

### 3DSecure - Sichere Online Geschäfte in der Praxis

**Gabriele Disselbeck**  
syngenio AG

Der Handel mit Waren und Dienstleistungen hat sich im 21. Jahrhundert gewaltig verändert. Das Internet entwickelte sich zum bevorzugten Marktplatz für die Beschaffung von Informationen und Produkten. Auch das kartengestützte Bezahlen von Gütern ist in dieser virtuellen Umgebung bereits gelebte Praxis – die Nutzung steigt von Jahr zu Jahr. Die Konsumenten schätzen vor allem die Flexibilität des Einsatzgebiets und die Vertrauenswürdigkeit des Mediums. Die Nase vorn haben heute Zahlverfahren, deren Nutzung bereits eine hohe Akzeptanz am Point of Sale (POS) erreicht hatte, deren analoge Nutzung im Internet aber keine zusätzliche Kompromittierbarkeit produziert.

Heute ist die Kreditkarte aufgrund dieser Messkriterien ein beliebtes Zahlungsmedium im Internet. Die Angabe von Kreditkartennummer und Verfalldatum - ggf. ergänzt durch den sogenannten CVC2 / CVV – reicht aus, um eine bargeldlose Zahlung im Internet zu initiieren. Im Notfall kann mittels eines Anrufs beim Kreditkartenherausgeber eine nicht autorisierte Zahlung reklamiert werden. Das ist einfach, bequem und – aus Sicht des Karteninhabers – sicher.

Andererseits bieten Bezahl-Anwendungen in der virtuellen Welt und die immer größere Vernetzung heute deutlich anonymere und weitgreifendere Angriffsszenarien für den Kartenmissbrauch. Attacken auf den elektronischen Zahlungsverkehr, welche vor ausgesuchten Geldausgabeautomaten oder POS zur Erlangung von Kartendaten dienen, sind schon lange keine Einzeldelikte mehr. Dagegen nehmen gezielte und DV-technisch gestützte Angriffsszenarien auf Massendaten mit weitgreifenden monetären Konsequenzen und imageschädigender Natur kontinuierlich zu.

Somit ist das Internet nicht nur ein chancenträchtiger neuer Markt zur Ertragssteigerung, sondern gleichzeitig auch Schauplatz einer neuen Form von Kartenkriminalität. Aktuell beklagen sowohl Online-Händler als auch kreditkartemittierende Banken einen dramatischen Anstieg der Ausfallquoten, bei denen zwar Waren im Internet verkauft, die Zahlungstransaktionen aber reklamiert werden. Diese Entwicklung schwächt nachhaltig den Business Case für den kartengestützten Zahlungsverkehr. Allein in den letzten 24 Monaten hat sich für eine Vielzahl der großen deutschen Kreditkartenherausgeber die Ausfallquote aus dem Card-not-Present (CNP) Geschäft mindestens verdoppelt.

Einen möglichen Lösungsansatz zur Aufhebung dieses Trends stellt die Einführung einer zusätzlichen Authentifizierung des Karteninhabers während des Bezahlvorgangs dar. Die Kartenorganisationen Mastercard und VISA haben hierzu unter den Brands „Mastercard SecureCode“ und „Verified by Visa“ ein gemeinsames Verfahren etabliert, welches losgelöst von der herkömmlichen Autorisierung einer Zahlungstransaktion eine zusätzliche, separate Karteninhaber-Authentifizierung durchführt. Dieses Verfahren wird zusammenfassend als 3DSecure Technologie bezeichnet.



Führt ein Händler dieses neue Verfahren in seinem Onlineshop ein, so erhält er für nahezu alle bei ihm mit Kreditkarte abgewickelten Zahlungstransaktionen eine Zahlungsgarantie. Damit greift im Internet erstmalig die sogenannte Haftungsumkehr (Liability Shift), die dazu führt, dass Reklamationen seitens des Karteninhabers nicht mehr auf den Händler zurück belastet werden, sondern bei der kartenausgebenden Bank verbleiben. Die Einführung dieser Business Rule seitens der Kartenorganisationen führt nun - ähnlich wie schon bei EMV - dazu, dass Henne-Ei Diskussionen zwischen kartenausgebenden und kartenakzeptierenden Banken verebben und die Akzeptanz der neuen Technologie auf beiden Seiten – Issuing wie Acquiring – gleichermaßen hoch ist.

#### 3DSecure – Authentisierung mit System

Was verbirgt sich nun hinter dieser neuen Funktionalität 3DSecure – wie funktioniert sie, und was muss man als kartenausgebende Bank bei ihrer Einführung berücksichtigen?

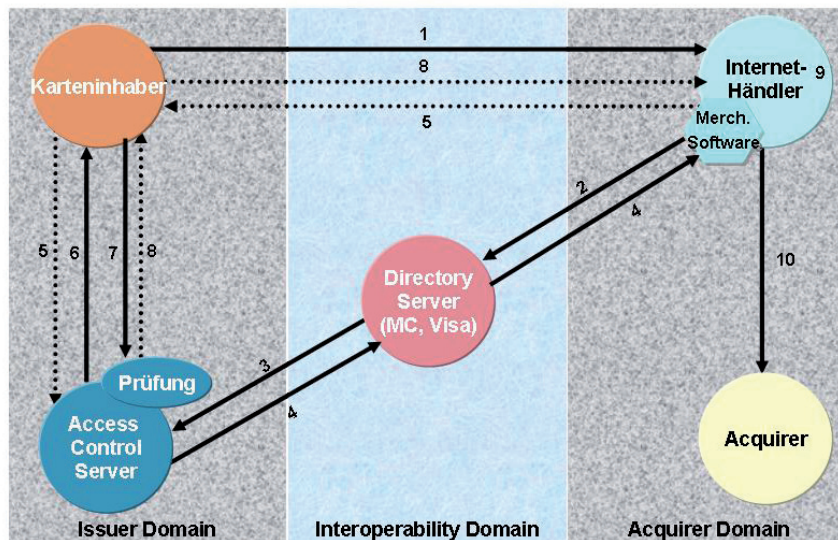
Zusätzlich zu den üblichen Systemen eines Issuing- und Acquiringprocessing wird für 3DSecure ein weiterer Server im Internet etabliert, der ausschließlich dafür verantwortlich ist, vor der Durchführung der klassischen Autorisierung einer Zahlungstransaktion eine weitere Authentisierung des Karteninhabers vorzunehmen.

Letztlich geht es bei 3DSecure immer darum, dass der Initiator einer Transaktion beweisen muss, dass er tatsächlich der Karteninhaber ist. Um das Abgreifen aller notwendigen Daten für die Durchführung einer Zahlungstransaktion zu verhindern, teilen sich zwei unabhängige Systeme die Daten. Das etablierte Autorisierungssystem des Issuers hält – wie gehabt – Kartennummer, Verfalldatum und CVC2/CVV sowie alle weiteren für die Durchführung einer Autorisierung notwendigen Daten. Der 3DSecure Server – auch Access Control Server (ACS) genannt – hält die Kartennummer und

das zusätzliche „Geheimnis“ für die Durchführung der Authentisierung.

Das Routing in den Netzen zu den jeweilig verantwortlichen Servern findet für beide Transaktionsbestandteile durch die Kartenorganisationen Mastercard und VISA anhand der Kartennummer (genauer gesagt, der BIN Range, in der sich die Kartennummer befindet) statt.

Als zweite Sicherheitsstufe wird vor der bekannten Autorisierung bei der Nutzung von 3D Secure durch den Internethändler und den Karteninhaber noch eine separate Authentisierung des Karteninhabers unter Nutzung des zweiten Servers durchgeführt. Da keines der beiden genutzten Systeme alle notwendigen Daten für Authentisierung plus Autorisierung hält, ist alleine durch die Teilung der Aufgaben ein Abgreifen aller notwendigen Daten für die Generierung einer sogenannten „fraudulent transaction“ deutlich erschwert.



### Grad der Authentisierung – Skalierbarkeit als Chance

Wenige Aspekte werden im Markt so kontrovers diskutiert und positioniert wie der „richtige“ Level der Authentisierung. Der Vorteil von 3D Secure ist, dass die Basislösung für die Nutzung des separaten Servers universell einsetzbar ist. Sie funktioniert mit statischem Passwort genauso wie mit kontextsensitiven One-Time-Passworts und allen Evolutionsstufen dazwischen. Die Entscheidung für den Grad der Authentisierung trifft jeder

Issuer im Rahmen der Etablierung der Lösung für sich und setzt damit auch die Standards für den Umfang des Projektes - proportional zu der Hürde für zukünftige Fraud-Attacken, die seine Kartenportfolien unbeschadet überstehen werden.

Hier die richtige Entscheidung auf der Skala zwischen Minimum und Maximum zu treffen, erfordert eine genaue Abwägung verschiedener Faktoren: Die relevanten Aspekte bewegen sich in dem Wertesystem Time-to-Market, Ease-of-Use und Akzeptanz beim Karteninhaber. Ein hoher Grad der Authentisierung würde beispielsweise eine Haftungsumkehr auf den Karteninhaber ermöglichen, was aber wiederum dazu führen kann, dass der Karteninhaber die Karte nicht mehr einsetzen möchte.

Viele Projekte beginnen aus diesem Grund auch heute noch mit einem statischen Passwort, von dem ggf. beim Einkauf nur Teile (einzelne Buchstaben) abgefragt werden, da diese Vorgehensweise schnell zu realisieren ist und vom Kunden sofort verstanden und genutzt werden kann. Die Erfahrung zeigt, dass diese Ease-of-Use-Strategie bereits ausreicht, um die wesentlichen Ziele des Issuers (Vertrauenswürdige Internet-Payment, Umsatzsteigerung durch Einsatz dieses Mediums, Reduzierung des Datenmissbrauchs) zu erreichen.

Selbstverständlich sind die heutigen Implementierungen von 3D Secure hinsichtlich ihres Authentisierungsgrades Einstiegslösungen, die sich im Verlauf der nächsten Jahre - ähnlich wie die Angriffsattacken - weiterentwickeln werden. Im Sinne des schnellstmöglichen und einfachen Einstiegs in das Verfahren leisten sie jedoch schon heute einen wichtigen Beitrag zur Akzeptanz. Die Erfahrung aus frühen Implementierungen höherwertiger Authentisierungen (beispielsweise kontextsensitive TANs, sogar mit Kartenleser) zeigt deutlich, dass die Komplexität der Lösung und organisatorische Hürden (Wie komme ich an den Kartenleser?) dazu führt, dass ambitionierte technologische Lösungen weder vom Kunden verstanden, noch in der Breite genutzt werden.

Das Erfolgsgeheimnis besteht demnach in einem schnellen, barrierefreien und komfortablen Einstieg, um rasch die kritische Masse an Nutzern zu erreichen. Hier kann man – wie in zahlreichen ähnlichen Projekten – vieles falsch, aber auch alles richtig machen.

### Motivation zur Teilnahme generieren – Push und Pull für Registrierungen

Das entscheidende Bewertungskriterium für den Erfolg dieser neuen Funktionalität ist eine möglichst hohe Akzeptanz seitens der Karteninhaber. Die Motivation zur Nutzung des Systems kann nur dann gelingen, wenn das Registrierungsverfahren für jeden Anwender ohne Vorkenntnisse durchführbar ist. Bankkunden, die das Internet zur Buchung und Zahlung

bereits aktiv nutzen, bilden die Kernzielgruppe für 3DSecure. Diese Kunden verfügen über ausreichende Erfahrung im Umgang mit den neuen Medien und akzeptieren eine geringfügige Veränderung ihrer Nutzungsgewohnheiten, wenn damit eine signifikante Erhöhung der Datensicherheit erreicht werden kann. Mit gezielten Maßnahmen können potenzielle Teilnehmer während einer Transaktion auf das neue Verfahren hingewiesen werden: Mittels „Activation-during-shopping“ werden Karteninhaber, die gerade mit ihrer Karte im Internet einkaufen, auf den neuen Mechanismus aufmerksam gemacht und können sich sofort zur Teilnahme registrieren.

Erscheint dem Karteninhaber diese Aufforderung zur Registrierung während des Einkaufs als störend, kann er den Einkaufsprozess zunächst ohne Registrierung abschließen und im Nachgang eine Registrierung auf der Homepage seiner Bank durchführen. Diese Kombination von freiwilliger Registrierung auf der Homepage der Bank und verpflichtender Registrierung während des Einkaufsprozesses ist ein bewährtes Modell beim Einsatz von 3DSecure. Kombiniert wird dieses Verfahren mit einer Vorgabe, wie oft ein Karteninhaber im Einkaufsprozess die Registrierung verweigern kann. Eine Anzahl von 1 bis 3 sogenannter „opt-outs“ wird momentan vorgesehen, wobei die Empfehlungen der Kartenorganisationen dazu übergehen, nach einer gewissen Etablierung der Funktion am Markt diesen Opt-out-Faktor in den laufenden Projekten weiter herabzusetzen.

### **Paradigmenwechsel in der Kommunikation**

Ein weiterer wesentlicher Aspekt für eine erfolgreiche Einführung und Nutzung des neuen Sicherheitsmediums ist die intensive Kunden-Kommunikation und Aufklärung durch die Bank. Mündige Karteninhaber sind längst sensibilisiert für die kriminellen Energien rund um den kartengestützten Zahlungsverkehr und erwarten die uneingeschränkte Offenheit ihrer Bank. In diesem Dialog ist es zwingend notwendig, dass Bank und Karteninhaber sich als Partner verstehen und darin übereinstimmen, dass es Missbrauch von kartengestütztem Zahlungsverkehr im Internet gibt, dem man nur zusammen erfolgreich begegnen kann.

Die aktuellen Einführungen von 3DSecure zeigen, dass mit diesem Verfahren nicht nur Missbrauch reduziert werden kann, sondern sogar Umsatzsteigerungen im Netz stattfinden. Somit wird die ursprüngliche Zielsetzung, die Ertragssituation des kartengestützten Zahlungsverkehrs zu verbessern, in mehrfacher Hinsicht und zur Zufriedenheit aller Beteiligten erreicht.