird durch digital signierte Nachweise erzielt.

2 Architektur des Bezahlsystems

Beim Anonymisierungsdienst JAP kann der Nutzer zwischen verschiedenen Mixkaskaden frei wählen. Generell werden die Mixe einer Kaskade nicht einzeln bezahlt, sondern eine Kaskaden-zentrale *Abrechnungsinstanz* (AI). Auf Grund der statischen Struktur einer Kaskade (insbesondere gleiches Datenvolumen für alle Mixe) kann diese Instanz das Geld auf die beteiligten Mixe verteilen. Als Vorteil ergeben sich geringerer Aufwand und Komplexität des gesamten Bezahlsystems.

Die AI befindet sich vor dem ersten Mix und kennt daher gemäß Angreifermodell die Zuordnung von abzurechnenden Datenpaketen zu Nutzern. Der hohe Aufwand für ein anonymes (kontobasiertes) Bezahlsystem ist daher nicht notwendig, zumal diese Verfahren (z. B. [LoMP94], [BüPf89]) selbst wieder auf einen Anonymisierungsdienst zurückgreifen.

Der Nutzer besitzt unter einem Pseudonym ein *Guthabenkonto*, von dem die Kosten abgebucht werden. Dieses muss er zuvor mit Hilfe verfügbarer Zahlungsmethoden aufladen. Abhängig von der gewählten Zahlungsmethode braucht der Nutzer seine Identität jedoch gegenüber dem Geldinstitut und der Konto-verwaltenden Stelle nicht offenzulegen.

Damit er nicht bei jeder Mixkaskade ein separates aufzuladendes Konto benötigt, verwaltet eine Anonymisierungsdienst-zentrale *Bezahlinstanz* (BI) die Nutzerkonten. Der Nutzer bezahlt bei ihr für den Dienst und erhält die Möglichkeit, ihn unter freier Auswahl der Kaskaden zu nutzen. Von der BI erhalten die Abrechnungsinstanzen der Mixkaskaden die Kontoinformationen und rechnen die Kosten der Nutzer ab. Die Abrechnungsinstanzen haben eine (temporäre) Verbindung zur Bezahlinstanz.

Das Bezahlsystem besteht somit aus den Komponenten: Bezahlinstanz, Abrechnungsinstanzen und lokale Proxies der Nutzer (Abbildung 1).

Um den Dienst einer Mixkaskade zu nutzen, muss sich der Nutzer mit seinem Pseudonym gegenüber der AI authentisieren. Diese rechnet die Kosten seiner gesendeten und empfangenen Mixpakete über sein Pseudonymkonto ab. Dazu müssen die von der BI verwalteten Pseudonym- und Kontodaten des Nutzers bei der AI vorliegen. Um Robustheit gegen Ausfälle der BI oder deren Nichterreichbarkeit zu gewährleisten, sind die Authentisierung des Nutzers und die Abrechnung seiner Mixpakete nicht von einer ständigen Erreichbarkeit der BI abhängig. Bei einem Ausfall der Bezahlinstanz wäre andernfalls der

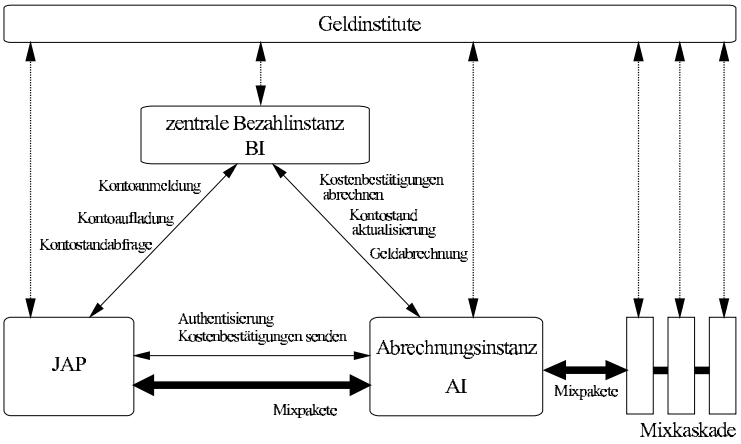

Abbildung 1: *Architektur des Bezahlsystems*

ganze Dienst bzw. die Abrechnung des Dienstes blockiert.

Die Abrechnung bzw. Zusammenführung der von den AIs übermittelten Kontostände bei der BI stellt sicher, dass die AIs das Geld für die geleisteten Dienste der Mixkaskaden erhalten. Gleichzeitig wird verhindert, dass die AIs die Möglichkeit des Betruges haben, indem sie Kosten eines Nutzers bei der BI abrechnen, die er nicht verursacht hat. Digitale Nachweise verhindern außerdem, dass die BI betrügt und dienen zur Kostenkontrolle durch den Nutzer.

3 Protokolle zwischen den Parteien

Generell erfolgt die Kommunikation zwischen den Beteiligten über konzelierte und integritätssichernde Verbindungen. Alle Protokollschritte sind durch ein Authentifizierungsprotokoll abgesichert, so dass z. B. man-in-the-middle- oder replay-Angriffe nicht möglich sind. Nachfolgend wird darauf nicht mehr explizit hingewiesen.

3.1 JAP-Bezahlinstanz-Protokoll

Kontoanmeldung Zur Kontoanmeldung generiert der JAP zuerst ein Schlüsselpaar eines Signatursystems. Der private Schlüssel bleibt dabei im Vertrauensbereich des Nutzers. Mit ihm authentisiert sich der Nutzer gegenüber den Abrechnungsinstanzen und der Bezahlinstanz und signiert unten näher erläuterte Kostenbestätigungen. Der öffentliche Schlüssel wird als Nutzerpseudonym P an ein Konto bei der BI gebunden (Abbildung 2).

Der JAP übermittelt zunächst den generierten öffentlichen Schlüssel. Die BI erzeugt eine

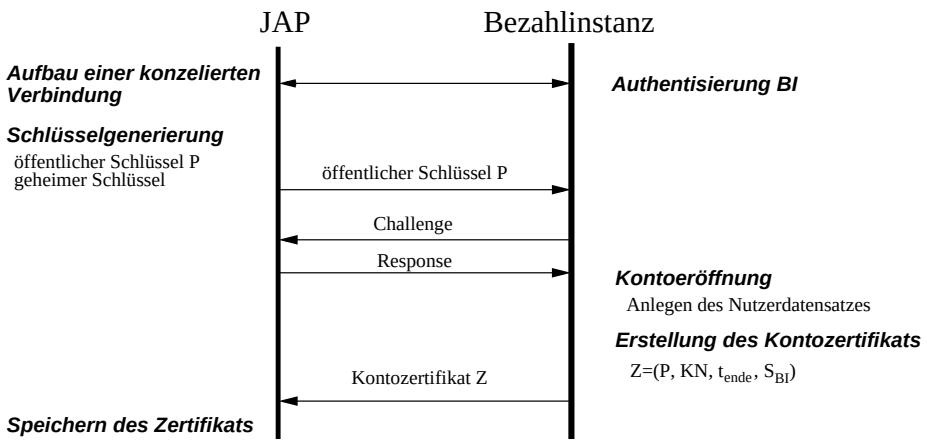

Abbildung 2: *Kommunikation bei der Kontoanmeldung*

für sie eindeutige Kontonummer *KN* und legt unter dieser ein Konto für den Nutzer an. Der öffentliche Schlüssel und die Kontonummer werden zusammen von der BI signiert und das resultierende Kontozertifikat

$$Z = (P, KN, t_{\text{ende}}, S_{\text{BI}})$$

an den JAP zurückgesendet. S_{BI} ist die digitale Signatur der BI über P, KN und t_{ende}. Der Zeitpunkt t_{ende} gibt das Gültigkeitsende des Zertifikats an. Mit dem Ablauf des Zertifikats wird auch das zugehörige Konto ungültig.

Kontoaufladung Zur Dienstnutzung muss das angemeldete Pseudonymkonto aufgeladen werden. Der JAP erfragt dafür bei der BI eine Überweisungsnummer *ÜN* als einmal gültiges Transaktionspseudonym. Die Überweisungsnummer wird durch die BI generiert, dort vermerkt und dem JAP zusammen mit der Pseudonymkontonummer und dem aktuellen $G_{\max}$ von ihr signiert übermittelt. Pro Konto können dabei nicht mehrere Aufladetransaktionen parallel durchgeführt werden.

Der Nutzer muss nun die Zahlung unter Angabe der Überweisungsnummer mit existierenden Zahlungsmethoden durchführen. Nach Eingang der Zahlung bei der Bezahlinstanz lädt diese das zugehörige Pseudonymkonto auf (Abbildung 3).

Als Nachweis der Kontoaufladung, erhält der Nutzer nach Eingang des Geldes eine Kontostandsinformation.

Kontostandsabfrage Wünscht der Nutzer eine aktuelle Kontostandsinformation, so sendet er eine entsprechende Anfrage an die BI. Er erhält von ihr eine signierte Bestätigung *KBN* seines aktuellen Kontostandes:

$$KBN = (KN, G_{\max}, K_{\text{Gesamt}}, t, S_{\text{BI}})$$

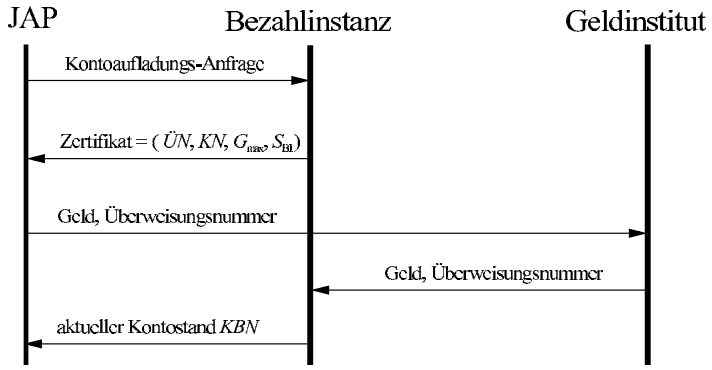

Abbildung 3: *Kommunikation bei der Kontoaufladung*

KN ist die Kontonummer des Kontos, $G_{\max}$ entspricht der *Gesamtsumme* des auf das Konto eingezahlten Geldes, K_{Gesamt} ist die *Gesamtsumme* der verursachten Kosten, t ist ein Zeitstempel und S_{BI} ist die digitale Signatur der BI über *KN*, $G_{\max}$, K_{Gesamt} und t. Damit ergibt sich das Guthaben $G = G_{\max} - K_{\text{Gesamt}}$, welches dem Nutzer noch zur Verfügung steht.

Die BI muss gleichzeitig die angefallenen Kosten K_{Gesamt} mit Kostenbestätigungen nachweisen. Dazu werden neben der Kontobestätigung *KBN* auch die entsprechenden Kostenbestätigungen B übermittelt. Die Kostenbestätigungen sind vom Nutzerpseudonym unterschriebene Erklärungen, mit denen es den Abrechnungsinstanzen bestätigt, den Dienst der jeweiligen Mixkaskade im angegebenen Umfang genutzt zu haben. Diese Erklärungen werden in Abschnitt 3.3 ausführlich erläutert.

Die signierte Kontobestätigung *KBN* gibt dem Nutzer unter der angegebenen Kontonummer das Recht, den Anonymisierungsdienst bis zur mit $G_{\max}$ angegebenen Kostenhöhe zu nutzen. Diese von der BI signierte Bestätigung muss lokal beim Nutzer bzw. dessen JAP gespeichert werden. Sie dient als Nachweis der Kontoaufladung. Bis zum Erhalt der Kontobestätigung nach einer Kontoaufladung muss sich der Nutzer den Nachweis der Zahlung (Kontoauszug o. ä.) und das Zertifikat, welches die Überweisungsnummer mit der Kontonummer verbindet, aufbewahren. Enthält die BI die Kontobestätigung *KBN* dem Nutzer vor, kann der Nutzer damit die Kontoaufladung und somit sein Dienstnutzungsrecht gegenüber Dritten nachweisen.

Um ein mehrmaliges Aufladen eines Pseudonymkontos zu ermöglichen, gilt für die Kontobestätigungen neben der oben genannten Nachweispflicht der Kosten K_{Gesamt} folgende Regel:

> *Die Kontobestätigung mit einem größeren Wert $G_{\max}$ ist die aktuell gültige Bestätigung und entwertet eine mit einem kleineren Wert $G_{\max}$.*

Speichert der Nutzer diesen Nachweis nicht, kann die Bezahlinstanz beim Nachweis der Dienstnutzung eine Kontobestätigung mit kleinerem $G_{\max}$ generieren und als aktuell präsentieren.

Wird ein Konto durch Ablauf des Kontozertifikates ungültig, verliert der zugehörige Nutzer auch das Recht an dem eventuell noch vorhandenen Guthaben des Kontos.

Sicherheitsbetrachtungen Behauptet der Nutzer ein höheres Guthaben $G_{\max}$ zu besitzen, als die BI zugibt, so muss er dies beweisen, indem er entweder folgendes vorlegt:

1. ein gültiges Kontozertifikat, für das er den privaten Schlüssel besitzt und eine zu dem Konto passende, gültige Kontobestätigung mit dem behaupteten $G_{\max}$

oder

2. ein gültiges Kontozertifikat, für das er den privaten Schlüssel besitzt, eine zu dem Konto passende, gültige Kontobestätigung mit einem $G'_{\max}$, ein passendes, gültiges Zertifikat, das die Zuordnung von einer Überweisungsnummer zu seinem Konto bestätigt und Beweise des Zahlungssystems, dass er eine Überweisung in Höhe von $G' = G_{\max} - G'_{\max}$ unter Angabe der Überweisungsnummer auf das Konto der BI getätigt hat.

Der erste Fall ist trivial. Im zweiten Fall kann die BI nicht betrügen, da auf Grund der vorgelegten Beweise klar ist, dass der Nutzer mindestens ein Guthaben von $G_{\max}$ besitzt. Gleichzeitig kann auch der Benutzer nicht betrügen, da der Versuch eines mehrmaligen Vorlegens desselben Überweisungsnummernzertifikats (inkl. Beweis des Zahlungseingangs) durch die Verkettung von altem Kontostand und Überweisungsnummer erkannt wird.

3.2 JAP-Abrechnungsinstanz-Protokoll

Will der Nutzer eine Mixkaskade nutzen, authentisiert sich sein JAP gegenüber der AI mit dem Kontozertifikat Z seines Nutzerpseudonyms und übermittelt eine Kontobestätigung *KBN*.

Mit Hilfe der Kontobestätigung kann die AI die Liquidität des Nutzers einschätzen. Enthält die Kontobestätigung einen älteren Zeitstempel, kann die AI von der BI einen aktuellen Kontostand anfordern (vgl. Abschnitt 3.3).

Ist auf dem Pseudonymkonto Guthaben vorhanden, antwortet die AI mit dem „Kostenanschlag“ der Mixkaskade. Dieser enthält Informationen über den Mixkaskadennutzungspreis (z. B. Preis pro Mixpaket) und die Länge des Bestätigungsintervalls. Dies gibt an, nach wieviel nicht bestätigten verursachten Kosten die AI eine Bestätigung des aktuellen Kostenstandes spätestens erwartet.

Wurde die Mixkaskade schon einmal genutzt, übermittelt die AI zusätzlich die vom Nutzerpseudonym zuletzt gesendete Kostenbestätigung

$$B = (\mathit{ID}, \mathit{KN}, K, S_P)$$

die aus der eindeutigen Kennung *ID* der Abrechnungsinstanz, der Kontonummer *KN* des Pseudonymkontos und dem bestätigten Kostenkontostand K des Pseudonyms bei der AI besteht. S_P ist die digitale Signatur des Nutzerpseudonyms P über *ID*, *KN* und K. Mit

der Signatur bestätigt das Nutzerpseudonym P, die Kosten K bei der AI bzw. deren Mixkaskade verursacht zu haben. Die AI kann mit der Kostenbestätigung B die Kosten K bei der BI vom Guthaben des Pseudonymkontos *KN* abrechnen. (siehe Abschnitt 3.3).

Der Kostenstand K ist kumulativ und gibt stets die Gesamtsumme der bei der Mixkaskade durch das Pseudonym verursachten Kosten an. Auf Grund der Bestätigung von Gesamtkosten, ist ein Betrug durch Doublespending von Kostenbestätigungen durch die AI nicht möglich.

Während der Dienstnutzung sendet und empfängt der Nutzer Mixpakete. Durch den übermittelten Kostenanschlag und die letzte Kostenbestätigung weiß der Nutzer, wann er welche Kostenbestätigung der AI übermitteln muss (Abbildung 4).

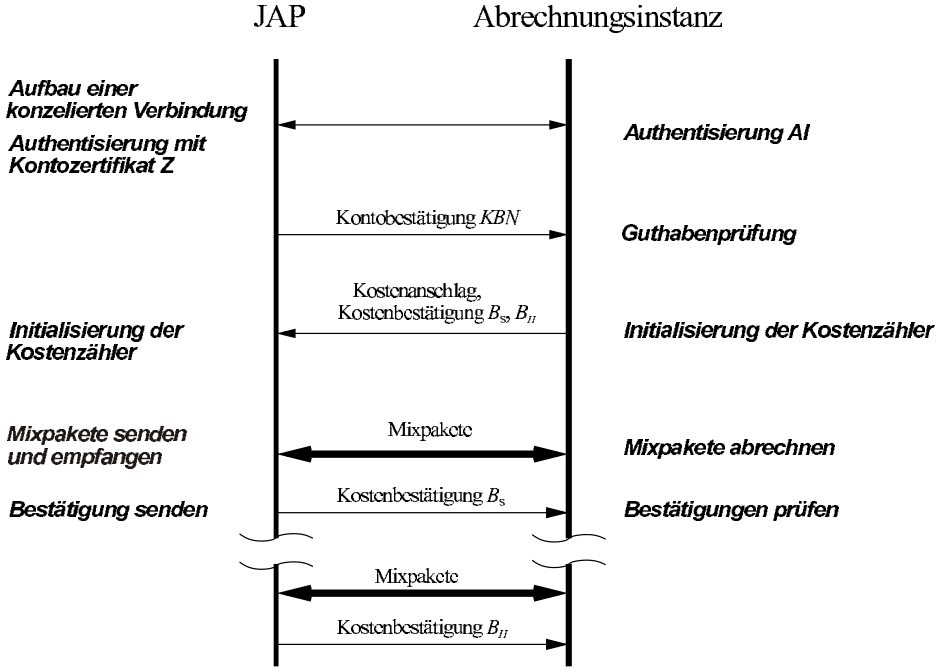

Abbildung 4: *Kommunikation zwischen JAP und Abrechnungsinstanz*

Zur Minimierung von Übertragungs- und Rechenaufwand wird nicht jedes Bestätigungsintervall durch eine *signierte* Erklärung bestätigt, sondern das in [Ped97] beschriebene Tickpayment-Verfahren genutzt. In jeder signierten Bestätigung B_{S} ist zusätzlich der Endwert einer Tickfolge enthalten. Eine Tickfolge ist eine Folge von Werten, die der Nutzer ausgehend von einem zufälligen Wert mit einer Einwegfunktion generiert und gespeichert hat. Der Nutzer übermittelt die Werte der Folge in umgekehrter Reihenfolge als Bestätigungen $B_{\mathrm{H}} = (h)$ an die AI. Die AI kann die Werte prüfen, indem sie die Einwegfunktion auf den neu erhaltenen Wert anwendet und das Ergebnis mit dem davor erhaltenen vergleicht.

Die signierte Bestätigung B_{S} wird um den Endwert h_{end} der Tickfolge, die Länge l der Folge und den Tickkostenwert w erweitert, der den Wert angibt, der durch einen Tickwert der Tickfolge bestätigt wird:

$$B_{\mathrm{S}} = (\mathit{ID}, \mathit{KN}, K, h_{\mathrm{end}}, l, w, S_P)$$

Durch diese signierte Bestätigung B_{S} und einen Tickwert h wird ein Kostenstand K_{result} bestätigt. Dieser ergibt sich aus dem in der signierten Bestätigung B_{S} enthaltenen Kostenstand K, dem Kostenwert w und dem Wert $k \leq l$, der für die Anzahl der Einwegfunktionsaufrufe steht, um von h zu dem Ergebnis h_{end} zu kommen[1]:

$$K_{\mathrm{result}} = K + k \cdot w$$

Sind die generierten Werte einer Tickfolge im JAP aufgebraucht, sendet er eine neue signierte Bestätigung, die den aktuellen Kostenkontostand und den Tickfolgenendwert einer neu generierten Tickfolge enthält. Die alte Bestätigung und den zugehörigen letzten Tickwert kann die AI löschen.

Sicherheitsbetrachtungen Versucht der Nutzer zu betrügen, indem er keine oder ungültige Bestätigungen schickt, blockiert die AI die Paketweiterleitung solange, bis der Nutzer die gewünschten Bestätigungen übermittelt. Dies bedeutet, dass eine Mixkaskade in Vorleistung tritt. Der Nutzer erreicht im Betrugsfall damit einen Vorteil gegenüber der AI, der jedoch den Umfang des durch die AI gewählten Bestätigungsintervalls nicht übersteigt.

Die AI kann versuchen zu betrügen, indem sie zu Beginn eine Kostenbestätigung B sendet, die höhere Kosten enthält, als durch den Nutzer bisher verursacht. Die Manipulation erkennt der Nutzer jedoch, da diese Bestätigung durch ihn selbst signiert sein muss. Da neben der AI auch der JAP des Nutzers das gesendete bzw. empfangene Datenvolumen messen kann, ist es auch nicht möglich, dass die AI Bestätigungen anfordert, obwohl das Bestätigungsintervall noch gar nicht vorüber ist.

3.3 Abrechnungsinstanz-Bezahlinstanz-Protokoll

Die Abrechnungsinstanzen kontaktieren in kurzfristigen Abständen die Bezahlinstanz zur Kostenbestätigungsabrechnung. In längerfristigen Intervallen, z. B. einmal im Monat, wird die BI von den AIs zur Geldabrechnung kontaktiert.

Abrechnung der Kostenbestätigungen Die AI kontaktiert in regelmäßigen Abständen die BI und rechnet die von den Nutzern erhaltenen Kostenbestätigungen B ab. Dazu übermittelt die AI die vom Nutzerpseudonym signierte Bestätigung

$$B_{\mathrm{S}} = (\mathit{ID}, \mathit{KN}, K, h_{\mathrm{end}}, l, w, S_P)$$

zuzüglich des zugehörigen zuletzt erhaltenen Tickwertes h an die BI.

[1] ist $f(x)$ die Einwegfunktion, so gilt $f^k(h) = h_{\mathrm{end}}$

Entsprechend dieser Bestätigung wird die neue Gesamtsumme der angefallenen Kosten K_{Gesamt} des zugehörigen Pseudonymkontos berechnet. Dazu wird das neue K_{Gesamt} aus den von den anderen AIs abgerechneten Kostenkontoständen K und dem neuen durch die Bestätigung B und dem Tickwert h bestätigten Kostenkontostand K der abrechnenden AI berechnet:

$$K_{\text{Gesamt}} = \sum_i K_i$$

Anschließend sendet die BI einen neuen Kontoschnappschuss

$$KSA = (ID, KN, G_{\max}, K_{\text{Gesamt}}, K, t, S_{\text{BI}})$$

des Pseudonymkontos *KN* signiert an die abrechnende AI zurück (siehe Abbildung 5).

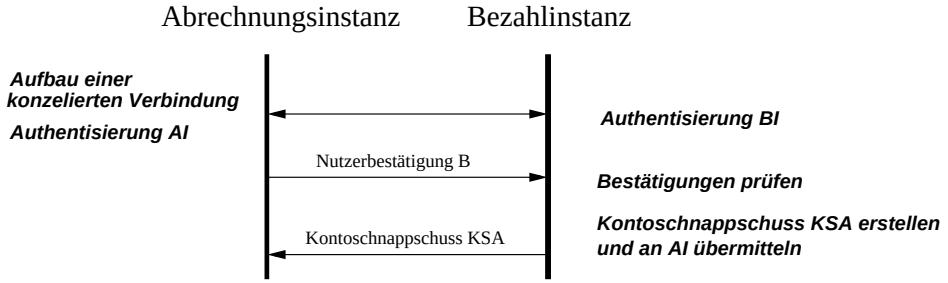

Abbildung 5: *Kommunikation beim Abrechnen der Kostenbestätigungen*

Mit diesem unterschriebenen Kontoschnappschuss erkennt die BI den Kostenkontostand K des Pseudonymkontos *KN* bei der AI *ID* zum Zeitpunkt t an. Der von der BI unterzeichnete Schnappschuss dient der AI als Nachweis der Dienstabrechnung.

Die BI speichert sich für jedes Pseudonymkonto und für jede AI den zuletzt bestätigten Kostenkontostand K und die dafür von der AI präsentierten Bestätigungen B. Mit diesen Bestätigungen muss die BI den Dienstnutzungsnachweis gemäß Abschnitt 3.1 führen.

Bei der Abrechnung besteht die Gefahr, dass das Guthaben des Pseudonymkontos nicht mehr die erforderliche Höhe hat, um der AI die Abrechnung zu bestätigen. Der AI gehen die Ausgaben verloren, die nicht durch das verbliebene Guthaben gedeckt sind. In diesem Fall hat der Nutzer zwar nachweisbar betrogen, eine Schadensregulierung kann jedoch nicht garantiert werden, da der Nutzer bei Verwendung einer anonymen Zahlungsmethode (z. B. Prepaid-Karte) gegenüber der Bezahlinstanz anonym bleiben kann.

Um die Gefahr eines Schadens zu verringern, sind die Kostenbestätigungen der Nutzerpseudonyme rechtzeitig bei der BI abzurechnen. Dabei gilt folgende Strategie:

> *Je geringer das Guthaben des Nutzers ist, bzw. je älter die Abrechnungsbestätigung der Bank ist, desto kürzer ist das Abrechnungsintervall für die Kostenbestätigungen durch die AI zu wählen.*

Kontostandsaktualisierung Wünscht die AI einen aktuellen Kontoschnappschuss *KSA* eines Nutzerpseudonymkontos, kann sie diesen von der BI anfordern — auch ohne eine Kostenbestätigung B des Nutzerpseudonyms abrechnen zu müssen.

Die Kommunikation verläuft analog zur Kostenabrechnung mit dem Unterschied, dass anstelle der Kostenbestätigung B die Kontobestätigung *KBN* an die BI übermittelt wird. Die BI antwortet wie bei der Kostenabrechnung mit einem aktuellen Kontoschnappschuss *KSA* des Pseudonymkontos.

Geldauszahlung an die Abrechnungsinstanzen Die Auszahlung von Geld durch die BI an die AI *ID* beginnt letztere durch Übermittelung einer Liste $(KN_1, \ldots, KN_n)$ mit Kontonummern, für deren Kostenkontostände $(K_{KN_1}, \ldots, K_{KN_n})$ sie Geld ausgezahlt bekommen möchte. Die BI übermittelt eine Überweisungsnummer, unter der sie die Geldüberweisung durchführen wird sowie die Höhe des auszuzahlenden Geldbetrages.

Das Geld kann die BI den AIs mit klassischen Zahlungsmethoden überweisen. Als Bestätigung des Geldempfangs übermitteln die AIs eine signierte Kostenauszahlungsbestätigung *KAB* an die BI (Abbildung 6).

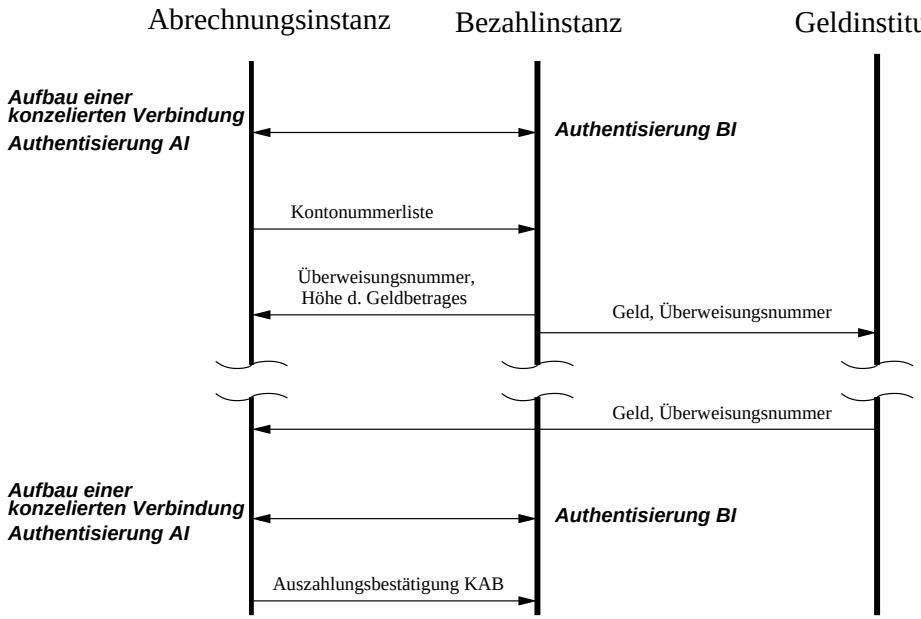

Abbildung 6: *Kommunikation bei der Geldabrechnung*

Die Kostenauszahlungsbestätigung *KAB* ist die von der AI signierte Liste der ausgezahlten Kostenkontostände der Pseudonymkonten. Leere Kostenkontostände sind in dieser

Bestätigung nicht enthalten.

$$KAB = (ID, \{KN_1, K_{KN_1}\}, ..., \{KN_n, K_{KN_n}\}, S_{ID})$$

ID ist die Kennung der AI, KN_i ist die Kontonummer und K_{KN_i} der Kostenkontostand K des Pseudonymkontos KN_i bei der AI *ID*. S_{ID} ist die digitale Signature der Abrechnungsinstanz *ID* über *ID* und alle übertragenen KN_i und K_{KN_i}. Damit bestätigt die AI von der BI für die angegebenen Kostenstände der Pseudonymkonten Geld empfangen zu haben. Diese signierte Bestätigung speichert sich die BI, bis sie eine Kostenauszahlungsbestätigung mit höheren oder gleichen Kostenständen der Pseudonymkonten von der AI erhält.

Die AI übermittelt bei der nächsten Geldauszahlung der BI eine neue Bestätigung der verrechneten Kontostände. In der neuen Bestätigung müssen alle Konten der Vorgängerbestätigung enthalten sein, damit die BI die vorherige Bestätigung löschen kann.

Sicherheitsbetrachtungen Betrügt eine AI, indem sie Geld von der BI für nicht erbrachte Leistungen erhalten will, so hat die AI zwei Möglichkeiten, dies zu versuchen:

1. Sie versucht, Kostenbestätigungen für nicht erbrachte Leistungen abzurechnen. Dabei kann sie jedoch nicht die Bestätigungen B_{S} fälschen, da diese durch den Nutzer signiert sind. Eine AI kann auch keinen Tickwert h berechnen, so dass $f^l(h) = h_{\text{end}}$ gilt. Dies beruht auf den Eigenschaften der zugrundeliegenden Hashfunktion f.

Versucht die AI mehrmals die selbe Kostenbestätigung B abzurechnen (Doublespending), so wird dies durch die BI erkannt, da die Kosten K kumulativ geführt werden und nach der ersten Abrechnung von B somit bei der BI ein größeres K gespeichert ist, als in der Bestätigung B angegeben.

2. Die AI versucht, bei der Geldauszahlung zu betrügen. Dabei kann sie nicht einfach beliebige Kosten K angeben, da die BI nur Kontoschnappschüsse *KSA* akzeptiert, die von ihr zuvor digital signiert wurden. Auch das mehrmalige Abrechnen wird erkannt, da die AI der BI bestätigen muss, für welche Kosten sie bereits Geld erhalten hat. Diese Bestätigung speichert sich die BI. Verweigert die AI das Senden der Bestätigung, so kann die BI mit Hilfe von durch das Zahlungssystem generierten Beweisen gegenüber Dritten belegen, dass sie für die abgerechneten Kosten bezahlt hat. Damit hat die AI betrogen.

Versucht die BI zu betrügen, indem sie der AI die Bezahlung angefallener Kosten bzw. das Senden von Kostenbestätigungen verweigert, so kann die AI mit den von der BI bzw. den Nutzer in der Vergangenheit zugesandten Bestätigungen gegenüber Dritten die ihr zustehende Bezahlung nachweisen.

4 Zusammenfassung und Ausblick

Es wurde ein Abrechnungssystem für einen Anonymisierungsdienst vorgestellt, das sich im Gegensatz zu den bekannten Verfahren mit heute verfügbaren Bezahlmöglichkeiten umsetzen lässt. Durch die Verwendung von digital signierten Belegen wird Schutz vor Betrug für jede beteiligte Partei erreicht. Da die Guthaben und angefallenen Kosten jeweils

nur kumulativ geführt werden, werden Probleme mit Doublespending bzw. einer umfangreichen Speicherung von bereits abgerechneten Quittungen vermieden.

Das vorgeschlagene System wird momentan implementiert und in den vorhandenen Anonymisierungsdienst JAP integriert. Anschließend soll eine Evaluierung (ein „Proof of Concept“) durchgeführt werden. Dies wird unter Beteiligung der „echten“ Nutzer des Dienstes geschehen (allerdings zunächst unter Verwendung von „Spielgeld“).

Literatur

[BaNe99] Matthias Baumgart, Heike Neumann. *Bezahlen von Mix-Netz-Diensten*. Verläßliche IT-Systeme – VIS 1999, Vieweg-Verlag, 1999

[BeFK01] Oliver Berthold, Hannes Federrath, Stefan Köpsell. *Web MIXes: A system for anonymous and unobservable Internet access*. in: Hannes Federrath (Ed.): Designing Privacy Enhancing Technologies. Proc. Workshop on Design Issues in Anonymity and Unobservability, LNCS 2009, Springer-Verlag, Heidelberg 2001, 115–129.

[BFRW02] Thomas Butzlaff, Florian Jäger, Björn Rober, David Weber, Andreas Wilm. *Praxisprojekt: JAP – Anonymität im Internet*. Handelshochschule Leipzig, Dezember 2002.

[BüPf89] Holger Bürk, Andreas Pfitzmann. *Digital Payment Systems Enabling Security and Unobservability*. Computers & Security 8/5, 1989, 399–416.

[Chau81] David Chaum. *Untraceable Electronic Mail, Return Addresses, and Digital Pseudonyms*. Communications of the ACM 24/2, 1981, 84–88.

[FrJe98] Elke Franz, Anja Jerichow. *A Mix-Mediated Anonymity Service and Its Payment*. ESORICS ’98 (5th European Symposium on Research in Computer Security), Louvain-la-Neuve, LNCS 1485, Springer, Berlin, 1998, 313–327.

[FrJW98] Elke Franz, Anja Jerichow, Guntram Wicke. *Payment Scheme for Mixes Providing Anonymity*. IFIP Working Conference on Electronic Commerce 98, LNCS 1402, Springer, Berlin 1998, 94–108.

[LoMP94] S. Low, N. Maxemchuk, and Sanjoy Paul. *Anonymous credit cards*. 2nd ACM Conference on Computer and Communications Security, Fairfax, Virginia, ACM Press, 1994, 108–117.

[Ped97] Torben P. Pedersen. *Electronic Payments of Small Amounts*. Security Protocols 96, LNCS 1189, Springer, Berlin, 1997, 59–68.