
Sichere Zahlungssysteme in offenen Netzen

Thomas Denny

SRC Security Research & Consulting GmbH, Bonn

1 Motivation

Die kartengestützten Zahlungssysteme stellen einen wesentlichen Ausgangspunkt bei der Entwicklung von Verfahren zur elektronischen Abwicklung von Zahlungen über offene Netze dar. Bereits sehr frühzeitig wurde z. B. der Einsatzrahmen von Kreditkarten auf das Internet ausgeweitet durch Definition entsprechender Transaktionen als Mail Order/Telephone Order (MO/TO)-Transaktionen, die "remote" und ohne Karteninhaberverifikation abgewickelt werden. Im Falle einer Reklamation durch den Karteninhaber kann der Kartenemittent (Issuer) die bestrittene Transaktion im Wege eines sogenannten Chargebacks an die Händlerbank (Acquirer) zurückgeben. Zahlungen mit Kreditkarte verfügen aktuell weltweit über einen sehr hohen Marktanteil bei allen Internet-Zahlungen, während der Marktanteil des kartengestützten Zahlungsverkehrs an den Zahlungsvorgängen an Ladenkassen deutlich niedriger liegt.

Europay International stellte für das Jahr 2001 bis Oktober 2001 bereits insgesamt 2,5 Millionen E-Commerce-Transaktionen mit Europay-Kreditkarten in Europa mit einem Gesamtvolumen von 175 Millionen Euro fest. Die Steigerungsraten sind dabei sehr hoch: Im Oktober des Vorjahres lag die Zahl der registrierten E-Commerce-Transaktionen noch unter 500.000. Europay International geht davon aus, dass bereits 2 % des gesamten Umsatzes mit Kreditkarten über öffentliche Netze, also über das Internet oder über Mobilfunknetze, abgewickelt werden.

Es zeigte sich allerdings frühzeitig, dass die Durchführung von Kreditkartenzahlungen als (MO/TO)-Zahlungen auf Dauer ungeeignet ist, um wirtschaftlich Kartenzahlungen über das Internet abwickeln zu können. Die Zahl von Reklamationen zu Kreditkartentransaktionen über das Internet ist innerhalb kurzer Zeit so stark angestiegen, dass es dringend erforderlich wurde, zu anderen Verfahren zu kommen. Bei dem enormen prognostizierten Wachstum für Online-Transaktionen stellen die Wachstumsraten bei Reklamationen ein enormes wirtschaftliches Risiko für die an den Zahlungssystemen beteiligten Kreditinstitute dar, das nicht vernachlässigt werden darf.

Aufgrund der fehlenden Authentisierung des Kunden bei (MO/TO)-Transaktionen kann der Händler nicht beweisen, dass der Kunde die Transaktion getätigt hat und muss eine Rückgabe akzeptieren. Diese Situation stellt ein großes Hindernis für die Ausweitung des elektronischen Handels speziell auf den Handel mit Informationen oder Online-Dienstleistungen dar. Anbieter, die entsprechende Leistungen anbieten, sind auf eine Zahlungsgarantie angewiesen, da die Leistung direkt konsumiert wird.

Die internationalen Kartengesellschaften haben außerdem eine Migration der Kartentechnik auf die Chiptechnologie für Zahlungs- und Geldautomaten-Anwendungen gemäß dem von Europay International, Visa International und MasterCard-International vorgelegten EMV-Standard beschlossen. Ziel ist es, die Migration bis zum 1.1.2005 abzuschließen.

2 Unterschied Point of Sale (POS) und offene Netze

Am POS setzt der Kunde eine Karte (Chipkarte oder Magnetstreifen) an einem Zahlungsverkehrsterminal ein. Die Autorisierung kann offline (bei Einsatz der Chipkarte) oder per Online-Nachfrage beim Issuer erfolgen. Bei der Offline-Variante hat der Issuer dem Karteninhaber im voraus einen Offline-Verfügungsrahmen eingeräumt und das Zusammenspiel zwischen Terminal und Kundenkarte stellt dessen ordnungsgemäße Verwendung sicher. Bei der Online-Nachfrage werden Authentisierungsdaten des Kunden zum Issuer gesendet. Die Antwort mit positivem Returncode ist für den Händler die Zahlungsgarantie und wird durch das Terminal abgesichert.

Am POS werden die schützenswerten Daten des Kunden über den Händler und dessen Kommunikationswege zum Issuer gesendet. Dies ist nicht mehr unbedingt notwendig, falls der Kunde "online" ist und selbst eine Verbindung zum Issuer herstellen kann.

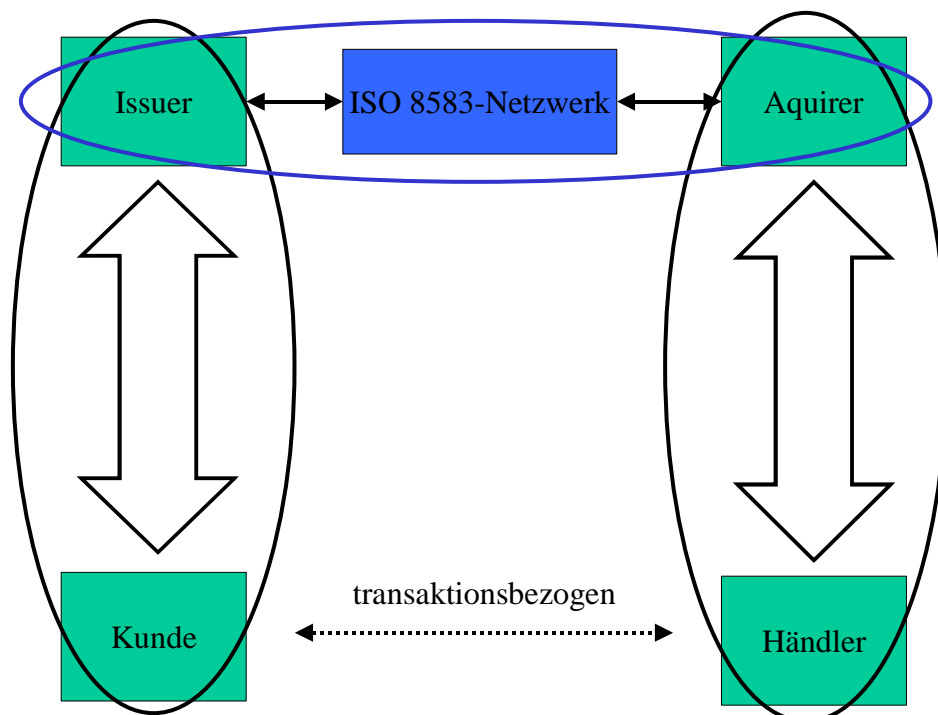


Abbildung 1: 3-Domänenmodell

Das Händlerterminal am POS erfüllt wichtige Aufgaben wie die Ablaufkontrolle und informiert über den Zahlungsausgang. Sowohl der Kunde als auch der Händler vertrauen dem Terminal und den Anzeigen bzgl. des Transaktionsbetrages. Im E-Commerce fällt das POS-

Terminal zumindest in der bekannten Form weg und andere Komponenten müssen die folgenden Aufgaben übernehmen:

- Authentisierung zwischen Kunde und Issuer
- Absicherung des Transaktionbetrages
- Festlegung des Zahlungsempfängers

3 Lösungsansätze

In der Vergangenheit wurde bereits mehrfach versucht, technische Lösungen zu etablieren, um diesem Problem zu begegnen. In der Praxis konnte sich allerdings noch keine dieser Lösungen durchsetzen. Die internationalen Zahlungssysteme begegnen daher dem Problem nunmehr nicht allein durch die Bereitstellung einer technischen Lösung, sondern auch durch begleitende geschäfts- und preispolitische Maßnahmen, die die Einführung entsprechender Verfahren fördern. Neben den möglichst gering zu haltenden Anpassungen an den Systemen der Händler, der Issuer und der Kunden haben diese Maßnahmen einen entscheidenden Einfluss auf den Erfolg dieser neuen Zahlungsverfahren in der Praxis.

Mit 3D-Secure und UCAF (Universal Cardholder Authentication Field) stehen sowohl bei VISA International als auch bei MasterCard International technische Lösungen zur Verfügung, die eine Authentikation des Karteninhabers durch den Kartenemittenten im Rahmen einer Autorisierung ermöglichen und den Anforderungen der Trennung der realen Welt von der Welt des Internets begegnen. Die Einführung entsprechender Verfahren wird z.B. bei MasterCard sowohl durch preispolitische als auch durch geschäftspolitische Instrumente gefördert. Händler, die das sog. UCAF-Feld zur Weitergabe der Authentikationsdaten des Karteninhabers unterstützen, sollen künftig, unabhängig davon, ob der Kartenemittent UCAF bereits unterstützt oder nicht, eine Zahlungsgarantie erhalten. Darüber hinaus soll für UCAF-fähige Händler zwischen Acquirer und Issuer eine günstigere Interchange für den Acquirer gelten, die die mit UCAF verbundene technische Änderung für Acquirer und Händler zusätzlich wirtschaftlich interessant machen kann.

Werden vom Kartenemittenten keine Maßnahmen zur Authentisierung des Kunden etabliert, so kann dies dazu führen, dass der Kunde einer vom Issuer autorisierten E-Commerce-Transaktionen widersprechen kann, ohne dass der Issuer die Möglichkeit hat, den Schaden an den Acquirer zurückzubelasten. Für die Kartenemittenten geht es daher zunächst einmal darum, sich vor einem missbräuchlichen Bestreiten von Transaktionen zu schützen. Zusätzlich geht es aber auch darum, Transaktionen über öffentliche Netze insgesamt sicherer zu machen und damit auch zusätzliche Kundenkreise für solche Transaktionen zu interessieren. Neben der Höhe der Transaktion ist z. B. auch die Identität des Empfängers abzusichern.

4 UCAF

Das UCAF-Verfahren stellt einen normierten Transportmechanismus von Daten des Kunden zum Issuer über die Systeme des Händlers und des Acquirers dar. Die Software, die beim Kunden die Kommunikation steuert, wird als Wallet bezeichnet. Zur Übertragung von Daten zwischen Wallet und Händler werden sogenannte Hidden-Fields eingesetzt. Das sind für den Kunden unsichtbare Felder auf den Internetseiten des Händlers, denen Daten entnommen und in die Daten zur Übertragung an den Händler eingetragen werden können. Die Entnahme und das Eintragen der Daten erfolgt durch das Wallet.

Die Art der Prüfung der Authentizität des Kunden obliegt dem Issuer. Das Konzept sieht zur Erzeugung von Kundenauthentisierungsdaten (UAD) die Kommunikation der Wallet mit einem zentralen System des Issuers dem sogenannten IWS (Issuer Wallet Server) vor. Somit kann auf einfache Art eine Übertragen von Daten des Issuers zum Händler über den Kunden erfolgen.

Die Kommunikation zwischen Issuer und Acquirer erfolgt über standardisierte Online-Nachrichten. Der Konzeptansatz geht dabei normalerweise von einer Kommunikation über den IWS aus. Die folgende Abbildung erläutert die Kommunikationsbeziehungen für ein UCAF-basiertes Verfahren.

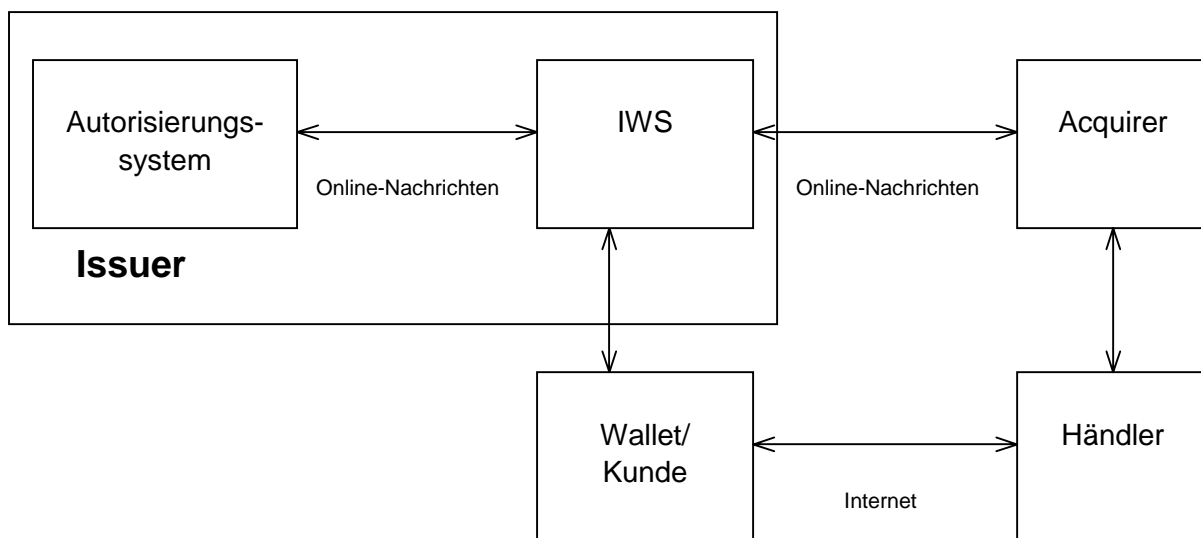


Abbildung 2: UCAF-Modell

Bei einer eingehenden Autorisierungsanfrage eines Acquirers prüft der IWS die zuvor generierten Kundenauthentisierungsdaten, ob eine entsprechende vom Kunden initiierte Transaktion existiert und leitet die Anfrage nach einer evtl. notwendigen Anpassung der Nachricht an das Autorisierungssystem weiter. Die Antwort des Autorisierungssystems wird auch über den IWS an den Acquirer und den Händler weitergeleitet. Der Lösungsansatz eines IWS sorgt dabei dafür, dass die Autorisierungssysteme des Issuers nicht zwingend angepasst werden müssen.

Die Aufgaben des IWS im Konzeptansatz bestehen somit aus:

- der Prüfung der Authentizität des Karteninhabers,
- der Unterstützung bei bzw. der Erzeugung von UAD,
- der Prüfung der UAD und
- dem evtl. Ersetzen bzw. Anpassen von Daten in Online-Nachrichten.

Das UCAF-Konzept kann für verschiedene Zahlungsverfahren benutzt werden, da die Struktur der Daten nicht auf eine Anwendung beschränkt wurde. Insgesamt stehen 24 Byte für die Übertragung von Daten (1 Byte Systemdaten und 23 Byte Issuer-Daten) zur Verfügung.

5 Umsetzung

Bei Transaktionen im Internet sind die Anforderungen aus der Kundenauthentifizierung und der Absicherung der Transaktionsdaten nicht immer einfach umsetzbar. Aus Sicherheitssicht und aufgrund der bevorstehenden EMV-Migration ist die Umsetzung mit einer Chipkarte beim Kunden naheliegend. Die Chipkarte übernimmt die Identifikation des Karteninhabers und die Generierung eines Transaktionskryptogramms. Die vertrauenswürdige Anzeige der Transaktionsdaten kann von einem vom Karteninhaber kontrollierten Chipkartenleser übernommen werden.

Aus Sicht des Kartenemittenten sollten keine technischen Unterschiede in der Autorisierung in Abhängigkeit vom technischen Kommunikationskanal existieren. Um die Abwicklungskosten von Transaktionen möglichst niedrig zu halten, ist es vorteilhaft, wenn am Point of Sale und bei Transaktionen über öffentliche Netze dieselben Technologien und Verfahren zum Einsatz kommen. Für die Chipkarten-gestützte Abwicklung bedeutet dies, dass eine Orientierung am EMV-Standard vorteilhaft wäre. Die Verwendung eines Standards, der übergreifend am Point of Sale zum Einsatz kommt, spart sowohl bei den Karten als auch bei den Hintergrundsystemen (IWS) zusätzliche Entwicklungs- und Pflegekosten. Eine Anpassung der Online-Nachrichten durch das IWS und die Überprüfung der Autorisierungsdaten des Kunden durch das IWS könnte somit entfallen.

Gelingt es die Aufgabe der Erzeugung der UAD an eine geeignete Komponente des Kunden zu delegieren, so wird bei einer Orientierung am EMV-Standard kein IWS auf Seiten des Issuers benötigt. Dann sind die drei folgenden Themenbereiche zu betrachten:

1. Entwicklung einer EMV-fähigen Chipkarte,
2. Bereitstellung eines entsprechenden Chipkartenlesers für den Kunden und
3. Limitierung der UAD auf die 23 Byte, die bei UCAF zur Verfügung stehen.

Entwicklung einer EMV-fähigen Chipkarte

Zur Umsetzung des EMV-Standards auf ZKA-Chipkarten wurde das Betriebssystem SECCOS ergänzt, die EMV-Kommandos umgesetzt und die EMV-Anwendung spezifiziert. Dadurch sind die Voraussetzungen zum Einsatz von EMV-fähigen ZKA-Chipkarten bei Zahlungen über offene Netze geschaffen.

Bereitstellung eines entsprechenden Chipkartenlesers für den Kunden

Einerseits wird es darum gehen, dem Kunden eine möglichst große Zahl von Anwendungen zu erschließen, die er mit dem Sicherheitsmodul seiner Bank (seiner Chipkarte) nutzen kann, andererseits ist nicht auszuschließen, dass – zumindest in gewissem Umfang – Karte und Terminal technisch miteinander verbunden werden.

Die Nutzungsmöglichkeiten für „Persönliche PIN-Pads“ können vielfältig sein. Von der Möglichkeit der Verwendung für das Bezahlen von Waren und Diensten im Internet über die Absicherung der Kommunikation zwischen Kunde und Bank (z.B. für Homebanking-Transaktionen oder zum Laden der GeldKarte) bis hin zu Zusatzdiensten, die nicht unmittelbar mit der Karte zu tun haben, vom Karteninhaber aber als nützlich empfunden werden.

Neben der Anpassung der vom ZKA entwickelten Internet-Kundenterminals für Debit- und Credit-Anwendungen im Internet können auch weitere Geräte wie PDAs oder spezielle Low Cost-Geräte, die nicht mit einem Kunden-PC verbunden sind, als „Persönliche PIN-Pads“ eingesetzt werden. Die Möglichkeit zur mobilen Kommunikation durch die Integration einer Mobilfunkschnittstelle in PDAs und die Einsatzmöglichkeiten über mehrere Kanäle stellen interessante Funktionserweiterungen für Persönliche PIN-Pads dar.

Limitierung der UAD auf die 23 Byte

Eine geschickte Generierung und der Aufbau der Transaktionskryptogramme innerhalb der Vorgaben der Spezifikation der EMV-Anwendung erlauben die Übertragung der zur Überprüfung des Kryptogramms durch den Issuer benötigten dynamischen Daten, innerhalb der Vorgaben des UCAF-Konzeptes.

6 Fazit

Insgesamt zeigt sich, dass sich durch den Einsatz der normierten Verfahren und Konzepte der internationalen Zahlungssysteme und deren nationaler Umsetzung auf der ZKA-Chipkarte ein sicheres Zahlungsverfahren über offene Netze etablieren lässt. Die skizzierte Umsetzung benötigt dabei neben den Anpassungen für die EMV-Migration auf Chipkarten keine nennenswerten spezifischen Anpassungen durch den Einsatz in offenen Netzen an den Systemen der Issuer. Somit bestehen neben der generellen Umsetzung der EMV-Anwendung der Issuer keine weiteren Abhängigkeiten, die einer schnellen Umsetzung im Wege stehen.

Mittel- bis langfristig dürften auf dem EMV-Standard basierende Chipkarten in Verbindung mit Kundenterminals, die unterschiedlichen Zwecken dienen, eine wichtige Rolle spielen. Die Tatsache, dass diese Terminals für den weltweiten Einsatz geeignet sind, dürfte einer raschen und kostengünstigen Umsetzung der zu entwickelnden Persönliche PIN-Pads zuträglich sein.